Annual Report Summary 2017

úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-8914-3

Foreword by the Office President

Ladies and gentlemen,

You are holding in your hands the Annual Report of the Office for Personal Data Protection for the year 2017. I am certainly not going to lecture you here on how to read these lines and thus preordain what you should find in them - or even between them.

This annual report concludes the seventeen-year period of the Office for Personal Data Protection founded on the basis of Act No. 101/2000 Coll., on Personal Data Protection. As is generally known, starting 25 May 2018 it is being replaced by the General Data Protection Regulation (GDPR). Integrated protection of personal data and the free movement thereof are crucial for fulfilling the four fundamental freedoms on which the functioning of the European Union is based. The free movement of persons, services, goods and capital is organically tied to digitised personal data, and the GDPR merely reflects the situation whereby personal data are a desired commodity, and sometimes even an unquestioned currency.

In this regard I would thus like to mention that over this past year this regulation was deliberately demonised, being used to offer services and


2017

conclude deals with those who are bound by its obligations. The Office for Personal Data Protection attempted to face down this demonisation while at the same time not downplaying the need to prepare for the regulation's provisions. I would venture to say that whoever has devoted adequate attention to personal data protection should have no significant problems with putting the regulation into practice.

This should be helped along by the trend of less formal yet still factually substantiated decisions the Office for Personal Data Protection has been striving for in recent years, something that continued in 2017 as a gradual and focused process. In practice this means primarily assessing the purpose being pursued in the processing of personal data with due diligence and even at the price of moving away from purely formal perspectives and established methodologies. This all while maintaining respect for the right of each of us to have our well-grounded claims redressed or our legitimate interests and privacy protected. The Office would approach certain cases from the past more prudently, for example ekolo or Kravaře, which went to court. In both cases the Office would no longer issue a fine. This is just one of the ways I want to send a clear signal to the public that the Office's decisions are gradually evolving towards not punishing those who are protecting their right against intruders in a reasonable manner.

It is always primarily necessary to properly examine whether the personal data processing is in pursuit of a legitimate, legally certified goal, or whether it unduly encroaches on the sphere of another. At the same time it is necessary to evaluate whether there were not also other options available, ones that encroach less into the legal sphere of other persons, by which the goal of data processing could have been achieved. It is primarily the one whose privacy has been infringed upon that should defend their rights, which does not prevent the Office from protecting the public interest in other cases as well. The record fine of CZK 4.25 million imposed for unsolicited commercial communications is proof of this.

The Office for Personal Data Protection will continue to approach its tasks thusly in the future as well. It is the only way to continue to maintain harmony between fundamental human rights, among which number both the right to privacy and the right to protection of personal data, and rapid technological advancement. By that I mean the development of processing genetic and biometric personal data, artificial intelligence or monitoring systems, and the creation of new, technologically dependent personal data in generally enthusiastically received applications and services. It would be short-sighted to reject such systems across the board, just as it would be not to revise their form and use using appropriate criteria. In a globalised world with the universal spread of technologies based on the creation and utilisation of personal data, no other realistic possibility for protecting our privacy exists.

Dr. Ivana Janů
President of the Office for Personal Data Protection

Contents

The Office in numbers

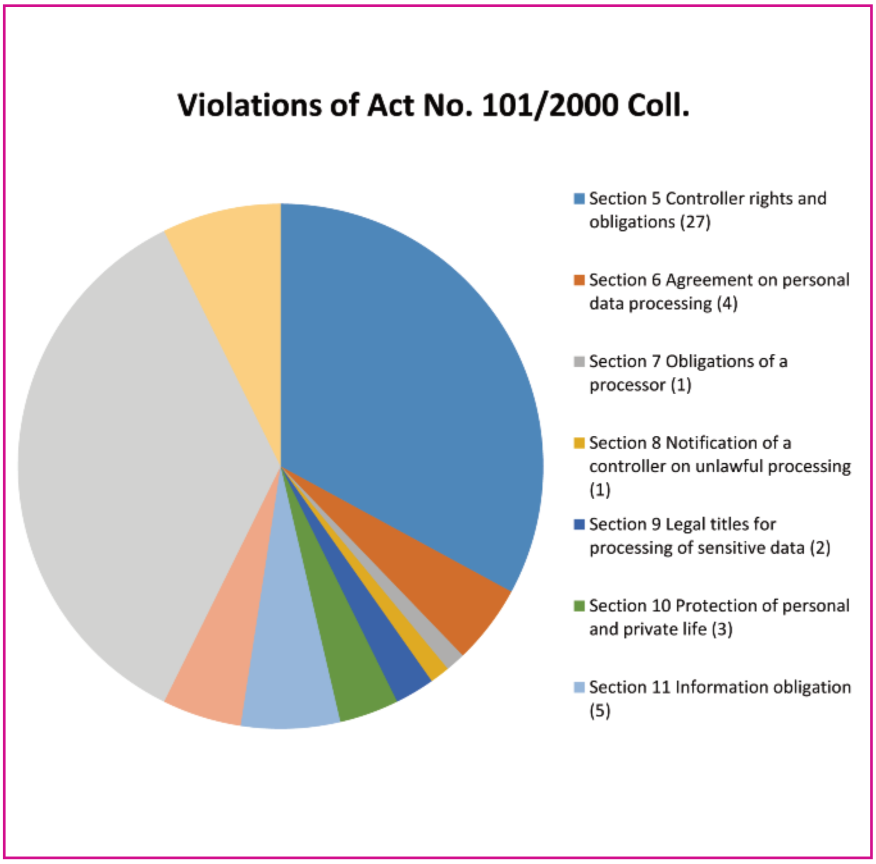
Questions and consultations	Czech Republic	2305
	international	28
	of those	
	private sector	1748
	public administration	557
Submissions and complaints	submissions received	1684
	of those information of controller about its responsibilities	254
	of those complaints passed on for inspection or administrative proceedings	152
Supervisory activities **excluding inspections** concerning Act No. 480/2004 Coll.)	commenced	100
	completed	110
	z toho z předchozích let	
	from previous years	41
	passed along to other state authorities	1
	corrective measures imposed	16
	contested by objections	18
	objections upheld	0
	rejected	12
	mostly upheld	1
	mostly rejected	3
	pre-inspection acts without subsequent commencement of inspection	27
Unsolicited commercial (communications (jurisdiction under No. 480/2004 Coll.)	total submissions	2710
	resolved	2218
	inspections commenced	19
	inspections completed	19
	from previous years	6
	sanction proceedings	18
	contested by objections	7
	objections upheld	0
	rejected	5
	mostly upheld	1

	mostly rejected	0
	pre-inspection acts without subsequent commencement of inspection	7
Administrative punishment	sanctions proceedings for violation of Act No. 101/2000 Coll. and No. 133/2000 with legal persons and natural persons engaged in business	50
	sanctions proceedings for violation of Act No. 101/2000 Coll. with natural persons	11
	waiving of fine under Section 40a of Act No. 101/2000 Coll.	34
Decisions on appeals	decisions contested by an appeal	25
	rejected appeals	16
	overturned and returned for new proceedings	3
	decision overturned and proceedings stopped	1
	change of decision	1
Judicial review (Note.: * *total since 2001*)	court actions submitted	2 (147*)
	actions rejected by court	11
	decisions overturned by court	3
	completed/uncompleted court proceedings since 2001	127/20
Registration	notifications received (under Section 16 of Act No. 101/2000 Coll.)	9241
	processing cases registered	9002
	still in proceedings	513
	registrations cancelled	156
	notifications on processing change	887
	proceedings under Section 17	31
	stopped (no violation of the law)stopped on procedural	23
	grounds (e.g. notification withdrawn)	2
	not permitted	1
Permits for transfer of personal data abroad	applications for transfer of personal data abroad received (under Section 27 of Act No. 101/2000 Coll.)	31
	decision to permit transfer	32
	decision not to permit	0
	proceedings halted on procedural grounds	2
Notifications under Act No. 127/2005 Coll.	notifications received	1
	resolved as justified	0
	resolved as unjustified0	

Complaints under Section 175 of the Administrative Procedure Code	complaints received	34
	vresolved as justified	4
	resolved as partially justified	7
	resolved as groundless	23
Requests under Act No. 106/1999 Coll.	requests received	30
	fully obliged	24
	partially rejected	3
	rejected applications	3
Published materials	Office Journal (number of issues)	1
Bills commented upon	acts	21
	implementing regulations	88
	draft government orders	16
	draft decrees	72
	other	48
	foreign materials	6

Supervisory activities of the Office

The Office's supervisory activities are conducted on the basis of a supervisory plan or at the initiative of tips and complaints (see Section 31 of Act No. 101/2000 Coll.); some inspections also take place at the initiative of the Office President.



• SUPERVISORY PLAN

The Office's Supervisory Plan is compiled in a similar manner each year. One part of the Supervisory Plan consists of inspections that can be termed obligatory and regular. These include inspections in terms of the Schengen Information System, Visa Information System, etc. In 2017 the Supervisory Plan included the processing of personal data under the domestic part of the Schengen Information System (SIS II). A regular inspection was also conducted of the legality of processing under the EURODAC system, which processes personal data of applicants for international shelter. From the perspective of the Czech legal code both these systems are information systems of Critical Information Infrastructure within the meaning of Act No. 181/2016 Coll., on Cyber Security and Amendments to Related Acts (the Cyber Security Act).

Another subject of the inspections carried out under the Supervisory Plan is the processing of personal data that are detected as potentially problematic at the level of European Union Member States as part of the WP29 Data Protection Working Party or the sub-groups thereof. An instance of this activity in 2017 was in particular the inspection of personal data processing during use of mobile applications by public administration bodies.

The creation of the Supervisory Plan is also influenced by prior inspections and the more general supervisory activity of the Office. It is in conducting supervisory activities that the Office often encounters phenomena that arouse the suspicion that personal data could be at risk of unauthorised processing in a whole sector, etc. An example of such an inspection included in the Supervisory Plan for 2017 were the checks on telephone operators focused on the security of customer personal data. It came to light that conducting such an inspection could be appropriate based on the discovered leak of customer data from T-Mobile Czech Republic a.s. that took place in 2016. Another example was the inspection of personal data processing by a recruitment agency, which was the result of checks performed based on complaints also received by the Office in 2016, which cast doubts on observance of obligations when processing the personal data of agency employees.

Another group of documents upon which the Supervisory Plan is based are submissions to the Office, which themselves are not a sufficient basis for launching an inspection, but it is evident from their overall number, for example, that it is an area of data processing that should be subjected to closer investigation or which is perceived by the public as problematic. Thus in 2017 inspections were conducted on the basis of the Supervisory Plan of, for example, an entity that requested data on the salaries and bonuses of its employees based on Act No. 106/1999 Coll., on Free Access to Information. The inspection focused on the further handling of the obtained personal data. Also included in the Supervisory Plan was an inspection of the operator of the debt register, which among other things was to focus on the transfer of data into this register and the use of birth numbers during its operation.

Once again in 2017 further planned inspections were added to the Supervisory Plan halfway through the year in reaction to current suspicions or doubts concerning personal data processing beginning to be conducted, in part on the basis of new legislation. A particular example in 2017 was the processing of personal data taking place on the basis of Act No. 112/2016 Coll., on Registration of Sales, including a separate inspection focused on the receipt lottery held according to Section 35 of the act in question.

In the following part of this annual report you can learn more on certain cases that were the subject of inspection based on the Supervisory Plan.

• FINDINGS OF INSPECTORS FROM SUPERVISORY ACTIVITY

Inspector František Bartoš

Collection of personal data via police camera systems

Based on a complaint and the Supervisory Plan, the Office conducted an inspection of the Police of the Czech Republic on the matter of observing the obligations of the controller and processor of personal data processed while using information collected via automated camera systems - section speed measurement, spot speed measurement, the LOOK System, strategic traffic detectors, weight-in-motion, red light violation detection, and toll inspection stations (gates) from the company Kapsch – hereinafter "section measurement".

The inspection was carried out at three regional directorates of the Police of the Czech Republic. As part of the conducted inspection, not only was the right of the Czech Police to collect personal data via the camera system in connection with section measurement checked, but also its subsequent processing.

The inspection found that the individual regional directorates of the Czech Police sign contracts with the operators of the automated camera systems, i.e. various municipalities and the Road and Motorway Directorate, on the basis of which information is automatically transferred to the operator of the individual technical devices and at the same time the Czech Police. This information concerns all vehicles regardless of whether a recording was made.

The basis for these automatic systems, which record all passing vehicles regardless of whether or not legal obligations are being violated (exceeding the speed limit, running a red light, overloaded vehicle, etc.) is photographs taken of the front of the vehicle and its licence plate. At the same time the camera system "reads" the vehicle's licence plate and consults the vehicle database. Photographs and recordings made are stored in the systems of the Czech Police for 6–12 months.

As part of the inspectors' authority an inspection was conducted of the use of this information with respect to the activities of the police, including a check of the rightfulness of access to the data. The internal control mechanisms of the Police set up to prevent misuse of the processed information were checked, also checking the security thereof.

The inspection found that the primary legal regulation according to which the Police of the Czech Republic proceeds in section measurement by a camera system with a recording device is Act No. 273/2008 Coll., on the Police of the Czech Republic, in particular the provisions of Sections 2, 60, 62 and 85. The processing of personal data in connection with section measurement is contained in Section 79a of Act No. 361/2000 Coll., on Road Traffic, which states that "in order to increase the safety of traffic on roads, the police and municipal police are entitled to measure the speed of vehicles". The general provisions of Section 2 of Act No. 273/2008 Coll. charge the Police of the Czech Republic with serving the public. Its mission is to protect the safety of persons and property and public order, to prevent crime, to fulfil the tasks of the

Criminal Code and other tasks in the field of domestic order and safety entrusted to it by law. It was also found that under *Section 60 (1) of Act No. 273/2008 Coll.* the Czech Police is authorised to process information in accordance with this law and other legislation, including personal data to the extent essential for performing its tasks, with paragraph 2 of the aforementioned provision stating the Czech Police must secure the processed information against unauthorised access, alteration, destruction, loss or theft, misuse or other unauthorised processing.

The inspection found and stated that the fundamental provision that allows the Czech Police to procure recordings is *Section 62 of Act No. 273/2008 Coll*. According to paragraph 1 of this provision, the police may, if it is essential for fulfilling its tasks, procure audio, visual or other recordings of persons or things found in publicly accessible places, and audio, visual or other recordings of the course of the act. According to para. 2, if permanent automatic technical systems are set up to procure the recordings under paragraph 1, the police shall make information on the establishing of such systems public in a suitable manner. This legal mandate of the Police of the Czech Republic represents what is called an official licence, which is essential for infringing on the personal rights of natural persons, and according to the provisions of Section 85 (1) of Act *No. 273/2008 Coll*. the Czech Police can do the following in connection with processing personal data to prevent, seek out or uncover crime and the punishment of crimes and securing the safety of the Czech Republic, public order and domestic safety: a) process vague or unverified personal data; if possible the police shall label such personal data as such, b) process personal data for a purpose other than that for which they were collected, c) collect person data openly and in secret or under the pretence of another purpose or activity, d) combine personal data acquired for various purposes in order to prevent, seek out, or uncover crime and the punishment of crimes and securing the safety of the Czech Republic, public order and domestic safety. According to para. 2 of the aforementioned provision, the Police of the Czech Republic shall process personal data under paragraph 1 separately from personal data processed for performing other police tasks. The Czech Police also deals with section measurement through internal regulations and agreements with entities outside the Police, which the inspectors duly verified.

Inspection of the company Partners Financial Services, a.s., in connection with brokering life insurance

The subject of inspection was compliance with the obligations of a personal data controller/processor laid down by Act No. 101/2000 Coll. in connection with the processing of personal data of natural persons, clients, in concluding contracts and brokering the conclusion of contracts in the field of insurance.

The complainant stated that in connection with the brokering of life insurance, they granted and signed consent to personal and sensitive data processing as part of the initial negotiations with the company Partners Financial Services, a.s. (hereinafter "Partners"), and not just to the insurance company but also the brokering company. During negotiations on the contract they passed along documents for the insurance company that had been filled out by their attending physician (medical questionnaire, lab results, medical record print-out) attesting to their state of health. Subsequently the insurance company ended up deciding to terminate the negotiations. Thus no contract was concluded. The complainant therefore revoked their consent to the processing of personal and sensitive data in writing and requested that the Partners brokering company return the documents containing information on their state of health and all sensitive data be destroyed. The inspected company Partners refused this request.

The inspection found that the contract had not been concluded and thereby the purpose of processing and storing sensitive data had passed. In the given case the party to the proceedings was obliged to terminate processing and storage of the complainant's medical documentation with sensitive data and demonstrably destroy the medical documentation within the meaning of Section 20 (1) of Act No. 101/2000 Coll. or return it to the complainant.

During the inspection, representatives of Partners argued that in this matter they proceed according to the instructions of the National Bank for the purposes of inspection in supervising the activities of insurance brokers, and that they are obliged to retain the documents pursuant to Act No. 253/2008 Coll. on Selected Measures against the Legitimisation of Proceeds of Crime and Financing of Terrorism, according to which they are obliged to retain all data obtained as part of identifying and checking the client (including sensitive data) for a period of ten years following the end of cooperation.

The inspection found that in connection with unauthorised retention of sensitive data on the complainant's state of health, the party to the proceedings violated Section 5 (1) d) of Act No. 101/2000 Coll., in which a personal data controller is obliged to only collect personal data for the intended purpose and in the scope necessary to fulfil such a purpose. With withdrawal of consent to sensitive data processing and failure to conclude a contract, the purpose of sensitive data processing disappeared, i.e. the performance of a life insurance contract. The party to the proceedings retained the complainant's sensitive data without a specifically defined purpose and without the knowledge of the personal and sensitive data processor, i.e. the relevant insurance company, and at the same time the inspected brokering company was not able to demonstrate the existence of the data subject's consent to personal and sensitive data processing within the meaning of Section 9 a) of Act No. 101/2000 Coll. after the complainant's consent was withdrawn.

The inspected company submitted objections against the inspection report, which were rejected in full. In the subsequent administrative proceedings it was ordered to destroy the complainant's personal and sensitive data and return the requested documents. The inspected company fulfilled this obligation. Misdemeanour proceedings will be held on the matter.

Inspector Jiřina Rippelová

Inspection in connection with processing of personal data of customers of Hornbach Baumarkt CS, s.r.o.

The subject of this inspection, launched on the basis of a submission received by the Office, was compliance with the obligations laid down by Act No. 101/2000 Coll. in connection with processing of customer personal data, in particular of customers suspected of theft or damaging of goods in hobby market locations. The means of processing such personal data was a camera system and then software for keeping track of the goods the detainees attempted to steal.

In relation to the camera system the inspection found that in the retail space selected for inspection the inspected entity operates a camera system consisting of several types of camera (tube, fixed and rotating), with all cameras allowing zooming. The specific focus of the cameras can be adjusted freely so as to suit the current needs of the inspected entity. The cameras monitor the interior of the shop as well as the outdoor area of the in and out roads by the terminal for issuing goods. The camera system was installed in order to protect the property of the inspected entity and is controlled and run by employees of the company providing security for the shop. In light of the fact that, based on the specific circumstances, the inspectors assessed that the camera system in question only infringes on rights protected under Act No. 101/2000 Coll. to an extent appropriate to the significance of the rights and interests of the inspected entity, in this case the legal entitlement for personal data processing under Section 5 (2) e) of Act No. 101/2000 Coll. can be applied. At the same time the fulfilment of the inspected entity's other obligations was also assessed, specifically informing about the operation of a camera system as per Section 11 of Act No. 101/2000 Coll. and ensuring the security of processed personal data under Section 13 of this Act. In both these aspects it was found that the inspected entity proceeds in accordance with the requirements of the provisions cited. In terms of the software for keeping track of goods the detained persons attempted to steal, the inspection found that the company providing security for the shop is obliged to use this software on the basis of contractual arrangements. Among other things, the software in question serves to keep track of the goods detained persons have attempted to steal (or damage), including records of the personal data of such persons. The inspection nevertheless found that in practice the personal data of detained persons are not kept on record and the software is merely used to keep track of goods whose theft was prevented, along with the identity of the security employee that intervened. In light of this finding the processing of personal data of detained persons (the inspection found only one specific case) was not assessed as a violation of Section 5 (2) of Act No. 101/2000 Coll., but as a violation of the obligation laid down in Section 13 (1) thereof, as the inspected entity did not adopt clearly defined measures to prevent the unauthorised or accidental processing of personal data.

Following this inspection the inspected entity adopted measures to rectify the errors found. In particular in light of this fact (and also taking into account the inspection found but one case), the imposition of sanctions was dropped.

Town of Černošice - inspection in connection with personal data processing via a camera system operated in classrooms

Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených v zákoně č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů prostřednictvím kamerového systému provozovaného v učebnách, v nichž probíhají zkoušky odborné způsobilosti žadatelů o řidičské oprávnění. Kontrolující konstatovali, že monitorování průběhu těchto zkoušek prostřednictvím kamerového systému se záznamem není zákonnou povinností kontrolované osoby a že mu nelze přiznat ani jiný právní titul dle § 5 odst. 2 zákona č. 101/2000 Sb. V daném případě není dán žádný zákonný ani jiný důvod hodnotit zkoušky vykonávané kontrolovaným jinak, než jakékoli jiné zkoušky odborné způsobilosti nebo zkoušky na akademické půdě (maturitní, vysokoškolské). Kontrolovaný tedy porušil povinnost stanovenou v § 5 odst. 2 zákona č. 101/2000 Sb.

V návaznosti na provedenou kontrolu byla kontrolované osobě uložena opatření k nápravě zjištěného stavu (tj. ukončení nezákonného zpracování osobních údajů). Sankce za uvedené jednání uložena nebyla, neboť s ohledem na informace, které měl Úřad k dispozici před registrací oznámení o tomto zpracování, bylo provedením registrace založeno legitimní očekávání města, že zpracování je v souladu s právem.

EURODAC - inspection conducted on the basis of the Office Supervisory Plan

The inspection was conducted on the basis of the Supervisory Plan of the Office and the obligations that follow from Regulation of the European Parliament and of the Council No. 603/2013 of 26 June 2013 on the establishment of EURODAC.

The Czech Republic has been a member state of the EURODAC system since 2004, with the processing of personal data in this system by the competent authorities being directly governed by Regulation No. 603/2013. The architecture of the EURODAC system is described in Art. 3 of Regulation No. 603/2013 Coll., according to which this system consists of a central fingerprint database and the communication infrastructure between the Central System and Member States (in the form of an encrypted virtual network dedicated to EURODAC data). Another part of this system are the National Access Points in the various Member States. The EURODAC system processes the personal data of applicants for international asylum (i.e. third-country nationals or stateless persons who have submitted a request for international asylum) as well as third-country nationals or stateless persons detained by the competent authorities in connection with illegal border-crossing of a Member State. For both categories a further condition for personal data processing is age – they must be persons over 14 years in age. Also assigned to the fingerprints are information on the Member State that entered the prints into the system, the date they were taken, the date and place the asylum request was submitted, the sex of the applicant and any other potential information concerning their arrival or departure to or from Member State territory, or the date of a decision on their application. The personal data of asylum applicants are retained in the EURODAC Central System for a period of ten years from the taking of fingerprints and then automatically erased; for persons detained while illegally crossing the external borders of the Member States, this period is 18 months. In accordance with Regulation No. 603/2013, fingerprints entered into the EURODAC system may only be used to compare with fingerprints of third-country nationals or stateless persons that are residing illegally within a certain Member State in order to check whether such a person has already submitted an asylum request in another Member State. The controller of the personal data processed by the competent authorities of the Czech Republic in the EURODAC system is the Czech Interior Ministry's Asylum and Migration Policy Department (OAMP). OAMP's tasks consist primarily of coordinating activities and methodological guidance, as well as communicating with other Member States in assessing specific cases. Units of the Police of the Czech Republic also have access to personal data processing in EURODAC (in particular the Foreign Police Directorate, the Foreign Police departments of the individual Regional Directorates, and the Prague Criminology Institute). The role of the Prague Criminology Institute in relation to the EURODAC system consists mainly of entering data into this system if the fingerprints were not taken in electronic form but with fingerprinting ink, as well as to verify matches when checking fingerprint data against EURODAC. The Foreign Police has the position of a depositor workplace in personal data processing in EURODAC, thus it is not authorised to alter or amend the entered data.

The inspection checked the practices of OAMP, Prague Criminology Institute and the Foreign Police at the Foreigners Reception Centre Zastávka, including assessing measures adopted to ensure the security of the personal data processed in EURODAC; no violation of the obligations arising from Regulation No. 603/213 and subsidiarily from Act No. 101/2000 Coll. was found.

Inspector Jana Rybínová

Inspection of information system of company Falck Emergency, a.s.

The complainant notified the Office that even three months after terminating employment with the company Falck Emergency a.s. (hereinafter the "Company"), which provides medical transport services, they still had electronic access to the Company's information system ("FOS") through their mobile telephone, specifically to the plan for transport of patients.

The inspection found that over the course of 2017 six employees terminated employment at the Company at the position of driver, with five of the employees having access to the FOS withdrawn as of the day their employment ended, while one employee only had access blocked more than 4 months after employment ended, and it was found that they continued to have access to personal and sensitive data of transported patients. According to the Company, this was caused by a technical shortcoming of version 5.1.1 of the Android operating system being used for the FOS information system, which allowed a user's password to be changed without knowing the original password. The employee utilised their knowledge of their user name for direct access to FOS and due to this error they changed their password, thereby acquiring access to FOS from their own device (mobile phone) without having to use the Company's protected tablet. The employee did not inform the employer of this fact. It was also found that FOS allows a check of activity on the Company's mail account to be performed, revealing what kind of access was used, from what IP address and on what date or time. The submitted summary showed that on 18 July 2017, the FOS system was accessed from a mobile device from an IP address that was not one used by the Company.

By allowing unauthorised access to personal and sensitive patient data processed in FOS in the period from 5 April to 10 August 2017 to a person that was no longer employed with the Company, the Company did not have sufficient control mechanisms in place to prevent unauthorised access to personal or sensitive data, thus it did not sufficiently assess the risks within the meaning of Section 13 (3) c) of Act No. 101/2000 Coll., thereby violating the provisions of Section 13 (1) of Act No. 101/2000 Coll. During the inspection the Company stated that it can responsibly declare that it was a completely exceptional case, and a repeat check of all access rights did not find any other similar failure.

During the inspection the Company rectified this violation by blocking the former employee's access, furthermore introducing automatic notification for the IT specialist of every password change and every access to FOS from a foreign device. The current user name and password are always known solely by the IT specialist and the operating manager that assigns them and checks they are up-to-date quarterly.

Administrative proceedings imposing measures to rectify the identified shortcomings as per Section 40 of Act No. 101/2000 Coll. were not held with the Company, as it rectified the situation during the inspection. In the follow-up administrative proceedings a fine of CZK 8000 was issued for an administrative offence.

Identity management system at University of South Bohemia in České Budějovice

The inspection of University of South Bohemia in České Budějovice (hereinafter the "University") was launched on the basis of the Office's Supervisory Plan for 2017 and the authorisation of Section 33 (3) of Act No. 101/2000 Coll. The inspection focused on the scope of data processed, the securing thereof to the extent required under Section 13 of Act No. 101/2000 Coll., the obligation to inform data subjects and the duration of retention in the university's identity management systems, transferring of data to third parties and fulfilling of obligations under Section 6 of Act No. 101/2000 Coll.

The inspection found that the University operates an identity management system ("IdM") which is based on a central repository in which the user's identity is stored, i.e. a unique identification of a natural person and their assigned user role. In the university environment this thus includes students, teachers and other University employees. Aside from access to the information systems ("IS"), the user role also precisely determines the extent of access privileges (authorisations) in the given IS.

Only those user data that are essential for using the IS functions are transferred to the given IS from the central repository. The authorised user-administrator then assigns and modifies the privileges of "regular" users from one place, e.g. when their job class changes, when a teacher moves to a different faculty, a student changes majors, etc. The ISs are synchronised to the state of the central repository. The identity management systems can also control other technical features, e.g. managing access to certain buildings/spaces. The identity management system serves to manage the life cycle of identities at the university and to transfer data on identities to other components of the University's information system.

As of 2 June 2017, 71 094 identities were stored in the IdM system, of those 12 292 active. The period of retention of non-active identities was set at 45 years for both employees (the personal files of managers and other employees) and students (the personal files of students).

Over the course of the inspection the University carried out an analysis of identities being revived due to registration of returning students or employees. Based on the analysis conducted, the University stated that using the statistics it will set the duration for retaining non-active identities to seven years. Identities shall be erased seven years after the termination of a legal relationship to the University; for non-active identities kept in the IdM, only the essential information will be retained (name, surname, user name, ID number, personal number from source agendas, e-mail), and shall be pseudonymised. The University also stated that if a data subject requests provision of a service from it even after the legal relationship has ended, their personal data shall be retained in the IdM after provision of consent by the data subject in question.

The University, as the controller of the person data of students, employees and attendees of lifelong learning processed in the Identity Management System, violated the provisions of Section 5 (1) e) of Act No. 101/2000 Coll., as it set the period for retaining the personal data of students, employees and attendees of lifelong learning in the IdM system - or rather the period of non-active identities - to 45 years. Such a period of retention is not essential for the purpose of their processing, which is administering the life cycle of identities and passing on identity data to the other components of the University's information system.

Without commencing proceedings, the Office put aside the matter within the meaning of Section 40a of Act No. 101/2000 Coll. because the University remedied the unlawful situation immediately after the breach of duty was detected. Additionally, in light of the fact that retention period of 45 years originally set by the University in processing personal data in the IdM system was not fully used, it refrained from imposing a fine as per Section 40a of Act No. 101/2000 Coll.

Right to be forgotten - Google Czech Republic, s.r.o.

At the initiative of a data subject whose data was being processed through internet links and who asked for their removal, thereby bringing to bear their "right to be forgotten", the Office inspector conducted an investigation of the complaint and in the sense of Section 3 of the Act on Inspection No. 255/2012 Coll. called for access to the specified URL addresses via the Google search engine to be blocked, specifically the company Google Czech Republic, s.r.o. The Office inspector backed the call for blockage with a statement that the complainant has a court decision, a copy of which is part of the file material on the matter, on the basis of which the print media apologised for the false information on their private life published in articles in these media and which are also contained in some of the articles published via these URLs.

The Office inspector subsequently received a response from Google Czech Republic, s.r.o. with the information that the request for blocking of access had been passed along to Google Inc., of registered office 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, adding that the Office should send the request directly to Google Inc., which is the owner, operator and provider of the Google search engine.

The Office inspector sent an identical call for blocking of access to the specified URL addresses to Google Inc. Subsequently the Office received information from Google Inc. that the searching and display of the given websites had been blocked in the Google search engine. In checking the measures taken, the inspectors found that at a URL which was not specified in the original request the complainant's personal data are also being published, thus an additional call for blocking of the stated URL was sent to Google Inc.

Inspector Božena Čajková

Inspection of monitoring and subsequent processing of recordings made while serving for the Hradec Králové Municipal Police

The inspection was commenced on the basis of the Office's Supervisory Plan for 2017 and its subject was the fulfilling of obligations laid down by Act No. 101/2000 Coll. in connection with monitoring and subsequent processing of recordings made while municipal police officers are serving. Municipal police officers make video recordings of some of their operations based on Section 24b (1) of Act No. 553/1991 Coll., on Municipal Police. They then save these recordings on the municipal police data repository. They also pass along certain of these recordings to the authorities active in criminal proceedings for further use, or to other competent authorities for administrative proceedings. Some video recordings of municipal police operations are also made available to citizens via the media. The municipal police modifies (anonymises) video recordings intended for the media before handing it over so that the persons captured therein are not recognisable. Assessed in the inspection were two specific recordings made during municipal police acts and published on the internet, in which as a result of insufficient anonymisation, or rather provision of additional information (personal data), it was possible to come to the conclusion that even in the form in which they were published on the internet they contained personal data of the data subjects against whom the officers' operation was targeted.

V In the case of these video recordings, the procedures adopted for anonymising video recordings were thus not observed, resulting in infringement on the rights of the persons captured on those recordings. The municipal police thus acted at odds with the requirements of Section 13 (1) Act No. 101/2000 Coll. The inspection also found that the municipal police does not keep a summary of what recordings have been published or made accessible and to which parties. After transferring or providing access to the recordings it thus lose the ability to verify whether the published recording was truly made by municipal police officers and did not undergo unauthorised manipulation or have information added from other sources. This approach was evaluated as a violation of Section 13 (3) d) of Act No. 101/2000 Coll.

Following this inspection the municipal police carried out measures to rectify the shortcomings found. Subsequently a sanction of CZK 30 000 was imposed for the above actions.

Processing of personal data on the website of the company FORDESK, s.r.o.

The subject of the inspection, which was launched on the basis of a complaint, was the processing of personal data in connection with a service the inspected party provides via its website www.firmo.cz, and which consists of the provision of clear and comprehensive information about legal persons and natural persons engaged in business.

In providing the above services, the inspected entity collects freely available information from public registers (open data) on businesses, compiles it and provides further access at www.firmo.cz. The inspected entity's actions are thus generally in compliance with Section 5 (2) d) of Act No. 101/2000 Coll. In the case of information taken from the trade register however, it is necessary to take into account that under Section 60 (3) b) of the Act on Trade Licensing No. 455/1991 Coll., after 4 years of the termination of an entrepreneur's last trade licence, the information on the entrepreneur passes from the public part of this register to the non-public part. Following this move, the given personal data can no longer be considered data lawfully published due to their nature and the application of Section 5 (2) d) of Act No. 101/2000 Coll. is no longer possible. Thus the inspected entity does not have any legal entitlement to such personal data. The inspection also checked whether the inspected person had adopted measures relating to the legal restrictions on the public nature of data arising from Section 60 (3) b) of Act No. 455/1991 Coll. and came to the conclusion that the measures adopted by the inspected entity do not ensure the desired state, i.e. true updating of the processed personal data and erasure of those that are no longer publicly available. The inspected entity thereby breached the obligation laid down under Section 13 (1) of Act No. 101/2000 Coll. The inspected entity also violated the obligation under Section 21 (2) of Act No. 101/2000 Coll., as it did not erase the complainant's personal data on the basis of their request, even though at the time of the request the complainant's personal data were no longer publicly available.

Following up on this inspection, measures were ordered for the inspected entity to remedy the shortcomings found. The company was subsequently fined in the amount of CZK 30 000.

Inspection of security and access to recordings from camera system operated in building of the Ohradní housing cooperative

The inspection was launched on the basis of a submission, the subject of which was the handling of recordings from a camera system operated in a residential building.

The inspection found that the inspected entity was operating a camera system with recording in a residential building that it owns (the cameras monitor the main and rear entrances to the building, entrance hall with mailboxes, area in front of the lifts and the lift cabin). The cameras placed by the main entrance also monitor the public space in front of the building (parking lot). With regard for the scope and focus of the camera system (individual cameras), and taking under advisement the purpose of their operation, the inspectors came to the conclusion that, with the exception of the cameras monitoring the parking lot, the legal entitlement expressed under Section 5 (2) e) of Act No. 101/2000 Coll. can be applied. In terms of the cameras monitoring the parking lot it was found that the obligations under Section 5 (2) of Act No. 101/2000 Coll. had been violated, as no legally anticipated entitlement to process personal data was found. No other violation of the obligations under Act No. 101/2000 Coll. were found by the inspection, not even in relation to the subject of the complainant's submission (unlawful handling of recordings).

Following this inspection the inspected entity took measures to remedy the detected situation. A sanction of CZK 5000 was imposed on the housing cooperative for the above actions.

Inspector Petr Krejčí

Inspection of the company Čedok, a.s. based on the Office's supervisory plan

The Office for Personal Data Protection carried out and completed an inspection of the company Čedok a.s., of registered office Na Příkopě 857/18, Nové Město, 110 00 Prague 1, Reg. No.: 60192755 (hereinafter the "inspected entity").

This inspection was carried out on the basis of the Office's Supervisory Plan for 2017. The subject of the inspection was compliance with the obligations of a controller/processor of personal data stipulated by Act No. 101/2000 Coll., on Personal Data Protection and Amending Certain Acts, in connection with processing the personal data of the inspected entity's clients obtained on the basis of a Package Tour Agreement or Agreement on Provision of Individual Services, including the related handling of visa applications and transferring personal data to the authorised processor, guide, delegate or other person authorised to provide tourism services to selected specific third countries that are not Member States of the European Union, i.e. outside the boundaries of the Schengen Area. The objective of the inspection was primarily to check compliance with the obligations laid down for controllers and processors by Act No. 101/2000 Coll. when transferring personal data of data subjects to those third countries that are not Member States of the European Union and to which the prohibition does not apply limiting free movement of personal data stemming from an international treaty Parliament has agreed to ratify and by which the Czech Republic is bound, and to third countries to which data are not transferred based on a decision by a body of the European Union, i.e. to those third countries to which data can be transferred under the provisions of Section 27 (4) of Act no. 101/2000 Coll., but only if the OPDP issues a permit for such transfer. Of these third countries, Russia and Turkey were selected. As it was an inspection conducted according to the provisions of Section 31 of Act No. 101/2000 Coll., on the basis of the Supervisory Plan, it checked the compliance of the inspected entity with regard to the aforementioned subject of inspection with all provisions of Act No. 101/2000 Coll. in which obligations of a controller/processor are stipulated.

The inspected entity laid out the purposes for which the personal data were to be processed, which were processing of customer personal data in order to conclude and perform a Guided

Tour Agreement, Agreement on Provision of Individual Services, Agreement on Čedok Club Membership concerning the loyalty system in order to provide loyalty discounts and offer Čedok service to faithful customers, guided tour participants or participants in individual services provided to them and third parties in whose favour any of the contracts concluded with the customer and the inspected entity are, and for the purpose of offering trade or services to the data subject, which according to the provisions of Section 4 d) of Act No. 101/2000 Coll. are natural persons to whom the personal data apply, which the travel agency Čedok a.s. has listed in its General Terms and Conditions, which are an integral part of such contracts, are published by the inspected entity on its website and are also contained in the inspected entity's tour catalogue. The inspected entity transfers personal data to the selected third countries according to the permits issued to it for their transfer to those countries by the Office for Personal Data Protection.

The inspection conducted found that while processing person data of the data subjects for the relevant purposes, the inspected entity observes the obligations laid down for it within the meaning of Section 4 j) of Act No. 101/2000 Coll., and thus no violation of the Act on Personal Data Protection was determined.

Inspection of compliance with obligations of personal data controller/processor at company INDEX NOSLUŠ, s.r.o.

The Office for Personal Data Protection carried out and completed an inspection of the company INDEX NOSLUŠ s.r.o., of registered office Hornokrčská 583/30, Krč, 140 00 Prague 4, Reg. No.: 25131419 (hereinafter the "inspected entity").

The subject of the inspection was compliance with obligations of a controller/processor of personal data laid down by Act No. 101/2000 Coll., on Personal Data Protection and Amending Certain Acts, in connection with the processing of personal data that were not duly destroyed in accordance with the purpose of their collection as per the provisions of Section 4 i) and Section 20 of Act No. 101/2000 Coll., with the materials containing these personal data being found by the Municipal Police of the City of Slaný in a publicly accessible spot.

Included when the Slaný Municipal Police handed the matter over to the Office was a large amount of papers, particularly employment and tax documents, as well as registration contracts, work agreements, confirmations on school attendance and income tax declarations for employed activity and functional benefits, containing the personal data of agency employees of the inspected entity from the years 1999-2003 in connection with the inspected entity's activity as a labour agency performed on the basis of a permit issued by the Ministry of Labour and Social Affairs. The inspection found that the documents totalled 177 files containing, in individual translucent plastic document sleeves (A4 format) separate for each data subject, several documents for the given time period containing in sum the personal data of name, surname, date of birth, birth number, ID card number, nationality, permanent address, temporary address, telephone contact, e-mail address, name and address of health insurer, state of health, health restrictions, health care, name of school, name of faculty, year, address of school, confirmation of studies, job knowledge/experience/skills. In these sets of documents the personal data of some data subjects were listed more than once, but with personal data filled out for differing periods of arranged employment, thus the documents had the personal data of a total of 136 data subjects. The inspectors found that the collection of personal data by the inspected entity was justified, including in terms of the scope in accordance with the purpose of processing.

In light of the fact that the inspected entity did not secure the processed data of its agency employees against unauthorised access and that they were found in a publicly accessible spot, it failed to ensure their due destruction, thereby violating the provisions of Section 13 (1) of Act No. 101/2000 Coll., on Personal Data Protection, which obliges a controller and processor to adopt measures to prevent unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data. This obligation remains valid even after termination of personal data processing. It furthermore violated the provisions of Section 20 (1) of this act, which lays down the obligation for a controller or, on the basis of its instructions the processor, to destroy personal data as soon as the purpose for which the personal data were processed ceases to exist, for which the inspected entity was fined CZK 30 000 in administrative proceedings.

Inspection based on objection installation of camera system in locker room area at company Novoměstské služby, s.r.o.

The Office for Personal Data Protection conducted and concluded an inspection on the basis of a complaint of the company Novoměstské služby s.r.o., of registered office Soškova 1346, 592 31 Nové Město na Moravě, Reg. No.: 03022641, (hereinafter the "inspected entity"), which is the operator of the City Spa in Nové Město na Moravě, the owner of which is the city of Nové Město na Moravě. The essence of the complaint from a visitor to the City Spa was an objection against the installation of a large number of cameras which are to use a camera system with recording to monitor the area of the locker rooms for changing clothes, including the lockers, hallways, benches, etc., with these spaces not being labelled with information signs, thus it is not evident which parts of the locker rooms are monitored by the cameras, and thus the submitter was of the opinion that these cameras, which also capture people getting changed, including naked underage children, violate the Act on Personal Data Protection.

The subject of the inspection was compliance with the obligations of a personal data controller/processor laid down by Act No. 101/2000 Coll., on Personal Data Protection and Amending Certain Acts, in connection with the processing of personal data of data subjects obtained from an installed camera system with recording via cameras placed in particular in the area of the locker rooms and places designated for visitors to the City Spa In Nové Město na Moravě to get changed.

The inspection found that the inspected entity operates a camera system with visual recordings in the City Spa of Nové Město na Moravě in order to protect the life, health and property of visitors and employees of this spa, as well as the property of the inspected entity. The changing stalls and lockers are distinguished by colour so that it is evident based on the installed signs which spaces are monitored by the cameras, thus the cameras of the camera system with visual recording operated by the inspected entity do not monitor, and do not record, the area of the changing stalls intended for visitors to the City Spa of Nové Město na Moravě to get changed. The cameras of this camera system with visual recording monitor, and thus record, only the spaces for storing and leaving items, i.e. the cloakroom and lockers for storing personal items of the visitors to the Nové Město na Moravě City Spa. The changing stalls are labelled with signs containing the text "changing stall" with instructions for visitors. The "City Spa Visiting Rules", placed on the board for visitors to the Nové Město na Moravě City Spa, set out the obligation for visitors to get changed in the changing stalls, to place all their personal items in a selected locker in the locker room, lock the locker with the chip bracelet issued to them upon entry to the spa, and to wear this chip bracelet on them in a visible spot, for example on their wrist, for the whole duration of their visit to the Nové Město na Moravě City Spa premises. Should then a visitor to the Nové Město na Moravě City Spa get changed in range of the cameras of the camera system with visual recording even though the space in the changing stalls not monitored by the cameras is reserved for such, they would have thereby violated the "City Spa Visiting Rules", in which the place designated for getting changed is set out, and the inspected entity can thus not be blamed, i.e. it cannot be considered a violation of the law, if persons getting changed in areas not intended for it are monitored. As only authorised persons have access to recordings from the camera system and only in exceptional circumstances, any monitoring of spa visitors can be ruled out.

In the given case no violation of the Personal Data Protection Act was found.

Inspector Daniel Rovan

Inspection of brokerage company 4LifeFinance, s.r.o. which brokers financial services

The Office conducted and completed an inspection initiated by a complainant, who stated in the complaint that they attended a meeting at the inspected company's registered office in order to review their insurance contracts. During this meeting it was to have emerged that those attending the meeting on behalf of the inspected company had at their disposal the complainant's name, telephone number, information that they were insured and with whom, as well as information on when the insurance was to expire, all without the complainant being its client. The company also had the same information about the complainant's wife. At the site of the meeting the complainant demanded the source of these personal data be revealed, which was allegedly promised.

During the inspection the inspected entity produced a Cooperation Agreement concluded with a brokerage company, the subject of which was power of attorney from a financial advisor to act on its behalf to handle its affairs according to the instructions of the client. This activity means primarily the brokering of sale of financial products of institutions contractually tied to the client. For this activity the advisor is entitled to use the client's know-how and its internal information system.

The contract includes a commitment of the financial advisor that it will act as a processor of personal data of the data subjects with a contractual relationship to the company, or data subjects with an interest in financial products of the financial institutions contractually bound to the company. It is also stated that the financial advisor undertakes that it will provide a client that so requests with information on the personal data the company processes about them in the internal information system within the meaning of Section 12 of Act No. 101/2000 Coll., on Personal Data Protection (i.e. in particular on the purpose of processing, the personal data about the client processed, the recipients of personal data) and that the Contract meets the requirements of an agreement on personal data processing within the meaning of Section 6 of Act No. 101/2000 Coll., on Personal Data Protection.

It also followed from the internal regulations that the advisor may not collect client personal data before acquiring from the client or potential client consent to processing thereof electronically or in writing.

The inspection checked the obligations following from the wording of Section 6, as it followed from the inspection findings that the inspected company is a processor on the basis of a contract concluded with the controller of the complainant's personal data, as well as the obligations under Section 12 (1)-(4).

The inspection found a violation of Section 12 (2) b) of Act No. 101/2000 Coll., as it follows from both the paragraph in question and from the cooperation agreement between the inspected entity and the partner company acting as personal data controller that there is an obligation to provide the client with information on the personal data the company processes in its IIS (internal information system), which the inspected entity did not sufficiently do.

In light of the fact that the inspected entity rectified the objectionable situation immediately following the inspection, no administrative proceedings on corrective measures were launched. The imposition of a fine was also dropped because it was a completely isolated case.

Based on the Office's experience in this field, this is a very frequent practice of providers of this type of service and the aforementioned controller has managed to build up a relatively extensive network of processor partner companies. For this reason an inspection of this brokerage company has been included in the Supervisory Plan for 2018.

Inspection of primary school in Trutnov in connection with creating electronic addresses in a format that contained student personal data allowing their identification

Based on a complaint, the Office conducted and completed an inspection of one of the primary schools in Trutnov. The complainant states in their complaint that the fourth-grade students were to have had e-mail addresses set up using the Google Suite service without the consent or informing of their legal guardians. The e-mail addresses were created in the format name.surname@school domain. According to the complaint, with the opening of these e-mail accounts, Google was to have been provided with student personal data of at least the name, surname and school the student was attending.

In the inspection it was founded that after the inspected entity was notified by the complainant, the school also informed the other legal guardians of pupils about their actions in processing personal data. The school also stated that the establishing of student internet addresses is necessary to fulfil the requirements of the General Curriculum Programme. According to a statement from the Ministry of Education, Youth and Sport on the complaint, the objective of the General Curriculum Programme (GCP) is for pupils to be able to safely work in an electronic mail environment and recognise possible risks so as to not endanger themselves or others. If the use of student personal data is required to set up mailboxes, one must proceed in accordance with the legislation on personal data protection. Thus neither the General Plan or the Ministry force schools to have a specific form for e-mail addresses, in contrast drawing attention to the necessity to comply with personal data protection obligations.

The school submitted an internal document *Directive on Personal Data Protection*, governing the rules for protecting the personal data of employees, school pupils and also persons in another labour law relationship with the school. Among other things this directive states that for personal data processing beyond the scope laid out by the legal regulations, the consent of the person whose data are being processed is required. Before commencing personal data processing, the organisation must demonstrably make sure such persons are fully informed in the scope laid down by Act No. 101/2000 Coll., on Personal Data Protection, as amended, and instructed as to their rights. It is to ensure instruction on the obligation to maintain confidentiality about personal data and security measures, which if made public would endanger the security of personal data, even after the employment or relevant work has ended. Consent is signed on behalf of pupils by their legal guardians. The "general consent" used does not however list the service G Suite for Education among the purposes of processing.

The inspected entity furthermore stated that it has an on-line contract with Google Inc., solely and exclusively for the G Suite for Education service. Pupils do not have access to other services where their personal data is required, and if they attempt to access them, their account is automatically blocked. Under G Suite for Education, the inspected entity had restrictions in place on access to G+ social network services. In setting up the accounts, a csv table is imported under the Google Suite administration with three columns: name, surname, default password. During the pupil's first login, the account asks for a password of at least eight characters, which the student chooses. At the same time the student is informed by the system about the conditions of setting up the e-mail account, which they must accept. Only the network administrators have access to the administration, and they are employees of the school. They have the power to block individual accounts, change passwords, or delete accounts. Once the pupil stops attending the school, their e-mail account is deleted.

A standard guarantee of protection for users against unauthorised access follows from the contract with Google Inc. Google's liability does not apply to internal management or administration of services provided to the customer; Google is merely the data processor. Under the point Representations, Warranties and Disclaimers it is stated, among other things, that the customer agrees that it is liable for obtaining parental consent with collection of the pupils' personal data to be used in connection with the provision or use of services by the customer or end users; end users are defined as the individual the customer allows to use the services. It does not follow from the submitted text that the addresses must be made using the students' names.

The inspection particularly checked the obligations stemming from Section 5 (1) d), Section 5 (2), Section 6 and Section 11 (1) and (2) of Act No. 101/2000 Coll. According to the inspection findings, for identifying the end user (pupil) in the G Suite for Education service the inspected school uses their name and surname. Using these it creates an account for the end user (pupil). As it is not essential to use the pupil's name and surname and they can be identified with a less invasive infringement of their privacy, it thereby violated Section 5 (1) d) of Act No. 101/2000 Coll. It was also found that the school did not have the consent of the pupils' legal guardians to process their personal data for this purpose, thus it thereby violated Section 5 (2) of Act No. 101/2000 Coll. It also follows from the inspection findings that as a personal data controller it failed to inform the legal guardians of the data subjects of the scope and for what purpose the personal data are to be processed, who will process the personal data and in what manner, and to whom access may be provided to the personal data, thereby violating Section 11 (1) of Act No. 101/2000 Coll. From the further inspection findings it was evident that the school was utilising a "general consent", which is submitted to the legal guardians of children for signature; by signing the parent grants consent to a range of processing of the child's personal data, and they are asked for consent even in cases where such personal data processing is laid down by the law. The affected parent to whom the inspected entity claimed that the processing of their child's personal data is taking place on the basis of consent thus had improper information about the processing of the child's personal data, and from the perspective of the inspected entity this is untruthful and thus insufficient fulfilment of the obligation to inform when collecting the personal data of pupils. Thus was Section 11 (2) of Act No. 101/2000 Coll. violated.

In light of the fact that the inspected entity took extraordinary efforts to remedy the objectionable situation immediately following the inspection, no administrative proceedings on corrective measures were launched.

Inspection of personal data processing by a company creating a database and trading in such at the company SOLIDIS, s.r.o.

On the basis of repeated complaints, the Office conducted and completed an inspection of a company that trades in databases, SOLIDIS, s.r.o., that focused on compliance with obligations laid down by Act No. 101/2000 Coll. in connection with the processing of personal data in databases and offering them to third parties, and observing the obligations arising from Act No. 480/2004 Coll., on Certain Information Society Services, in connection with the sending of commercial communications by electronic means.

The complainants repeatedly referred to the fact that they were contacted by telephone by operators offering various goods or services. When questioned as to where they acquired their personal information from, the callers generally provided a standard prepared response from which it was evident that their personal data had been purchased from a vaguely specified personal data controller, and this controller had guaranteed they were acquired in accordance with the law. The most frequently provided source was the company SOLIDIS.

The Office conducted its last inspection at SOLIDIS, s.r.o. in 2013. The inspection focused on compliance with obligations laid down by Act No. 101/2000 Coll. in connection with the processing of personal data in databases and offering them to third parties, and observing the obligations arising from Act No. 480/2004 Coll., on Certain Information Society Services, in connection with the sending of commercial communications by electronic means. The inspection found violation of the obligations under Section 7 (2) and (4) c) of Act No. 480/2004 Coll.

SOLIDIS numbers among one of most frequently mentioned controllers that provide customers with "tailormade" databases. The inspection focused primarily on the transferability of the consent of data subjects to processing of their personal data and the informing of subjects of their transfer to third parties.

The inspection findings showed that the inspected entity obtains personal data predominantly from publicly available sources, or acquires access to them on the basis of controller authorisation. To a limited extent the data are acquired on the basis of licensing agreements in which the provider declares that it is processing in accordance with the Personal Data Protection Act and they can be processed for the purpose declared in the agreement. The inspected entity provided copies of three licensing agreement under Section 90 et seq. of At No. 121/2000 Coll., the Copyright Act.

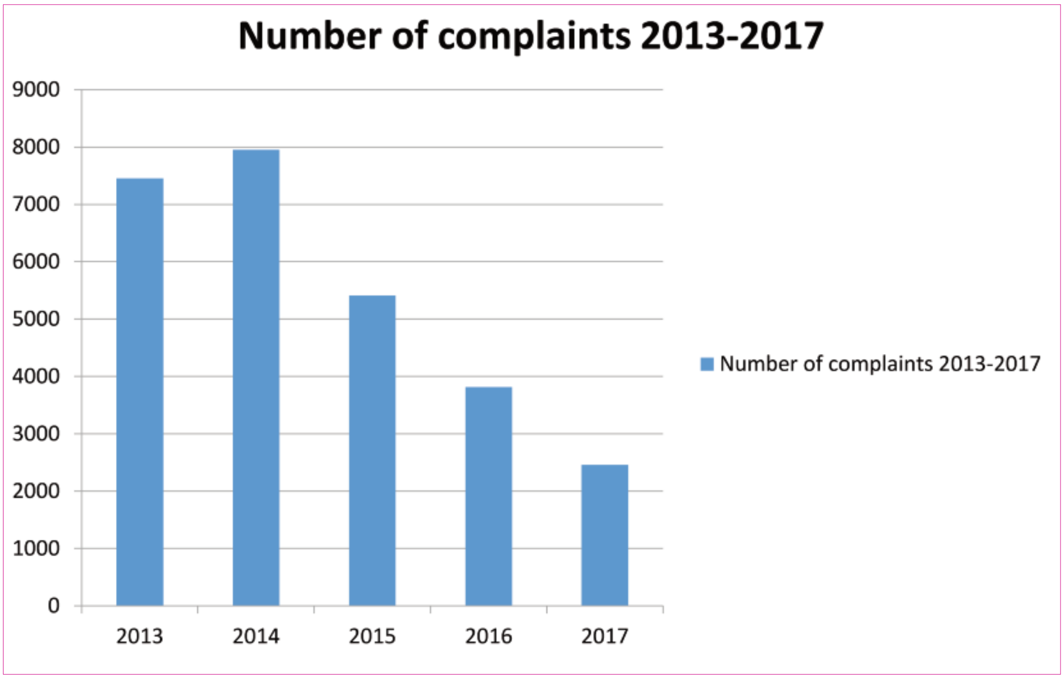
The inspected entity also submitted a blank order form which stated, inter alia, that the inspected entity provides services consisting of processing of personal data according to the specifications of the order. The purpose and scope of personal data is stated in the specifications of the order. If output is arrange, this is provided electronically in xls format. The client declares that it is acquainted with the Provider's General Terms and Conditions, which are provided on the reverse side of the order form, and that it consents to the arrangements listed there. These specify the term "service" as *including but not limited to surveys, creation of special databases, ..., with the services also able to include personal data processing*. Part of the services may be the processing of personal data. The company carries out personal data processing with its own employees.

The inspection primarily checked the obligations arising from the wording of Section 5 (1) a) and b), Section 5 (2), (5), (7) and Section 12 (1)-(4) of Act No. 101/2000 Coll. The inspection results showed that the inspected entity purchased a database of data subjects from a different controller, including declared consent to processing thereof. Since the consents of the data subjects listed in the database of one controller and provided to another controller cannot automatically be considered consent to personal data processing, Section 5 (2) was violated. As the inspected entity utilised these personal data to contact and send out commercial communications, additionally providing them to further controllers without the consent of the data subjects, it violated Section 5 (5) and (7) of Act No. 101/2000 Coll. The inspection findings also showed that the inspected entity, despite repeated requests by the data subjects (complainants), did not provide complete information on the scope of processing and source of personal data, thus failing to meet its obligation under Section 12 (2) b) of Act. No. 101/2000 Coll.

Remedial measures were ordered against the inspected entity by administrative injunction. SOLIDIS fulfilled these corrective measures by the stipulated deadline. Based on the inspection findings, misdemeanour proceedings are underway against the company.

Inspector Josef Vacula

UNSOLICITED COMMERCIAL COMMUNICATIONS



It is evident from the above graph that the number of complaints received against unsolicited commercial communications reached its maximum in 2014, when nearly eight thousand complaints were delivered to the Office. Since that time however a downward trend in the number of submissions received can be observed. In the opinion of the OPDP, this trend can be explained primarily by two factors.

The first factor is the reduced promotion of discount websites. The phenomenon of discount sites in Czech Republic primarily experienced a boom around the year 2010. In the following years however the interest in discount sites faded. Behind this drop-off is for one thing the fact that the discount sales on offered goods and services ceased being as attractive, and also the publicised cases of certain discount websites that took money from their customers, but did not provide what was promised.

The second reason the Office sees as decisive for the shrinking number of received complaints is the fact that the operators of free e-mail services began better protecting their clients from mass and harassing e-mails by automatically rerouting these types of messages into "bulk" or "spam" folders without the account user having to do a single thing for this selection.

Last but not least it is worth mentioning that the education of persons in relation to electronic communication has changed considerably, as has their approach to submitting complaints. In previous years, OPDP often received complaints which at first glance could not be considered commercial communications within the meaning of Section 2 f) of Act No. 480/2004 Coll. In 2017 a marked drop could be observed in complaints that in subsequent analysis could be labelled SPAM (in 2017 this was 57 complaints, in 2016 it was 167 complaints and in 2015 165 complaints), i.e. messages that are not commercial communications but merely harassment.

Although it is evident from the above graph that there has been a marked drop in complaints, it is not possible to speak of a drop in work for the inspectorate dealing with unsolicited commercial communications, as this issue has become more challenging, primarily in terms of uncovering the perpetrators of offences. There is also often interdependence between the various entities that figure within the inspection. Inspectorate employees must also work with a greater number of obliged parties and often with chains of sub-contractors (the actual disseminators). All these aspects prolong proceedings with regard to the legal deadlines. The price for longer duration of proceedings however is generally the uncovering of both the disseminators of commercial communications and of the persons who take part in spreading commercial communications and subsequently punishing them in administrative proceedings.

The company anji s.r.o.

In January 2017 the Office began receiving complaints against the company anji s.r.o. about the sending of unsolicited commercial communications. Due to the number of complaints received, on 2 March 2017 an inspection under Act No. 255/2012 Coll., on Inspection (Inspection Code), the objective of which was to assess compliance with Act No. 480/2004 Coll., on Certain Information Society Services and Amending Certain Acts in connection with the sending of unsolicited commercial communications.

It was discovered during the inspection acts that the inspected entity purchased databases of e-mail contacts and utilised two companies to send out commercial communications to these contacts, specifically Effective online s.r.o. and Clever Monitor s.r.o.

The first problem that evidently gave rise to the whole inspection procedure was the purchase of the database. As OPDP has already stated several times, it is highly unlikely that there is a database that meets the criterion of informed consent, which is the most important thing for distribution of commercial communications. For sake of completeness it should be added that consent must be 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. Consent to the sending of commercial communications cannot be given generally, i.e. to an undefined range of entities (disseminators of commercial communications) for unspecified offers. When purchasing a database, the obligation for a valid legal entitlement to send commercial communications applies mutatis mutandis. The Office has thus repeatedly stated that it is highly unlikely that there exists a database containing electronic addresses whose users have provided consent to the sending of commercial communications, for the very reason that consent must be granted to a specific disseminator before the commercial communication is sent, or it must be granted to the subject on whose behalf the commercial communication is sent. In addition it must be said that the inspected entity informed the company selling the database (Imper CZ s.r.o.) of the purpose for purchasing the database product. Despite this however, Imper CZ s.r.o. sold this database product and following agreement with the purchaser (the inspected entity) the contract was amended. Nevertheless, despite the amendment of the agreement on provision of a licence to the database, this database could not have been used in accordance with Act No. 480/2004 Coll.

On the previous paragraph the Office states that there is no link between legal processing of personal data by a personal data controller (Section 4 j) of Act No. 101/2000 Coll.) and sending of commercial communications by another entity, whether for its own benefit or for that of a third party. In other words, if entity A legally processes personal data, say e-mail addresses, this does not mean that their use by entity B, even if for the same purpose (offering of goods or services), is also legal, as it is necessary to obtain consent to such commercial contacting of the electronic address user (see above on the issue of consent to sending of commercial communications).

Another problematic point of the whole case was the use of another two companies (Effective online s.r.o. and Clever Monitor s.r.o.) for the actual distribution of the commercial communications. On this issue the Office notes that the responsible party for distribution is not just the one that gives the order, concludes a contract for that purpose or offers other consideration, but also the one that realises it without expressing the level of precaution that can be fairly demanded and checking whether the recipient of the commercial communications has truly expressed their consent to such electronic mail. Following the new legal treatment of the Misdemeanour Act (Act No. 250/2016 Coll., on Liability for Offences and Proceedings on Them), it is necessary to add on the liability of a legal person that under Section 20 of the cited act it is necessary for actions of a natural person to take place, which are then attributed to the legal entity. The group of natural persons whose actions are attributed to a legal person are exhaustively defined under Section 20 (2) of Act No. 250/2016 Coll.

In the described case however the Office did not proceed according to the new legal treatment, but in light of the temporary provisions in Act No. 250/2016 and due to the fact that the administrative offences of the inspected entity accumulated (aside from failure to prove consent and thus sending commercial communications without consent, the inspected entity also erred in terms of the formal aspects of the commercial communications), OPDP held joint proceedings with the companies anji s.r.o., Effective online s.r.o. and Clever Monitor s.r.o. under the "old" legislation.

Joint proceedings were launched by delivery of the Notification of Commencement of Proceedings, which was sent and delivered to all involved companies. The Office provided all parties to the proceedings space to comment on the whole proceedings and then issued its decision. In this decision the Office primarily accented the issue of database systems described above. The Office furthermore addressed the issue of the term "disseminator of commercial communications", in its decision repeating its previously published position (see https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=23490&n=za-sireni-obchodnich-sdeleni-je-odpovedny-nejen-rozesilatel-ale-i-objednatel). On this term OPDP added that it must be viewed primarily from a linguistic perspective, where in the Dictionary of the Czech Literary Language, šiřitel (disseminator) can be understood as "one who spreads something, makes it known". For this reason the disseminator of commercial communications must be considered to be both the entity that actually sends the commercial communications and the one who gives the order to send them, concludes a contract for the purpose of sending them, or takes a step toward the making of a commercial communication known that results in the actual sending of the commercial communication.

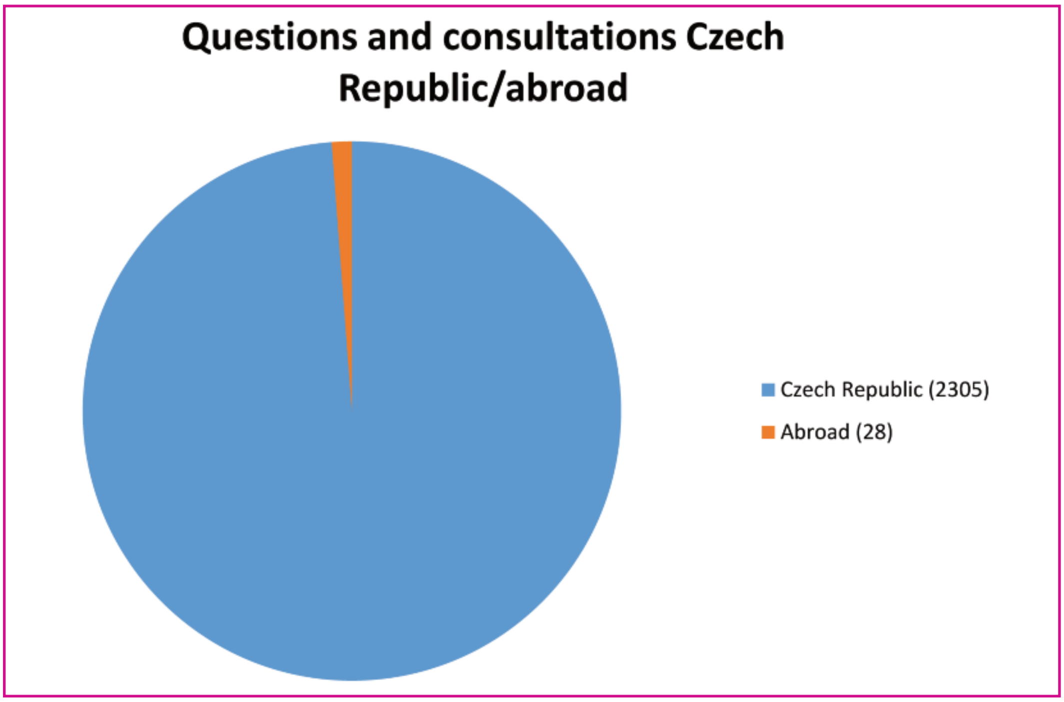
From the perspective of administrative punishment, the Office took into account several facts which decided about the sanctions for the individual parties. On the part of the inspected party it was primarily the fact that immediately after the inspection proceedings began, the e-mail campaign was stopped and inspected entity actively cooperated with the inspectors for the whole duration of both the inspection and following administration proceedings. Another fact that cannot be omitted is the relatively small impact on the privacy of individual complainants based on the number of complaints received by OPDP. In the case of the companies that carried out the sending of commercial communications, the Office assessed as decisive the fact that both companies are professionals in their field, both being engaged in marketing activities. Moreover, both companies were aware of the contract between the inspected entity and Imper CZ s. r. o. on provision of authorisation to use of the database. As professionals in the field within the meaning of Section 5 (1) of Act No. 89/2012 Coll., the Civil Code, both companies should have known that a contract set up in this way does not entitle either one of the companies to disseminate commercial communications.

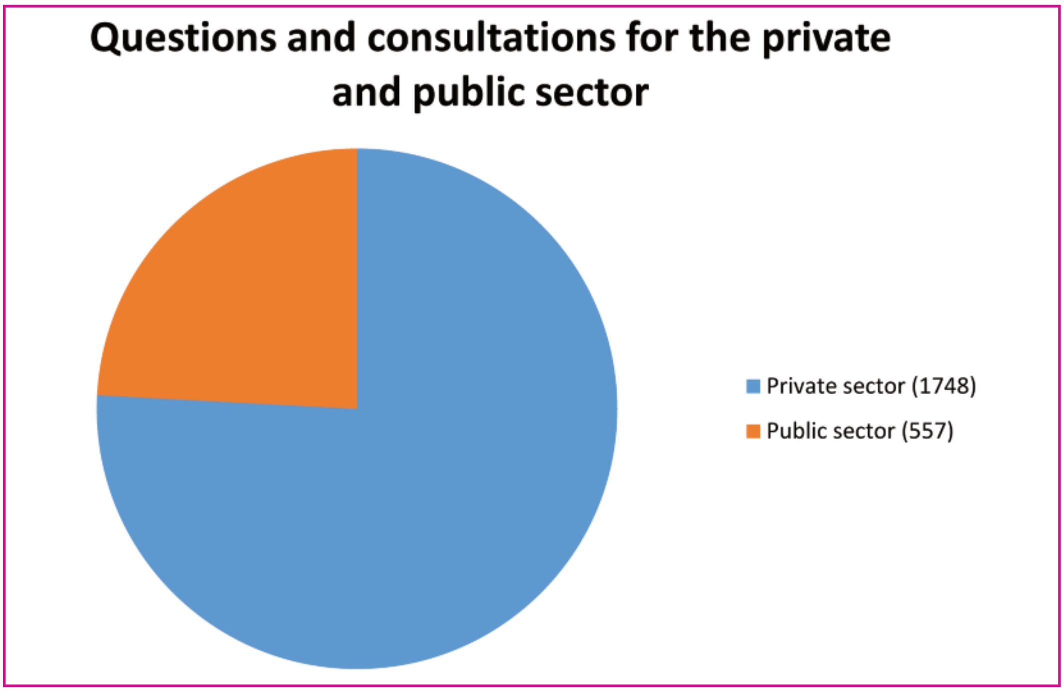
On the whole case it is necessary to add that the company Clever Monitor s. r. o. filed an appeal against the OPDP decision, which the Office President rejected.

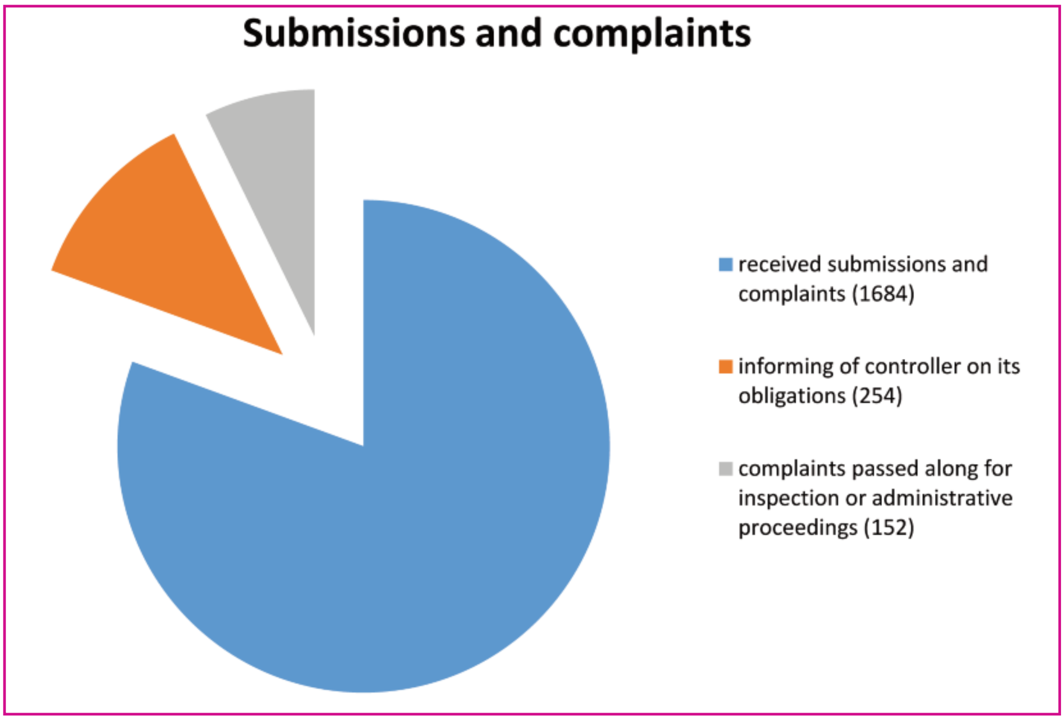
---

[1] http://ssjc.ujc.cas.cz/search.php?hledej=Hledat&heslo=%C5%A1i%C5%99itel&sti=EMPTY&where=hesla&hsubstr=no

Other Supervisory Activities







• COMPLAINTS HANDLING AND CONSULTATIONS

Execution of the complaints agenda in 2017 took place in the standard manner without any serious impact by new or amended legislation in comparison with the previous year.

Roughly one fifth of the complaints agenda in 2017 comprised complaints over camera systems operated by various entities, whether in the position of personal data controller or by private natural persons acting under their civic liability. Another area that can be mentioned is the processing of personal data for the purpose of direct marketing and other marketing activities. The resonance of this topic in the complaints agenda led to the Public Relations Department proposing this area for the Supervisory Plan for 2018. Nor can we forget complaints about personal data processing by financial institutions, particularly in relation to related personal data processing in information databases on consumer credit rating. A large portion of complaints also related to personal data processing by employers or local governments, as well as for example educational institutions. Other complaints received concerned other aspects of life in which personal data end up being processed.

Compared to the previous year, in 2017 there was more frequent use of informative letters in dealing with the complaints agenda, the purpose of which was to inform a controller of its obligations, particularly in cases where the complaint was clearly a minor breach of obligations that can be remedied without requiring public intervention in the form of administrative proceedings or inspection, or when it falls outside jurisdiction. These were most frequently sent to personal data controllers, but also to other entities whom the Office informed of their legal obligations and recommendations on how to proceed in order to comply primarily with Act No. 101/2000 Coll. This was done in 254 cases, in particular for:

• publishing identifying information on applicants for information under Act No. 106/1999 Coll., on Free Access to Information
• certain obliged entities
• improperly formulated information for data subjects
• superfluous requesting of consent to personal data processing

Informative letters were also used quite frequently in the field of camera systems operated by controllers. Private natural persons were sent information concerning their use of cameras relating to the protection of privacy of other natural persons and the inability to cross the boundaries laid down by Act No. 89/2012 Coll., the Civil Code. It can be stated that this form of informative letter proved very effective and most cases were remedied immediately.

The consultation agenda of OPDP saw significant changes in terms of content in 2017 compared to previous years in connection with the impending entry into force of the General Data Protection Regulation.[2] From the first quarter of 2017 the trend from the end of last year grew, when both written questions and telephone requests for consultation on the future legislation on personal data protection began to increase. The growing media campaign on this issue unfortunately brought about many incorrect opinions and misinterpretations. An example is the alleged expansion of the term personal data to include other data or the alleged imposing of new obligations that the Act on Personal Data Protection had already long ago imposed. Such misinterpretations thus had to be explained and the record set straight. On the other hand a positive aspect of this campaign was that it attracted the attention of most controllers to the issue of personal data protection, including those that had not previously taken a sufficient interest in it. This was also felt in the enormous growth in telephone inquiries the employees of the Public Relations Department dealt with. By the end of 2017 the topic of the General Regulation dominated in the consultation agenda.

The most frequent inquiries on the content of the GDPR were questions on Data Protection Officers, especially which entities must name one, who can hold this function and in what way the qualifications for this function can be obtained. Other frequent topics were questions on personal data protection impact assessments: in what cases they must be conducted, especially when the list of operations that will be subject to this assessment will be made public and when prior consultation with the Office will need to be made. It was also necessary to explain for example the conditions for application of the new right to portability of personal data, as well as exemptions from the obligation to keep records on processing activities and who is competent to draw up codes of conduct. Questions were also directed at clarifying certain vague terms, e.g. what processing can be considered extensive, or the term "high risk". In some cases the inquirers were interested in whether the force of the General Regulation alters existing approaches, e.g. to back-up systems for biometric identification of data subjects. Also worthy of mention are numerous general questions on the impact of the GDPR on individual controllers.

To answer the questions, not only was the text of the General Regulation itself used, but also the guidelines issued by the WP29 group on its application. These are available to the public

[2] Regulation (EU) of the European Parlament and of the Council No. 2016/679 of 27. April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

on the Office's website. It was nevertheless difficult to respond to certain specifically worded inquiries, as only application in practice can lead to a settled interpretation of certain generally worded terms. Serving to facilitate answering of frequent questions on the Office's website are the section Frequently Asked Questions on the General Regulation and Basic Guide.

More significant personal consultations on the GDPR were conducted including employees from other OPDP units. These were provided, for example, to various sectoral employers, for example the Czech Banking Association, the Association for Internet Development, the Association of Innovative Pharmaceutical Industry and delegation of future Data Protection Officers.

Dominating inquiries on the Personal Data Protection Act were again requests for explanation of the conditions for operating camera systems. Also frequent were questions on the possibility of making visual and audio recordings in another, non-automated way. Our experts also devoted much time to questions on the topic of personal data processing in the activities of municipalities, including the options for publishing personal data on the basis of the law and options for making them available on the basis of the Act on Free Access to Information without violating the Personal Data Protection Act, and on the manner of recording personal data in municipal chronicles. There were also questions on a possible change to the valid legislation in order to improve personal data protection as concerns the massive dissemination of birth numbers of entrepreneurs as part of the VAT number on receipts based on the Act on Registration of Sales, and the obligation of physicians to issue electronic prescriptions stored in the central repository of the State Institute for Drug Control under the Act on Pharmaceuticals.

• FINDINGS FROM ADMINISTRATIVE PROCEEDINGS

In 2017 the Office issued fines for administrative offences and misdemeanours in a total amount of CZK 6 097 000, of which CZK 4 618 000 was for unsolicited commercial communications. A summary of statistics on proceedings OPDP held in 2017 can be found in the section of this annual report entitled The Office in Numbers.

The primary challenge for the Office in terms of administrative proceedings in 2017 was the new legal treatment of "administrative punishment" contained in Act No. 250/2016 Coll., on Liability for Offences and Proceedings on Them, which took effect 1 July 2017. The law in question clarifies and unifies certain rules for administrative proceedings on sanctions. It terms the violation of a law entailing administrative criminal liability an offence, regardless of whether it was committed by a natural person for one thing (i.e. the same as previously) or a legal person or natural person doing business for another.[3]

From the perspective of the offences dealt with by the Office, a significant change is the setting and harmonising of the limitation period for offences. With regard to the amount of fines that can be imposed for perpetrating such, the period is five years from when they were

[3] I.e. those entities that previously cimmited what were called administrative offences.

committed. There is a new option of imposing merely an admonition against legal entities and natural persons doing business for the offences they commit, or under the conditions laid down by the law[4] the imposition of an administrative penalty may be waived. OPDP made use of the option of imposing an admonition in five cases in 2017. One example was the case of a municipality which, as part of the information provided on the basis of a request under Act No. 106/1999 Coll., on Free Access to Information, also provided the applicant personal data in the scope of the number of complaints, requests and submissions a specific person had submitted to them in the previous years. It must be stated that the purpose of processing the personal data of persons who come to the municipality (or any other legally bound entity under Act No. 106/1999 Coll.) with the complaints, requests or submissions for which these data were collected, is the receipt, registration and resolution thereof. Subsequent disclosure of the personal data of applicants in connection with provision of information under Act No. 106/1999 Coll. evidently oversteps this purpose. The inadmissibility of providing the aforementioned personal data can also be deduced from Section 8a of Act No. 106/1999 Coll., according to which a legally bound entity shall only provide personal data in accordance with the legal regulations governing their protection, i.e. in accordance with Act No. 101/2000 Coll., which, as stated above, does not allow such an approach.

Also significant for the Office and its activity is the part of Act No. 250/2016 Coll. concerning determining the type and amount of the administrative penalty, particularly the criteria evaluated in determining the nature and severity of the offence. These include a non-exhaustive list of the mitigating and aggravating circumstances, which in the field of punishing misdemeanours and other administrative offences had previously not existed. Among the mitigating circumstances that could be relevant from the perspective of the Office's activity are for instance the fact that the offender helped eliminate the damaging consequences or reported the offence to the administrative authority and effectively helped in clearing it up. In contrast, from among the aggravating circumstances, in certain cases OPDP can factor in that the offender committed the offence on a child, someone pregnant, ill, disabled, elderly or infirm. In other words, the unlawful processing of personal data that is being punished affected this group of persons.

In terms of personal data processing in general, Act No. 250/2016 Coll. allows the imposition of an administrative punishment called "publication of a decision on an offence" (in a public medium and posting to the official bulletin). This type of administrative punishment cannot however be imposed on a natural person not doing business, and the law must explicitly provide for the possibility of imposing it. An example of such a law is Act No. 257/2016 Coll., on Consumer Credit, which under Section 156 orders the Czech National Bank to publish without needless delay a final decision imposing a fine in a manner allowing remote access and for a duration of five years. Should publication on the basis of the prior assessment be found to be unreasonable toward the affected natural person, the Czech National Bank shall publish the decision without identifying information on the fined person. A matter of course also addressed in Act No. 250/2016 Coll. is that the published decision on an offence may not contain data allowing the identification of a person other than the offender. A contrario it can be inferred

[4] If, in light of the severity of the offence, the circumstances of its perpetration, and the person of the offender, it can be reasonably expected that the hearing of the case before the administrative organ alone is sufficient to remedy it.

from the above text that if a decision on an offence was published without this fact being allowed by special legislation, or if the personal data of a person other than the offender were to be part of the published decision on an offence, this course of action would be unlawful.
In conclusion it can be stated that in 2018 changes will take place in the imposing of sanctions, as with many other Office procedures, in connection with the force of the General Data Protection Regulation. At the same time the Office and the public will only know the exact form of administrative punishment once the new Act on Personal Data Processing had been adopted. Nevertheless it can already be stated today that in determining the type and amount of sanctions, Article 83 of the Regulation will be followed, inter alia setting out independently of Act No. 250/2016 Coll. the circumstances which must be taken into account in imposing an administrative fine.[5]

• FINDINGS FROM JUDICIAL REVIEWS

In 2017 several decisions were submitted for judicial review and several judgments were announced. At the same time however many OPDP decisions are still awaiting judicial review. From the specific findings from the relevant judicial practice in 2017, the following rulings can be pointed out, concerning primarily the publishing of police recordings, the publishing of recordings by private entities, the monitoring of employees, and operation of camera systems:

1. The publishing of a shortened audiovisual recording that was originally made on 12 June 2013 by the Police of the Czech Republic when arresting Jana Nečasová, formerly Nagyová, on the Czech Television programme entitled "Questions with Václav Moravec". This act was in pursuit of the public interest in accordance with the provisions of Section 8d (1) of the Criminal Procedure Code.

On 22 December 2013, Col. Robert Šlachta, Director of the Organised Crime Unit of the Crime and Investigation Police Service, provided a shortened audiovisual recording for broadcast on the Czech Television programme entitled "Questions with Václav Moravec", which he attended as a guest, that was originally made on 12 June 2013 by the Police of the Czech Republic during the arrest of Jana Nečasová, formerly Nagyová. In this recording, the faces of the persons recorded had been blurred by technical means. Nevertheless the Office qualified this act as a violation of the obligations laid down under Section 13 (1) of Act No. 101/2000 Coll., consisting of failure to adopt measures preventing the unauthorised transmission of the recording in question, thus committing an administrative offence under Section 45 (1) h) of Act No. 101/2000 Coll., for which it imposed a fine of CZK 60 000. The decision of the first instance administrative authority no. UOOU-01670/14-11 of 18 April 2014 was then confirmed by decision of the Office President no. UOOU-01670/14-17 of 23 June 2014, but it was then challenged by an administrative action.

[5] E.g. steps taken to miligate the damages caused to data subjects, level of cooperation with the supervisory authority in order to remedy the given violation and mitigation of its possible adverse consequences, or aiso the manner in whitch the supervisory authority learned of the violation. In particular wither the controller or processor announced the violation and if so to what extent.

In judgment no. 5A 138/2014 of 2 November 2017, the Municipal Court in Prague upheld the action in question. In particular the court pointed out that the provisions of Section 8d (1) of Act No. 141/1961 Coll., on Criminal Procedure (Criminal Procedure Code), allows the publishing of information if justified by the public interest. At the same time however it is necessary for this interest to outweigh the right to privacy of the person affected. This provision of the Criminal Procedure Code represents an exception to the prohibition of publishing information. This is enshrined in the provisions of Section 8a of the Criminal Procedure Code. In the given case the court found that the publishing of information was, in light of the context of the situation, strongly in the public interest with regard for the need to maintain faith in the Police of the Czech Republic. For the publishing of specific information to be justified under Section 8d (1) of the Criminal Procedure Code, it was however necessary to also assess whether this public interest outweighed the right to privacy of the person concerned, here Jana Nagyová. The court had no doubt about the fact that the publishing of the video truly encroached on Jana Nagyová's private life. On this matter it also stated that the publishing of the police video from the arrest is not standard procedure. This fact did not however impact the assessment of fulfilment of the appropriateness of the step, but it is merely a question of proportionality in the strict sense.

The Municipal Court in Prague expressed agreement with the opinion of OPDP that the publishing of the video recording is a more sensitive encroachment on privacy than verbal or written information. The scope of information and intensity of the perception in a visual recording tends to be higher than in a verbal description. On the other hand however, it did not find the scope of this secondary information to be major. The court also considered it fundamental that the recording did not show Jana Nagyová in any delicate or undignified situation. Thus it was not able to negatively impact her honour and dignity, other than the information itself that she was arrested in her flat in the evening. This was however again information that was already known, and thus it was not made public by the video recording in question. It therefore followed from the ruling that the encroachment on Jana Nagyová's privacy was not great, while the legitimate interest pursued was of major significance.

Likewise, in the opinion of the court, the purpose pursued could not have been achieved by review by other authorities. The court also rejected the opinion that the publishing of the video recording had any negative impact on the criminal proceedings against Jana Nagyová.

2. *Processing of personal data of employees of Czech Post on the basis of a GPS localisation application, via which information was collected on employees in the position of postal carrier in the scope of length of route, time spent on route, evaluation of whether the carrier was only in their district, records and depiction of monitored events marked by carrier during their rounds, percentage of delivery district serviced (proportion of visited delivery sites compared to total number of delivery sites), delivery sites with greatest number of visits and a complete list of visited/unvisited delivery sites. This took place for the purposes of oversight and optimisation of delivery districts, or to adjust the database of delivery sites, and lacked a legal basis.*

An inspection conducted at Czech Post, completed with inspection report no. INSP1-3568/12-12/BYT of 4 October 2012, found the use of GPS localisation technology, through which the collection of personal data of employees was taking place in violation of Section 5 (2) of Act

No. 101/2000 Coll., and for the above reasons remedial measures were imposed consisting of the destruction of the collected personal data and prohibition of further personal data processing in the stipulated scope. Though the remedial measures were partially altered on the basis of submitted objections, the relevant decision of the Office President no. INSP1-3568/12-16 of 3 January 2013 was nevertheless challenged by an administrative action.

The Municipal Court in Prague however rejected this action in its judgment no. 6A 42/2013 of 5 May 2017. In the grounds for the judgment the court stated in particular that it is necessary to distinguish an employer obtaining information on the performance of work by employees and the collection of employee personal data. Surveillance of performance of work by an employer is justified if it does not invade the employee's privacy in the workplace. An exception may be serious grounds inherent in the special nature of the employer's activity.

In the given case the employer was collecting data systematically over a period of one year. The nature of its activity cannot, in the opinion of the court, be considered so special that rounds on a route in a delivery district justify invasion of the carriers' privacy in the workplace. Use of the technology in question could not have even prevented potential failure to delivery consignments to their addressees or other misconduct. The obligation to fulfil the conditions of the licence and the law alone do not make the employer's activity anything that would justify failure to respect employees' privacy in the workplace.

For the processing of personal data to be legal, it would be necessary for the employer to assess various options for processing and choose the one that encroaches on the privacy of carriers the least. This was not however the fulfilled when the employer was processing information of the above scope every day.

The court also stated that the Office took into account the employer's interest in living up to its obligations under the Act on Postal Services.[6] OPDP stressed that the processing of personal data via the technology in question with the scope of data concerning place and time attesting to the visited delivery sites in order to ensure the quality of the provided postal services and dealing with claims was not in violation of Act No. 101/2000 Coll., and for this reason it modified the remedial measures imposed in the corresponding manner. Although an employer has the right to supervise compliance with the labour-law obligations of its employees,[7] it must do so within the limits of the possibilities laid down by the legal code. The processing of employee personal data through the technology in question was not however an appropriately selected method of supervision or obtaining statistical data. In light of the above, it cannot be concluded that the data of the plaintiff's employees processed by the technology in question fall under the exception of Section 5 (2) a) and e) of Act No. 101/2000 Coll., as the processing of personal data in such a scope was not essential for complying with the plaintiff's legal obligations. Given the scope of the data obtained, in this case it took place in violation of the right of carriers to protection of privacy in the workplace.

3. The purpose of operating a camera system in the protection of property is merely collecting data for their potential transfer to the legally designated authorities for further acts, not

[6] Securing and duly delivery consignments, in particular in connection with dealing with claims, etc.
[7] See Section 316 (2) of the Labour Code.

their future publication. The investigation and prosecution of crime, under which the perpetration of offences can be included, is fully in the jurisdiction of state authorities. The right to protection of property should be brought to bear by transmitting acquired data tothe Police of the Czech Republic. The publishing of such acquired data on a social network transgresses the defined boundaries. The important thing here is not even whether this approach would lead to discovering the perpetrator or not.

In its judgment no. 3 As 118/2015 of 8 June 2016 on the basis of an appeal submitted by the Office, the Supreme Administrative Court overturned a prior ruling by the Municipal Court in Prague overturning a decision of the Office by which the operator of a camera system was fined for a total of CZK 5000 for two administrative offences - failure to notify of intent to process personal data via a camera system, and processing of personal data contrary to the purpose for which they were collected. The second offence was to have consisted of the fact that the camera system operator published a photograph on Facebook from the camera capturing a person suspected of theft without having their consent and despite the fact that the law does not allow for this approach. It was this second offence that was the subject of dispute.

A constitutional complaint on this matter was then rejected by the Constitutional Court in its resolution III. ÚS 3565/16 of 5 September 2017, upholding the opinion previously expressed primarily by the aforementioned judgment of the Supreme Administrative Court.[8] The Constitutional Court also stated that over the course of the previous proceedings the complainant evidently did not produce relevant doubts on the conclusion of an absence of "necessity" of publishing the photograph by the complainant on the social network. Indeed the complainant himself stated in the constitutional complaint that the police would evidently have published the photo itself, which the Police of the Czech Republic did not deny. This does not support the complainant's opinion, according to which the publishing was the only available, necessary, and effective solution to protecting his property rights.

Moreover it did not follow from the whole proceedings or the constitutional complaint that the Czech Police had refused to fulfil its legal obligations during handover of the recording. Over the course of the proceedings the complainant did not object to the actions of the police in any way. The actions of the complainant can thus not even be justified by the provisions of Section 89 (2) of the Criminal Procedure Code, which allow for proof against a perpetrator to be sought out in parallel with law enforcement authorities, as this would violate the legally regulated protection of personal data.

The Constitutional Court thus did not find that the conclusions of the public authorities were arbitrary or otherwise deviated from the bounds of the constitution.

The Office however took up this case again in detail and, following extensive discussion, issued an position on 3 October 2017 indicating a certain shift in its decision-making for assessing similar cases:

"*Under the current leadership of the Office, no fine would be issued to the company ekolo.cz. Its President, Ivana Janů, is convinced that no interpretation of any law can be detached from the perception of justice in society.*

---

[8] See 2016Annual Report

It is necessary to honour the principle that everyone should be able to bring their rights to bear in a reasonable manner if their legally protected interests have been infringed upon. The important thing is that it be reasonable and under the condition that it be clear that intervention by public authorities will not come in time. And this was such a case," explained Office President Ivana Janů.

At the same time it is important to point out that the Office's last active step in this case was to submit an appeal complaint to the Supreme Administrative Court on 1 June 2015, which took place three months before President Ivana Janů took over the institution.

"I had hoped that the specific nature of the ekolo.cz case would be taken into account in proceedings before the Constitutional Court and the practical impact of the court's decision would also be considered," the Office President declared.

At the same time she points out the misleading claims concerning the case that appeared in the media and which are not based on a complete reading of the valid law. The argument that consent of the person suspected of theft was allegedly required to make, or publish, the recording is not correct. On this matter the consent of the recorded person is not necessary for the robbed person. The important thing for assessing the case is whether he acted in the interest of protection of persons and property, which the Act on Personal Data Protection does not neglect.

The Office wishes to assure the public that its decision-making practice undergoes ongoing evolution (see Position No. 1/2016- Placement of camera systems in residential buildings). Such changes must not however be rapid one-off campaigns, but on the contrary it must be a deliberate process based always on a thorough evaluation of each individual case so as to respect the principle of proportionality in interpreting the Personal Data Protection Act and the protection of rights and legally protected interests in processing of personal data by a controller or other persons.

4. Operation of a camera system also recording the space of foreign neighbouring properties without the consent of the recorded persons cannot be legalised with the general statement that it is necessary protection against the damaging of one's own property.

With decision no. UOOU-08116/14 of 20 November 2014, the Office qualified the processing of personal data by means of a camera system installed and operated on a residential building that was making a recording of the space of neighbouring properties owned by other persons without the consent of the recorded persons as committing of a misdemeanour under Section 44 (2) e) of Act No. 101/2000 Coll., for which it imposed a fine of CZK 5000 on the operator. On the basis of an appeal, the decision of the first-instance administrative authority was altered on by decision of the Office President no. UOOU-08116/14-22 of 22 January 2015 primarily in that the amount of the fine was lowered to CZK 2000. The rest of the appeal was however essentially rejected, and the decision of the President was therefore contested by an administrative action.

The Supreme Administrative Court in its judgment no. 2 As 140/2017 of 20 September 2017 upheld the ruling of the Municipal Court in Prague no. 4A 21/2015 of 30 March 2017 rejecting the action against the OPDP decision to impose the fine. The court stated that the arguments of the camera system operator on the necessary and reasonable protection of their property against crime remained in the plane of purely subjective claims, or rather subjective feelings. Such have no objective basis in the case file and evidence contained therein.

The frequency of their complaints and repeated references to official records of submitted explanations have no significance in and of themselves. If no administrative or court decision attesting to the alleged version of facts has never been issued, then at least some sort of credible evidence would need to be submitted objectively supporting the claim in question. No such thing occurred however.

In addition, no explanation of the reasons for these actions was proffered in the appeal complaint even. The neighbour was alleged to be constantly committing illegal acts. The operated cameras (camera traps) did not however capture any such acts.

It was also stated that the exemption under the provisions of Section 3 (6) d) of Act No. 101/2000 Coll. concerns solely law enforcement authorities.

• REGISTRATION

Compared to 2016 there was a slight drop in the number of notifications on personal data processing last year. A total of 9241 notifications on personal data processing or change of processing were sent to the Office (compared to 9708 in 2016). Of those 513 notifications (i.e. over 5.5 percent) contained incomplete or improper information or it was not evident whether the notified processing would lead to violation of the law. Thus these notifiers were sent a request to amend the notification on personal data processing. Of the overall number of entities this was sent to, only 31 sent in the additional information, which confirmed the fears of possible violation of Act No. 101/2000 Coll., on Personal Data Protection, and thus proceedings under Section 17 of this act were launched. Of the overall number of submissions however, only for one notification was the commencement of personal data processing not permitted. For the others the parameters of personal data processing were adjusted or they withdrew the registration.

On the basis of requests from controllers, OPDP also carried out 156 cancellations of personal data processing.

The most frequent notifications on personal data processing in 2017 were personal data processing by camera systems with recording[9] and personal data processing as part of running an internet shop.

A total of 3202 controllers reported personal data processing by camera systems in 2017 (end-of-year estimate 3800), of which 2970 controllers were recorded in the register (end-of-year estimate 3550). The rest consisting of processing where the controller had ceased making a camera recording, or it was the personal need of the controller.

---

[9] About 40 percent of all notifications.

[10] Regulation (EU) of the European Parliament and of the the Council No. 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation).

Starting 25 May 2018 the new legislation governing personal data protection enters into force, which is the General Data Protection Regulation.[10] One of the many significant changes that the new legislation brings in is doing away with the notification obligation that was laid down for personal data controllers by Act No. 101/2000 Coll. At the same time the public register of personal data processing will be closed in May 2018. The notification obligation and keeping of a public personal data processing register will be replaced by other legal institutions.

The notification obligation allowed the Office to intervene in the processing of personal data at the stage before it even started, thus the registration process represented a certain form of preliminary supervision. The GDPR transfers this function to a large extent to the field of self-regulation, with personal data controllers themselves obliged to keep records on their processing activities (Art. 30), conduct a data protection impact assessment in the case of high risk processing (Art. 35), and only in the case a high risk cannot be eliminated to turn to the Office with a request for consultation (Art. 36).

The publishing of registered notifications also provided data subjects with basic information on the personal data processor and the processing being conducted by them (unless exemptions from the notification obligation were applied). The General Regulation replaces this function by deepening the principle of transparent processing (Art. 12), obligation of controllers to inform data subjects (Art. 13 and 14) and the introduction of an institution of a data protection officer (Art. 37 to 39).

These changes place an overall greater emphasis on the personal responsibility of personal data controllers, who must be able to produce proof they are processing data in accordance with the GDPR.

• TRANSFERS OF PERSONAL DATA ABROAD

In 2017 the Office received 31 new and finished dealing with three old requests for permits to transfer personal data to third countries under Section 27 (4) of Act No. 101/2000 Coll. OPDP managed to resolve all the requests within the given calendar year, thus all 34 proceedings were completed.

One case was suspended because the applicant failed to respond to a call to fill in information. One request was set aside because in the end the applicant provided for transfer of personal data to a third country with an insufficient data protection standard in a manner that does not require the Office's permission.[11] In general however the Office has long recommended using standard contractual clauses as per the European Commission decision.

In the other 32 cases, OPDP permitted the transfer of personal data to third countries based on the following legal titles.

The most frequent legal title under which the Office issued the permits was Section 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 21 cases.

[11] In this specific case via a US data recipient under the privacy shield programme.

In five cases the legal title for the permit was Section 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. In four cases the legal title was Section 27 (3) a), i.e. transfer of data with the consent of or based on an order from the data subject. In one case the Office issued a permit for transfer necessary to perform a contract concluded in the interest of a data subject between the controller and a third part under the provisions of Section 27 (3) d) of Act No. 101/2000 Coll. In one case the Office permitted the Czech National Bank a transfer necessary for exercising an important public interest under the provisions of Section 27 (3) d) of Act No. 101/2000 Coll.

In terms of target countries, in most cases transfer of personal data was taking place to multiple countries on all continents. This took place in cases where personal data are shared with other branches of multinational groups, with the processing and transfer of personal data governed by the binding corporate rules of the given multinational group.

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. This group ensures protection of personal data shared within the group via the aforementioned binding corporate rules. In the case of permitted transfers to one or two specific third countries, the target destination of personal data in eight cases was the United States of America, in four cases India, and in one case each Australia, Canada and Colombia. One case concerned the transfer of personal data of participants in the Olympic team to South Korea.

In several cases OPDP got involved in the cooperation approval procedure for the BCR of a certain multinational group in the role of a "co-reviewer". This approval procedure currently takes place according to the WP107 working paper adopted 14 April 2005 by the WP29 Working Party. As part of an unwritten gentlemen's agreement on mutual recognition among most of the supervisory authorities of the individual European Union Member States, one to two supervisory authorities help the lead authority carrying out the approval procedure for specific BCRs. They carry out comments proceedings on the consolidated draft of the BCR and assess whether the draft BCR corresponds to the principles defined in WP153 or WP195. This approval procedure will evidently be applied under the General Regulation as well,[12] although it is not entirely clear in what way it will be regulated and tied in to the mechanism of uniformity defined by the new regulation.

The Office grapples with the solution to this question and many other issues arising in connection with the impending effect of the General Data Protection Regulation in concert with the other supervisory authorities in the individual EU Member States under the International Transfers subgroup of the WP29 Working Party. The result of this subgroup so far has been preparation of three materials.

Two of them summarise the essential requirements for binding corporate rules in accordance with Art. 47 of the General Regulation; the revised principles that BCRs for controllers must

[12] Regulation (EU) of the European Parliament and of the Council No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movemennt of such data, and repealing Directive 95/46/EC (General Protection Regulation).

observe (WP256, originally WP153) and the revised principles that BCRs for processors must observe (WP257, originally WP195). Both these documents were submitted for public consultation at the end of 2017.

The third completed material prepared for presentation for public consultation is the revised principles for evaluating the adequacy of data protection standards in a third country (originally WP12). With this document, the WP29 Working Party provides the European Commission with a manual on how it should proceed in evaluating a corresponding standard of protection as per Art. 45 of the General Regulation.

Among the other documents that are to contribute to the interpretation of the GDPR provisions in the field of personal data transfer to third countries the Office is helping preparing are in particular the instructions for clarifying the criteria on the basis of which derogations under Art. 49 of the General Regulation can be used for personal data transfer.

The essential requirements for administrative arrangements, including enforceable data subject rights as per Art. 46(3b) of the General Regulation, will be provided by the position on personal data transfer under the administrative cooperation among public bodies.

Lastly, the material devoted to certification as an instrument of personal data transfer to third countries should above all clarify the nature of the binding and enforceable commitments of the controller or processor in the third country required by Article 46(2f) of the GDPR. These will then have the obligation to uphold the European principles for personal data protection in processing the transferred personal data.

A specific topic of recent years has been the Privacy Shield programme. More on this topic in the section Foreign Affairs and International Cooperation.

• SCHENGEN COOPERATION

Great emphasis is placed on the protection of personal data processed by the extensive European information systems, which include the Second generation Schengen Information System (SIS II), Visa Information System (VIS), Eurodac and the Customs Information System (CIS), in their legal treatment. In the field of Schengen cooperation the Office fulfils the role of supervisory authority, overseeing compliance with the applicable regulations, thus contributing to the protection of the fundamental rights of persons whose personal data are the subject of processing within the Schengen area. Additionally, the authorised OPDP representative takes part in regular meetings of the coordination groups, which are assembled for the individual systems at the European level.

Aside from supervision and inspection associated with the meeting of requirements for lawful processing of personal data on the part of the controller under the aforementioned information systems, the Office also dealt with the emergence of new information systems and legal regulations. These are to modify the existing form of such systems. An example of a new system is ETIAS (*European Travel Information and Authorisation System*), under which the personal data of persons from third countries that have no visa requirement for the European Union are to be processed. OPDP also commented on the newly emerging drafts for legal amendments concerning the SIS II and Eurodac systems.

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

The common denominator for coordination groups for individual information systems in 2017 was preparation of websites, including the content thereof. Links to these groups were placed on the Office's website as well. Another common activity was finalising the joint inspection models for the Eurodac, SIS II and CIS systems. These questionnaires are intended to harmonise the control procedures under the compulsory audits.

Major topics for 2017 were the concept of interoperability of information systems and the budgets of individual authorities for personal data protection. The coordination groups for VIS and SIS II also dealt with updating the Schengen recommendations concerning the regular evaluation of the fundamental aspects of Schengen cooperation of individual Member States.

Current problems being dealt with under the coordination groups

In the summer of 2017, the SIS II Coordination Group sent a letter to Mr Antonio Tajani, President of the European Parliament, on behalf of all its members. In it they expressed certain concerns over the new "legislative package" revising SIS II, consisting of three draft regulations. The changes accompanying the new proposals represent a transformation of the current system and they must be thoroughly analysed in relation to the basic principles of personal data protection. Aside from this topic, the group dealt intensively with the issue of logging in the national systems of individual Member States.

Over the first half of 2017, the Coordination Group for VIS (VIS SCG) completed a document dealing with implementation of Article 41 of Regulation (EU) of the Council No. 767/2008 of 9 July 2008 concerning the Visa Information System and the exchange of data between Member States on short-stay visas. This material charges national supervisory authorities with the obligation to conduct an audit on data processing in the national VIS at least once every four years. The Coordination Group also continued in preparing a study concerning system subcontractors and the legal regulations on personal data protection that apply to them.

One of the main activities of the Coordination Group for Eurodac (Eurodac SCG) was creating a questionnaire comparing the rights of data subjects. This questionnaire was circulated to Member States to be filled out at the beginning of 2018.

At the start of 2017 the Coordination Group for the Customs Information System (CIS SCG) completed a unified document governing the general rules for personal data processing in CIS. The document was made public on the Office's website. The Czech Republic is also actively involved in it as the rapporteur for completing the joint inspection plan for CIS.

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

One of the Office's obligations is dealing with received submissions from data subjects concerning the processing of personal data in SIS II. In 2017 the Office received ten submissions, with eight of them concerning realisation of the right to information or exercising the right to erasure of data from the system. These requests were passed along to the personal data controller at the national level, which is the Police of the Czech Republic. Two complaints against the controller's actions in processing personal data were included as part of the regular audit of the national component of SIS II, which OPDP carries out on the basis of obligations under EU legislation.

The Office furthermore received a total of 26 submissions in which the petitioners inquired about the Czech Republic's visa policy or the course of processing of their visa applications. In light of the fact that this matter does not fall under the legally defined jurisdiction of OPDP, the individual 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 EU legislation.

Evaluation of level of personal data protection

In accordance with Council Regulation (EU) No. 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen, evaluations of the basic aspects of Schengen cooperation are to be regularly conducted in each state of the Schengen area. Among these are protection of internal and external borders, police cooperation, and the level of protection of personal data in using SIS II.

The evaluation teams are always set up ad hoc for the individual evaluations. These are made up of representatives of the European Commission and experts from the Member States. On the basis of the submitted documents and an on-site inspection, the evaluation team prepares a report summarising its findings on compliance of practice in the given Member State with the requirements of the Schengen acquis. This inspection generally includes a visit to the police body that runs the national component of the Schengen database, the authority for personal data protection, and other relevant institutions.[13]

In 2017 an Office employee attended an evaluation mission in Spain as a national expert (October 2017).

[13] The Ministry of Foreign Affairs for the issuing of Schengen visas, the Asylum Office, Ministry of the Interior as the competent authority for Schengen cooperation.

Analytical Activities

1. **Analysis of collection of personal data through section measurement**

In connection with the issue of personal data of natural persons being collected during section measurement,[14] the Analysis Department (ANA) dealt with a model situation concerning the legitimacy of across-the-board retention of personal data by the Police of the Czech Republic for a certain (varying) period without any link to illegal activity by the persons in question. Repeated reports on the state of human rights in the Czech Republic have pointed out the same issue, for the first time in 2006: *The introduction of camera systems for what is called 'section measurement' of vehicle speed raises doubts in terms of protection of privacy. Specific data on the movement of persons (vehicles) are recorded across-the-board without the impulse for recording being a detected violation of the regulations... This infringes on the principle that law enforcement bodies may only be active on the basis of determined facts on violation of the rules*." According to a report published by the NGO Iuridicum Remedium as well,[15] the police record the movement of cars across-the-board, taking pictures of drivers and automatically reading licence plates, with the differing period for retaining recordings in various regions being hardly justifiable.

This collection of data takes place for the purpose of protecting public order, which has an exemption in terms of the Act on Personal Data Protection. The special legal treatment of the Act on the Police of the Czech Republic applies; this however does rule out general principles of personal data protection and the supervisory role of the Office. The title for processing of personal data in this case is the institution of section measurement contained in Section 79a of Act No. 361/2000 Coll., on Road Traffic, according to which the police and municipal police are entitled to measure the speed of vehicles in order to increase the safety of traffic on roads.[15]

---

[14] During "section measurement" of vehicles, the licence plate of a vehicle is recorder at the beginning and end of a road segment.

[15] See: Available at http://www.iure.org./15/1210/police-plosne-zaznamenava-pohyb-aut-foti ridice automa-tizovane-rozeznava-spz-udaje- o kazdem, obdobně http://www.autoforum.cz/zivot-ridice/policie-uchovava-fotky-vsech-co-projedou-kolem-jejich-radaru-i-kdyz-nic-neprovedli/. No dateis listed by the published report.

[16] For91 Coll., on the Municipal Police, as amended.

The relevant legislation that allows the Police of the Czech Republic to make recordings is Section 62 of Act No. 273/2008 Coll., on the Police of the Czech Republic. According to it, the police may, if it is essential for fulfilling its tasks, procure audio, visual or other recordings of persons or things found in publicly accessible places, as well as audio, visual or other recordings of the course of the act. It is also assumed that information on the establishing of firmly installed camera systems used by the police for, e.g., monitoring the traffic situation will be published.

In the majority of cases, the recordings collected during section measurement contain personal data to which the general rules governed by Section 79 et seq. of the Police Act apply. As for the retention period of personal data, under Section 87 (1) the police shall retain personal data for the purposes under Section 85 for the period that is necessary for the purpose of their processing. Should this purpose pass, the personal data shall be destroyed, with the exception of cases explicitly stated in the law. As regards the term "period necessary for the purpose of processing", though this formulation is general, it is certainly not arbitrary, but the period demonstrably necessary. As with any exercising of powers, it is necessary when making recordings to respect the principle of proportionality (Section 11 of the Police Act), both in terms of the level of encroachment on the rights of those affected by the recordings and the severity of the specific task the police is carrying out. For the purposes of interpreting the period necessary for processing, the general principles valid for personal data protection are also applied, in particular the "principle of minimisation" of personal data retention. The ANA analysis showed that it should be considered a weak point of data collection in section measurement if a varying retention period of recordings of persons in various regions were to be demonstrated. This would indicate that the data could be processed in a shorter period and it is not necessary to keep them longer.

Section measurement implemented by the Czech Police thus takes place on the basis of special legislation while preserving the supervisory role of OPDP. The collection of recordings in the field of road transport for the purpose of public order for a certain reasonable period set as "necessary for the purpose of processing", which is road traffic safety, must be considered compatible with the law in relation to upstanding persons as well. The Office itself has in the past stated on the issue of section measurement that this method of measurement also processes the personal data of persons who have not committed any offence, and thus the continuous monitoring of all passing vehicles is a strong encroachment on the privacy of the individual and the practice must be based on the actual hazard of the given segment, giving rise to the need for constant supervision.[17] From the perspective of personal data protection this means in practice that the cameras should be installed if there are safety grounds for it, and should not be placed and used excessively. The Austrian Constitutional Court has also stated in the past on the issue of section speed measurement that the collection of personal data must take place so as to be predictable for drivers in terms of place and time.[18] Information on the placement of cameras should be made public so that the collection of personal data takes place in a manner predictable for drivers. The reason for their placement is after all the prevention of accidents in an area of road traffic, i.e. protecting values, which are the health and life of citizens,[19] not the collecting of fines.

[17] https://www.uoou.cz/zpracovani-osobnich-udaju-v-souvislosti-s-merenim-rychlosti-vozidel/d-6230
[18] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Dokumentnummer=JFT_09929385_06G00147_00
[19] For example, 5 669 people died on Czech roads in 2015. Police investigated nearly 93 thousand accidents. The most tragic months were July and September, when accidents claimed 80 lives.

2. **Analysis of monitoring of the private dwelling of a neighbour by camera**

The subject of the ANA evaluation was a model situation whereby the owner of a property (natural person) objected that their right to privacy is being infringed upon because the entrance to their building is constantly monitored by a camera from the opposite building. The complainant demanded the situation be remedied by the Office and the Ombudsman. The operator of the camera denied the above facts and claimed they are not monitoring the privacy of another person. What was problematic from a legal perspective was the manner in which the complainant was to have redressed the objectionable situation. It is unquestionable that the monitoring of a natural person by cameras is a serious infringement on the privacy of natural persons and a boundary must be set. Particularly in a situation where a family home is being monitored by the camera of a neighbour or third party, the right to privacy in the space reserved for one's personal and intimate life is seriously affected. The rule should be that the owner of a camera should in principle only be able to monitor their own property or real estate by camera, with some exceptions. Only a low degree of tolerance is permissible, as is apparent from OPDP's decisions.

Although there is no special Act on Cameras in the Czech Republic, there is no doubt about the fact that in the case of personal data processing the Act on Personal Data Protection would be applied in the above case. According to the current interpretation, the operation of a camera with or without recording can be considered processing. The main problem in this case however is that the facts claimed by the camera owner and the complainant cannot be verified. The Office does not have the option of entering the property or dwelling of a natural person, thus not even the camera owner. It is thus debatable whether it is a case of personal data processing.

If it were not a case of personal data processing, one could consider protection of personality under the relevant provisions in the Civil Code (previously Sections 11-16 of Act No. 40/1964 Coll., now Sections 84-90 of Act No. 89/2012 Coll.). In legal theory they speak of complementarity of legislation of protection of a natural person, consisting of securing effective protection of the personality of a natural person by means of various legal branches of the legal code.[20] It must however be added that this concept of complementarity is not yet accompanied by relevant case law from the Supreme Court.

In addressing the question posed, the subject of protection is thus the right to privacy. The right to privacy,[21] or the right to information self-determination[22] are what are called fundamental rights, which in the rule of law are guaranteed by the constitutional order. As far as guarantees of the aforementioned rights go, according to the working paper laying down the conditions for encroachment on the right to privacy and protection of personal data drawn up by the expert Working Party WP29,[23] the following rules should be applied in general:

- processing should be based on clear, precise and accessible rules;
- necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
- an independent oversight mechanism should exist;
- effective remedies need to be available to the individual.[24]

[20] The Office's methodological materials demand that infringement on privacy not be excessive.
[21] Knap, Švestka, Jehlička, Pavlík, Plecitý: Ochrana osobnosti podle občanského práva (Protection of Personality under Civil Law). p. 25 Linde Praha, 2004.
[22] Decision of the office No. UOOU-01297/16–48.
[23] Art. 7 of the Charter of Fundamental Rights of the EU.
[24] Art. 10 (3) of the Charter. Art. 8 of the Charter of Fundamental Rights of the EU.

Also helping significantly to refine the question of the boundaries of monitoring by camera was Judgment of the Court on the case František Ryneš C-212/13 of 11 December 2014, where it ruled on the submitted request for a preliminary ruling on the basis of Directive 95/46/EC concerning personal data processing. It dealt here with the interpretation of the term "in the course of a purely personal or household activity" from the perspective of the directive's scope. The EU Court of Justice stated that the second indent of Article 3 (2) of Directive 95/46/EC of the European Parliament and of the Council must be interpreted as meaning that the operation of a camera system which also monitors a public space does not amount to the processing of personal data in the course of a purely personal or household activity for the purposes of that provision.[25] In other words, a video recording made via a camera system installed by a person on their family home that captures public space is not exempt from the jurisdiction of the Directive on Data Protection (and thus nor from rules governed by the Act on Personal Data Protection).

In terms of the question of to what extent and by what means the privacy of the individual at whose dwelling the cameras point is protected, it is always necessary to take into account the specific circumstances of the case, of which there may be a whole range, and they can lead to a different assessment of the case or varying intensity of punishment. At issue for example is whether a publicly accessible place or private space is being monitored, what type of camera is being used (a real one or a dummy, with or without recording), what the reach of the camera is outside the own property (small or great distance from the property line), where the camera is pointed (most sensitive is the entrance or places where private life takes place), whether the actual situation can be verified, whether the controller is a natural or legal person, the reasons for which the public space is being monitored, and more.

In the case of processing of personal data of an individual ("data subject") by the controller, the Act on Personal Data Protection applies, so the data subject can claim the rights granted by the law (e.g. the right to access to data and rights to collected information), or they can alert the Office to the objectionable conduct so it can apply administrative procedures and sanctions contained in the act. In situations that are not cases of data processing, privacy can only be the subject of protection in civil proceedings on the basis of a court action for protection of personality under the Civil Code. In this regard however it is necessary to wait for potential court rulings, in particular judgments of the highest courts (Supreme Administrative Court or Supreme Court).

The Office informs the public as needed what the rules are for handling cameras. It is however worth mentioning that it is not always necessary to take the judicial route to resolve contentious matters. For example, a camera owner who, for specific serious reasons, intends to choose this solution to protecting their property can in advance ask the person concerned for their consent, potentially showing them the camera and dispelling their qualms that their dwelling is being monitored. Then the person concerned cannot claim they are being monitored or have

[25] Article 3 (2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that the operation of a camera system does not amount to the processing of personal data in the course of a purely personal or household activity fot the purposes of tha provision. The video recording capturing persons must however in such a case be stored in the form of of a continuous recording device installed by an individual on their family home for the purposes of protecting the property, healthy and life of the home owners, but also monitor a public space. it can for example be a hard disk.

the subjective feeling they are being watched, unless of course the essence of the dispute is about something else (neighbourly dispute). Owners of cameras (or dummies) should also be advised about alternative methods of securing their property. In many cases reliable mechanical security is more efficient, and can also be cheaper and more effective. They should also be informed that courts could potentially consider the affected person's feeling that they are the subject of systematic, continuous and identifying surveillance as an invasion of another's privacy. Safeguarding the privacy of individuals must therefore be given protection, the manner and means of which are determined by the specific circumstances of the case. OPDP cannot provide protection to the affected subject in all cases of camera surveillance; it can only act within the bounds of its jurisdiction as laid down by the law. In a situation where there is not yet sufficient case law on protection of privacy, it is appropriate for the Office to provide instructions on how to proceed as part of its public awareness activities. OPDP also assumed these conclusions in its discussion with the Ombudsman.

3. **Analysis of data transmitted during cancer screening in terms of personal data protection**

Cancer screening programmes represent an ambitious project in the field of protecting public health, their realisation stemming from the fact that cancer is a key problem in all EU Member States. This has led to support for adopting national cancer programmes and introducing cancer screening for the most serious forms of cancer. At the core is public support for using cancer data for public health research in order to prevent and treat this disease. Cancer screening programmes (screening for colon cancer, breast cancer and cervical cancer) have been systematically launched in the Czech Republic on the basis of the EU Council recommendation from 2003 on cancer screen and gradually implemented. This implementation is fully in the competency of national authorities.

Closely tied to the implementation of cancer screening programmes is the issue of protection of personal data. In this regard the recommendation cited above stipulates that all procedures for collection, storing, transfer and analysing of data in medical registers must be fully in line with the level of protection laid down by both Directive 95/46/EC and the relevant Member State legislation on management and processing of medical data (in particular with reference to Art. 8 of Directive 95/46/EC). Lastly, according to Art. 3 of the recommendations, monitoring must comply with the standards defined by the European Network of Cancer Registries. The creation and management of screen databases must therefore be in full compliance with the relevant legislation on personal data protection.

In the past (in 2011-2012) the Office has already dealt with the observance of controller obligations in connection with the collection and processing of personal data for the purpose of data administration in the monitoring of cancer screening programmes. It came to the conclusion that in such cases it is not personal data that are processed, but anonymous data.[26] *In connection with the ongoing evolution and refinement of the legal framework for personal data protection, a need arose to theoretically review the aforementioned conclusion in terms of compliance with the newest theoretical findings in the field of personal data protection*, e.g.

[26] Annual report of the Office for Personal Data protection from 2012, pp. 35–36.

the WP29 opinion on the issue of the concept of personal data,[27] the recent judgment of the EU Court of Justice on the case *Breyer vs. Bundesrepublik Deutschland*,[28] and potentially with the forthcoming General Data Protection Regulation (effective starting 25 May 2018).

In general it is the case that the Office reviews its earlier positions in the field of personal data protection in connection with preparations for the GDPR. This potentially also concerned the issue of processing data about patients as part of cancer screening, which ANA took up as a model case; see below.

A fundamental question in the above context during the new assessment was whether personal data are transferred as part of screening and whether this is personal data processing that is subject to the Act on Personal Data Protection. If the controller were to receive anonymous data and work only with such, there would be no processing of personal data. Another fundamental question which was necessary to post in terms of the current understanding of the definition of personal data in the context of the Court of Justice judgment on the Breyer case, was the issue of identification of personal data, i.e. whether it is possible to place the data transferred to the controller into such a context so as to lead to identification of the data subject. In other words - whether they are personal data that can be identified indirectly.

Naturally however such questions could not be resolved merely in theory. Though it is necessary to draw on the relevant legislation, opinions and case law in order to evaluate them, one must also draw on knowledge of in what particular manner the transfer of personal data from medical facilities via screening centres to the controller takes place. The Office does not have any current findings from supervisory activities at this time. It could therefore only draw auxiliarily on earlier inspection findings. In connection with the shift in the field of personal data described above, in such a situation OPDP would gravitate toward the conclusion that the transferred data on examinations should be considered personal data.

Such a conclusion would of course theoretically mean that the legal treatment of personal data protection must be applied to the activity of the controller of personal data obtained during cancer screening programmes. The data subjects would thus be guaranteed exercising of their rights (access to data) and a higher level of protection of personal data and privacy of data subjects would be ensured, as the demands for ensuring greater security of such data against accidental leaks and possible misuse would be placed on the data controllers. At the same time it is evident from the public accessible sources that certain measures ensuring a higher level of personal data protection have already been applied in the area under consideration. These include for example application of the principles of *privacy by design*, which can be observed in the use of encryption or the logical partitioning of the data space. Further options in relation to personal data protection will be expanded by implementation of the General Regulation.

[27] Evidently this is the Opinion of the Article 29 Data Protection Working Party No. 4/2007 on the concept of personal data of June 2007.
[28] Case C-582/14 Patrick Breyer v Bundesrepublic Deutschland of 19 October 2016.

Legislative Activities

General

In 2017, OPDP focused primarily on implementation of the new EU regulatory framework for personal data protection (GDPR, JHAD & PNRD), which is the subject of a special chapter of the annual report.

For drafts of other legislation the Office is a mandatory comments site. Unfortunately it is systematically ignored by certain ministries whose proposals have a significant impact on protection of privacy.

Since 1 January 2013 OPDP has been monitoring Data Protection Impact Assessments (DPIA).[29] Unfortunately even after four years of practice, the form of the DPIA is not optimal. Certain departments repeatedly state untruthfully that "the processing of personal data shall not in any way infringe on protection of privacy".

One of the most important bills that the Office commented on as part of the legislative process was the draft bill for the Act on a Census of People, Buildings and Flats in 2021. The bill envisages maximum use of existing administrative sources of data and minimum burden on respondents, as the primary method of data collection from field investigation will be an online census. OPDP brought comments to bear on the specification of personal data and their further usage.

EU law

In light of the quantitative change in EU regulation and its influence on the Czech rule-making process, the importance of the EU legal order has grown. The Office has reacted to this by adding the active monitoring of EU legal regulations (Directives and Regulations) to its scope under the Ministerial Coordination Groups (MCG) as of 20 March 2017. These serve to draw up Czech positions for the negotiations of the working parties of the Council of the EU, i.e. the Council of Ministers of Member States. Output is confidential, and thus most information about it cannot be disclosed.

[29] The obligation under the government's legislative rules will now be a legal obligation under - Article 35 of the GDPR.

As of 1 January 2018, OPDP is incorporated into the MCGs of the Ministry of Finance, Ministry of Industry and Trade, Ministry of Justice, Ministry of the Interior, Ministry of Health, National Cyber and Information Security Agency, Office for Standards, Metrology and Testing, and the Office of the Government. Aside from the priorities described below, the Office dealt in greater detail with the fields of justice and the interior, in particular the draft regulations ECRIS-TCN, EURODAC, ETIAS and PNR.

Electronic privacy

The proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications (CELEX: 52017PC0010) has the English abbreviation ePrivacy or ePR and is to replace the existing Directive 2002/58/EC. The General Regulation has a supporting scope for this proposal.

Currently, ePR has already been approved in the European Parliament. Discussion is not as rapid in the Council of the EU; the original expectation that ePrivacy would take effect alongside the GDPR, i.e. 25 May 2018, is not technically possible anymore.

The coordinator is the Ministry of Industry and Trade. The proposal is highly controversial and being closely monitored by the professional community. At issue in particular are cookies, browser settings, data retention and machine-to-machine communication. The Office draws on the positions of the EU data protectors: WP29 and the European Data Protection Supervisor. It has focused primarily on the issue of direct marketing, spam or unsolicited calls, which are dealt with the most in the supervisory authority's practice.

Data retention

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 20016 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC was overturned by the ECJ judgment *Digital Rights Ireland* v Ireland, case no. C-293/12. For this reason the EU is preparing a new regulation on preventive retention of traffic and location data in telecommunication while respecting the ECJ judgment *Tele2 Sverige AB v Post-och telestyrelsen*, case no. C-203/15, prohibiting the blanket retention of data of EU citizens. The solution is therefore retention of data in specific and justified cases, while in other cases the police is to make use of data that telecommunications operators have for their own needs. The coordinator is the Ministry of the Interior.

Free movement of non-personal data

The proposal for a regulation on the free flow of non-personal data (CELEX: 52017PC0495) hopes to achieve information exchange that is not limited by borders. The coordinator is the Office of the Government. Neither corporations nor Member States should be allowed to demand retention of non-personal data in a single State aside from security exceptions. This should guarantee the competitiveness of the European data economy. OPDP pointed out here that in practice it will be difficult to distinguish between personal and non-personal data and that a data set that contains even a single piece of personal data is a set of personal data.

Implementation of the new EU regulatory framework for personal data protection (GDPR, JHAD and PNRD)

As coordinator the Ministry of the Interior submitted a draft Act on Personal Data Processing (APDP) for interministerial comments proceedings. The essence of this is adaptation of the Czech legal code to the GDPR, transposing JHAD[30] and reflecting the commitments of the Council of Europe Convention No. 108, for the Protection of Individuals with regard to Automatic Processing of Personal Data. OPDP is co-coordinator.

The APDP is to replace the existing Act No. 101/2000 Coll., on Personal Data Protection and Amending Certain Acts. Amending this law due to the need to implement secondary EU legal regulations has shown itself to be highly impractical in light of the major extent of changes. The provisions that relate to the competence of the Office are copied into the APDP from the Act on Personal Data Protection. The structure is however changed: the APDP no longer counts on the function of inspectors.

The Interior Ministry is also the coordinator for a bill amending certain acts in connection with the adoption of the Act on Personal Data Processing - an accompanying act to the APDP. The co-coordinator is the Ministry of the Transport. The essence of the draft accompanying act is transposing the PNRD[31] along with sectoral changes induced by the General Regulation or JHAD, in particular in the financial and justice regulations. In the comments proceedings it was proposed that a total of 19 acts would be amended.

With the proposed legislation, Act No. 341/2011 Coll., on the General Inspection of Security Services (GIBS), will also be amended. GIBS is to also now have certain new powers similar to those of the police. These include the publishing of information by mass media, removal of a case, as well as access to a dwelling, other space or to a property.

The Office brought 24 comments to bear on the bill, of those 19 major ones and five recommendations, with the key comments concerning the scope of personal data processed by the Police of the Czech Republic and the public prosecutor's offices. For example, OPDP asked the proposing entity to justify why Czech Police records concerning digital photographs for the purpose of searching, detecting or punishing criminal offences are not to be used solely in connection with crimes. The Office also asked that the public prosecutor's offices process personal data solely to the extent corresponding to the task being performed.

Presentation of employees of legislation unit

In the first week of April 2017, the 20th annual ISSS conference took place - Internet in State Administration and Local Government. From the perspective of personal data protection, the focus was on the topic of the GDPR (General Data Protection Regulation). In his presentation, unit head Vít Zvánovec set out the goal of dispelling the excessive concerns over the General Data Protection Regulation among both the lay and professional public and emphasising the Office's message that the General Regulation is a case of evolution, not a revolution.

---

[30] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by comprtent authorities for the purposes of the prevention, investigation,detection or prosecution of criminal offencs or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[31] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention. detection, investigation and prosecution of terrorist offences and serious crime.

At the start of July 2017 the head of the legislative unit also attended a seminar at TAIEX on personal data protection in healthcare in Ankara. He gave a talk on the fight against communicable diseases, the reason being that this area is regulated in detail by EU legislation, so Turkey must adapt to it.

At the conference Czech Law and Information Technology in Brno, Daniela Havlíková presented. At the event she presented the Office's perspective on the proposed ePrivacy regulation. Her presentation met with a strong reception.

Preparation of the Office for implementing the General Data Protection Regulation

The impending force of the General Regulation will influence the Office's activities in a fundamental manner and put its ability to deal with new tasks to the test. In 2017 OPDP began working systematically with the Regulation, responding to questions from the public, providing information on its website and, depending on its staffing capacity, gradually providing for a broader range of activities in the preparation process (lecturing, consultation and methodological activities). The interpretation of the new legal framework is becoming ever more structured with new knowledge, for one thing based on the areas in which personal data protection is secured (e.g. banking, the non-profit sector), and for another based on the nature of the obliged entities (public administration, the private sector). Starting in the second half of 2017, one could speak of a certain targeted approach to the methodology of preparations in terms of activity external to the Office.

Familiarisation with the General Regulation, the GDPR, is also being offered by a large number of training and educational entities, in particular law offices and training agencies. Provided the professional qualifications for handling the issue of personal data are met, this manner of education cannot be objected to. The feedback OPDP has received however points to certain pitfalls in the services offered. In some cases, in reaction to the nervousness and uncertainty of the public concerning future obligations stemming from the General Regulation and the threat of fines, the aforementioned educational entities are meeting the current demand and giving rise to the impression that it is a complicated issue that must be provided for in the form of outsourcing.[32] They also often lack an unbiased appraisal of the essential role of protection of privacy and personal data in the digital age, relegating the issue of personal data protection to the role of "yet another EU regulation", or the manner by which the Regulation can be understood and applied on the basis of general principles is not sufficiently explained.

In the process of preparations for the Regulation, which it realises as part of its own awareness and educational activities, the Office thus opts for appropriate conceptual approaches and methods. The nature of the Regulation itself predetermines how to work with the rules for data protection. The point is that there is not and will not be a single universal manual, methodology or exhaustive guide on how to implement or apply the GDPR. For each entity the protection of personal data must be applied in a specific manner corresponding to the nature of the personal data processed and the internal functioning of the organisation. What is required for this is a detailed knowledge of both the area being analysed and the principles of personal

[32] Outsourcing means that the contracting entity sets apart various auxiliary and secondary activities and contracts them out to another company or subcontractor that apecialises in the activity in question. It is thus a type of "division of labour", but the activity is not provided for by the company's own employees, but on the basis of a contract for financial consideration.

data protection. It is also necessary to have one's bearings in related fields such as IT, cyber security, archival and record management, and others. Lastly, it is important to accept the fact that personal data protection is not stationary, but will react to the risks associated with the evolution of information technology. One must therefore count on the fact that continuous attention must be paid to the protection of personal data and its development must be monitored.

Aside from this it is important to emphasise that one of the main structural elements of the Regulation is the principle of responsibility of the controller or processor. In practice this means that if OPDP provides consultation to future controllers, it demands that they actively take part in preparing the consultations. Only they know the specifics of the field in which they operate, the nature of the inner workings at their organisation and activities they perform and are able to prepare summaries and analyses of the processed personal data and formulate potential questions based on this. This all requires a certain level of understanding of the issue of personal data protection. The Office considers this method of preparation to be effective. On top of this it prefers that a chamber, association, organisation or other entity get involved in preparations for the General Regulation in the given sector that can take into account the ethnical aspects of the area in question. This cooperation also forms an appropriate platform for further activities in the future (e.g. codes of conduct) or methodological aid provided to specific entities when protecting personal data in the given area.

As was already stated, the activity of OPDP in the area of specific preparations for the Regulation can roughly be broken down into lecturing, consultation and methodological activities, with each of these activities applying approaches that strengthen the active participation of involved entities in implementing the General Regulation. For example, in lecturing activities it is preferred that the competent central authority of state administration take active part in the case of the public sector, or a representative of an special interest or professional association in the case of a private entity. In terms of methodological activity in the field of personal data protection, the Office considers an active approach by the authorities under whose jurisdiction the methodological management of the given area falls to be essential (e.g. guidelines from the Ministry of Education in the case of schools or guidelines from the Ministry of Health meant for hospitals). In such cases OPDP is not adverse to collaborating in the form of consultation, but it cannot stand in for the conceptual and methodological activities that behove the individual state authorities.

Last year specifically Office employees provided for or took part in a total of 86 free lectures around the country. Special attention was given to entities whose activities in some way contribute to the public interest, e.g. municipalities, professional associations, churches or non-profit organisations. Attention was also given to small and medium enterprises. A specific example of well-managed collaboration was the series of lectures for municipalities organised by the Union of Towns and Municipalities, which both OPDP and the Interior Ministry helped with.[33] The passing on of theoretical knowledge was in this case accompanied by the gradual creation of user-friendly methodological materials. Another example of inspiring cooperation were the interactive seminars organised by the Office for non-profits, e.g. the Salvation Army

[33] GDPR Academy, a long-term programme of seminars and swapping of experience organised by the Confederation of Industry of the Czech Republic with the professional support of the Office for Personal Data protection and experts from the Confederation of Industry, PRK Partners, IBM, KPMG andMasaryk University. See http://www.gdprakademie.cz/#o-akademii

of the Czech Republic. According to experiences of OPDP, proper explanation of the issue of the General Regulation leads to a reduction or elimination of fear of the new legislation, increases awareness and interest in the issue of personal data protection, and kick-starts work on implementing the GDPR.

The Office also considers it necessary to emphasise that personal data protection, in the public sector especially, should be provided for by organisations' own employees instead of making use of outsourcing. Solutions using organisations' own employees have multiple benefits for them. One of them is that core employees generally know the internal situation in the organisation well, they can take part in preparing internal regulations and in case of need they are easily accessible. This solution is also generally cost-effective compared to the financial burden of outsourcing.

It does not pay to underestimate preparations for implementing the General Regulation. Particularly in the period leading up to the Regulation's effect, it is good to consider activities related to personal data protection as a priority.

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

The provisions of Section 175 of Act No. 500/2004 Coll., the Administrative Procedure Code, are an institution that serves to protect the rights of affected persons if the law provides no other means of protection that an appeal or other standard or extraordinary remedial measures.

In accordance with Section 175 of Act No. 500/2004 Coll., affected persons have a statutory right of recourse to an administrative authority with a complaint if they believe an administrative authority has acted improperly. Under the cited provision they also have the right of recourse to an administrative authority with a complaint about improper behaviour by public officials.

The Office had to deal with complaints under Section 175 of Act No. 500/2004 Coll. in 2017 as well, handling a total of 34. In the majority of cases the complainants expressed disagreement with the handling of their prior submission in which the complainant raised suspicion of unlawful handling of personal data. Of the total number of such complaints, four were found to be justified and seven as partially justified. The remaining 23 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 remained practically unchanged.

Twenty-three complaints focused on the actions of the Public Relations Department, whose task is to deal with complaints and tips addressed to OPDP. 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 Section 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 14 complaints as groundless, four as justified and five as partially justified. 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 unit to launch administrative proceedings for suspicion of an administrative offence or misdemeanour.

In eleven 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 total, one complaint was assessed as partially justified and ten as 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.

In all cases the relevant Office section was informed about the handling of the complaint. 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.

Of the total of 34 complaints the Office received from complainants, not one targeted inappropriate conduct of public officials. It can therefore be stated that the Office is responsible 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

A priority for 2017 was active cooperation under the Article 29 Working Party (WP29). Aside from regular attendance of the plenary sessions, the Office has expanded its representation in the working subgroups, to which it sent out its representatives. This comprised six specialised working formations:

- Cooperation subgroup
- Technology subgroup
- Key Provisions subgroup for Directive 95/46
- Borders, Travel and Law Enforcement subgroup
- International Transfers subgroup
- E-government subgroup

The individual delegates are involved for example in producing guidelines and opinions meant to serve primarily for controllers and processors as an aid to prepare for the General Data Protection Regulation. For the majority of the materials issued from this series OPDP procured its own Czech translations shortly after their official publication. The goal was for the texts to reach as broad a range of interested parties as possible. These were the following specific materials:

- Guidelines for determining Lead Supervisory Authority of controller or processor
- Guidelines concerning Data Protection Officers
- Guidelines on the right to "data portability"
- Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679
- Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

- Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679
- Guidelines for Personal data breach notification under Regulation 2016/679
- Guidelines on Consent under Regulation 2016/679
- Opinion 2/2017 on data processing at work

For most of these documents the European Commission later produced its own translations into national languages. To distinguish the official versions from the translations procured by the Office, the Czech term "vodítka" was used for the unofficial working versions in contrast to the official term "pokyny".

At the end of spring, OPDP was visited by a delegation of Serbian colleagues, who were primarily interested in issues of protection of data and privacy in relation to the use of modern technologies (camera surveillance, protection of privacy on the internet, conducting inspections in these areas).

Shortly thereafter the management of the Japan's Personal Information Protection Commission expressed an interest in visiting the Office. The meeting took place in June, with the primary interest of the Japanese officials being in the General Data Protection Regulation and its impact on the activity of supervisory authorities.

As it does every year, OPDP sent its employees to various international conferences and professional seminars. The priority was events that take place regularly, such as the spring conference of data protection commissioners or the meeting of representatives of authorities from Central and Eastern Europe. In general, in the year in question a limited number of trips to seminars and conferences took place in favour or attending working sessions abroad. Due to the Office's competencies or in connection with efforts to develop activities in international working groups, attendance of such events tends to be required.

OPDP intends to approach the dispatching of its employees on foreign trips with a similar philosophy in 2018 as well.

A specific topic of recent years has been the Privacy Shield programme. By decision of the European Commission, this ensures adequate protection of personal data transferred to the United States of America to companies that have committed to upholding the principles contained in Annex II of the Decision on the adequacy of the protection provided by the "EU-US Privacy Shield" of July 2016. A list of companies participating in this programme is kept by the US Department of Commerce www.privacyshield.gov.

In September 2017 the first annual review of the Privacy Shield took place, attended on behalf of the European party by a team made up of representatives of the European Commission and WP29. On 28 November this latter issued, alongside the European Commission's report, its own report on the results of the annual review. This report notes the marked improvement the Privacy Shield has brought about compared to the revoked Safe Harbour, particular in terms of supervision of the US Department of Commerce over the certification process for individual programme participants. The WP29 report also enumerates areas where it is necessary to work on further improvement: guidance for companies and transparency for European data subjects, shortcomings in supervision over fulfilment of the principles on the part of companies, the issue of interpretation of the special regime for employee data, the problem of automated decisions and profiling.

In terms of the access of US intelligence authorities to personal data transferred from the European Union to the United States, the WP29 report states that the claims of the US side that there is no blanket access of intelligence authorities to the transferred personal data are not backed by any legally binding documents. At the same time it is not possible to rely on the new report from the understaffed Privacy and Civil Liberties Oversight Board (PCLOB).

For this reason WP29 calls on the European Commission and the competent authorities of the United States of America to renew talks on this matter. It also calls for the US side to rapidly fill the position of Privacy Shield Ombudsperson and the unfilled positions at PCLOB. At the same time the internal procedural rules for discussions between the Ombudsperson and the intelligence authorities should be declassified.

The Office, Media and Communication and Tools

From a media perspective the past year of 2017 was marked by several notional climaxes and one central topic, which wove its way through all twelve months.

In the first quarter the interest of media was focused on the traditional competition “My Privacy! Don't Look, Don't Poke About!" This was its 11th year. Celebrations for the international Data Privacy Day also attracted attention in the media. They included a discussion meeting with Office President Ivana Janů, as well as a presentation for regional authorities with a follow-up discussion on the topic of personal data protection, which elicited considerable interest among the hundreds of attendees.

The utterly dominant topic however was, since the start of the year, the impending entering into force of the General Data Protection Regulation, also known under the acronym GDPR.[34] The Office therefore devoted considerable attention to it from January on. At the level of the central government the Office President reached out to the individual ministers with an offer of assistance in preparing for the General Regulation, drawing particular attention to the obligation to set a Data Protection Officer (DPO). The Office organised a seminar for representatives of the ministries, and prepared further professional events for other central authorities and the organisations they run or fund. OPDP representatives also visited secondary schools with talks.

In 2017 the Office also joined in the celebrations of Safer Internet Day. The goal was to support safer and more responsible use of the internet and online technology, particularly by children and young people.

Another important event in the first half of the year from the perspective of the Office and the media was a conference on the General Regulation entitled GDPR 360°, which was intended for representatives of state administration,

[34] Regulation (EU) of the European Parliament and of the Council2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

corporate lawyers, data protection experts and company owners and executives. This too was kicked off in person by Office President Ivana Janů.

Pursuit of greater awareness in the field of personal data protection and preparation for the entering into force of the General Regulation were also behind the launching of work on publishing unofficial translations of the WP29 documents in the first half of the year. These allowed the public to become acquainted better and more quickly with the individual parts of the Regulation.

In the first six months the media took an intense interest in topics such as the use and publishing of police camera recordings, liability for disseminating commercial communications, and the record fine imposed for spam of CZK 4.25 million.

At the end of the first half of the year, OPDP officially announced the winner of the competition “My Privacy! Don't Look, Don't Poke About!”, with a record number of submissions, surpassing the previous maximum from 2009.

Even in the second half of the year, interest of the national and regional media on the topic of the GDPR did not let up. Resonating quite strongly in the media was the court battle lost by the MAFRA publishing house, which had submitted an action against the Office for the fine imposed for publishing private telephone conversations between former PM Petr Nečas and his wife Jana Nečasová (formerly Nagyová). OPDP encountered even greater media interest in the case of the inspection of the electronic registration of sales system that it included in its inspection plan. The same interest can be spoken of in the case of an inspection launched on the company Internal Mall.cz, a.s. This came as a result of a hacker strike on almost 750 000 pieces of client data.

At the end of the year the media took an interest in the topic of the publishing of salaries of public officials, on which the Constitutional Court also commented. Specifically at issue was the Office’s position emphasising the necessity of very carefully considering all invasions of privacy.

Through the end of the year OPDP continued to publish further guidelines as part of the documents issued by WP29 and continually worked on unofficial translations of other texts.

MEDIA IMAGE

For a long time the Office did not enjoy much media favour. The reasons can be seen in some of its decisions to impose a fine, to which journalists were constantly returning due to drawn-out court disputes, but also in the specialisation on personal data protection itself. The Office’s professional work requires time to deal with tips, which goes against current media trends, which present all news on the Office at ever greater speed and oversimplification.

A significant shift in the relationship between the media and OPDP could be observed in connection with the speech of Office President Ivana Janů on the ekolo case and the Office’s subsequent statement on the case of the municipality of Kravaře. This new approach, under which a fine would probably not have been imposed in either the ekolo or Kravaře case, was a strong signal for the public that a gradual evolution was taking place in the decision-making of OPDP, distinguishing it from the practices of the former leadership.

This change in approach under the current leadership, which aims to make the Office more helpful to the public and assess particular cases individually, has met with a very positive response on the part of the media.

OFFICE LIBRARY

The Office Library holds 2400 volumes, which is a year-on-year increase of roughly a hundred volumes compared to 2016, of which one was a donation.

In the first half of the year the library space fulfilled its standard function, which is as a resource for employees, to whom the publications necessary for their work were available. It also served the professional public however as a reference. Operations in the second half of the year were however strongly influenced by planned renovations, with the space also having to act as a large conference room. For this reason it was decided that the library would be moved to a separate space that better corresponds to its purpose.

OFFICE WEBSITE

The website remains among the core communication tools of the Office. Through its internet presence OPDP informs the public primarily about its activities and legislation on personal data protection. It follows from the above that one of the main topics for the Office in 2017 was preparation for the General Regulation, which was strongly reflected in modifications to the website's layout. Significant changes were made to the home page, where highlighted links to the individual parts of the new GDPR section were inserted. The goal was to facilitate orientation of page visitors, the interest of whom on this topic constantly grew towards the end of the year. With their own links on the home page for example are thus a basic guide on the GDPR, frequently asked questions and answers on the General Regulation and the guidelines of the WP29 Working Party.

The new GDPR (General Regulation) section was mentioned, having been created by reworking the section on the EU General Regulation, where information on the General Data Protection Regulation was collected. Over the course of 2017 however the section gained a clearer structure and new sub-sections. Office experts personally produced the content of most of them. In particular this is true of the clarification of the role of the Office under the GDPR, the basic twelve-point guide, as well as the frequently asked questions and answers on the General Regulation and the "ten commandments" of errors or misleading statements. With these changes the Office aimed to simplify access to important information on the GDPR for the broad professional and lay public.

ODPD continued to devote increased attention to certain sections on its website. Case law contains decisions of Czech and international courts relating to the field of personal data protection. Supervisory activity is the cornerstone of the Office's mission. In this section visitors can find a summary of detailed information on inspections.

In 2017 a mobile version was added to the website, increasing the availability of its content.

Information System ORG

Act No. 111/2009 Coll., on Basic Registers, and its amendment by Act No. 100/2010 Coll., brought the Office a new task: To create an ORG information system by 30 June 2012 as part of the system of basic registers, which is to provide for processes associated with identification of individuals and the security of their personal data.

The point of incorporating the ORG information system into the system of basic registers is to protect the identity of citizens against misuse of their personal data. ORG is the only institution that can transport agenda identifiers from one agenda to another.

Thus since July 2012 the system of basic registers has been collecting and storing basic information on individuals.

The ORG information system in the system of basic registers is realised under the Integrated Operational Programme, priority axis Modernisation of Public Administration - Objective Convergence, assisted area Development of Information Society in Public Administration. The Structural Funds Department of the Interior Ministry approved it at the end of November 2009 and this year its five-year sustainability ends.

In 2014, Act No. 181/2014 Coll., on Cyber Security, was adopted along with implementing Decree No. 316/2014 Coll., on Cyber Security. At the same time, Government Order No. 315/2014 Coll., on the Criteria for Determining Elements of Critical Infrastructure, came out, supplemented by Government Resolution No. 390/2015 on the 2nd Update to the List of Critical Infrastructure Elements whose Operator is an Organisational Unit of the State.

The ORG information system in the system of basic registers was identified as an information system of critical infrastructure and is part of e-Government.

This designation places extraordinary demands on the technical equipment and security of the workplaces where ORG is located. The demands for perfection and work procedures in maintaining the system, updating it and introducing new functions and expansions are also high. Each module and function must undergo arduous testing in the development and testing environment of the ORG system. For this reason the requests for links to information systems are recorded into all environments of the ORG system nearly every day.

At the recommendation of the National Registers Authority for ISMS certification under ČSN/ISO 27001:2014 under the individual registers, OPDP as the administrator of IS ORG, decided to carry out ISMS certification for IS ORG. This certification is meant to confirm that IS ORG meets the requirements and demands for ensuring information security.

The activities of the ORG unit focused on fulfilling this recommendation for a substantial part of last year, being in the sign of ISMS certification for IS ORG.

A part of the certification process for example was inspecting the directives for managing access to the data centres, operating procedures, security policy, register of risks and assets, recovery plan, etc.

The instruments for monitoring access to the system were set up and fine-tuned. These instruments report and register likely and actual cyber attacks on IS ORG.

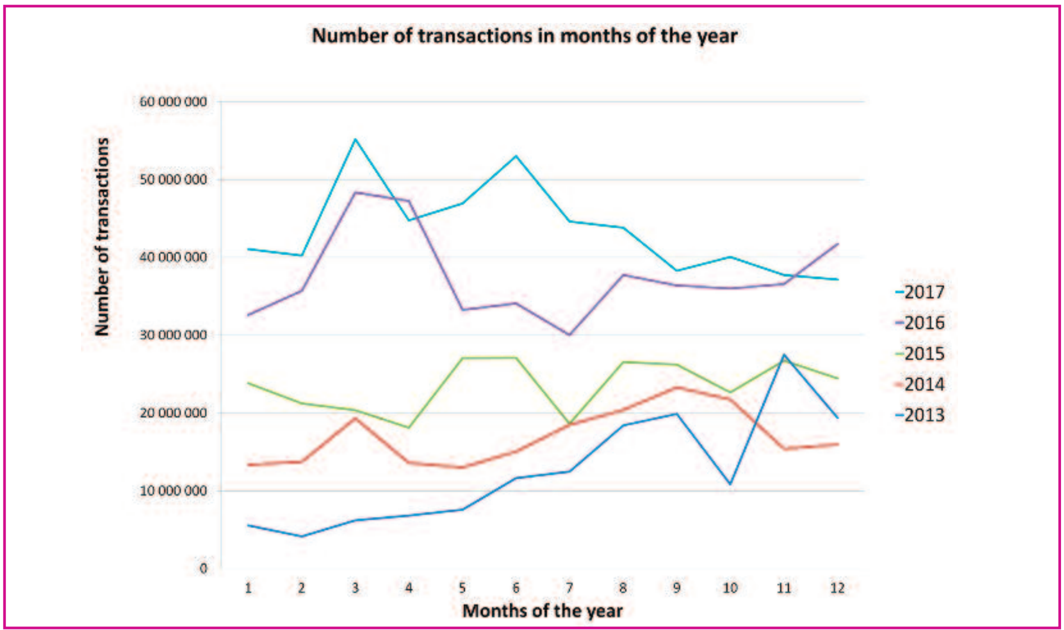
At the start of November 2017, a security audit focused on IS ORG traffic took place at the Office's headquarters. This followed up on a previous audit from 2016, which awarded OPDP a certificate under ČSN ISO/IEC 27001:2014 for IS ORG.

The operation of the system itself saw no significant interruptions in communication and dat availability.

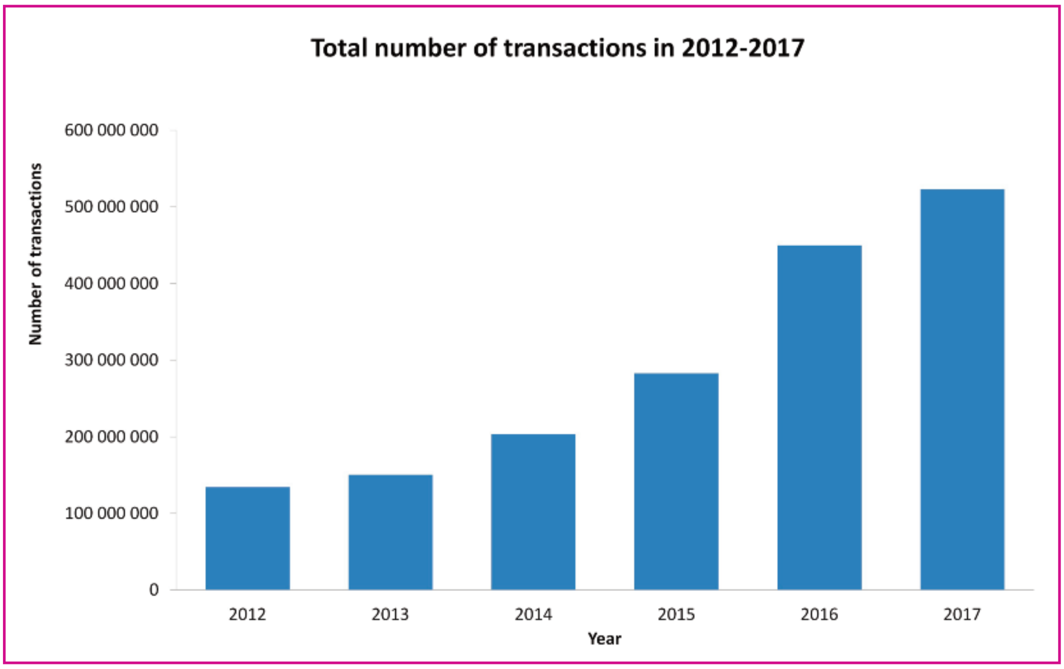
There are 403 agendas registered in the system. This means that the system is used in 403 areas where a resident can encounter them on a daily basis. These contain nearly all areas of human interest. From the field of human tissues and organs, to copyright, through to the course of service of reserve soldiers.

Unlike in previous years, the transition from 2016 to 2017 went smoothly without a sudden leap or drop in the number of transactions between December and January.

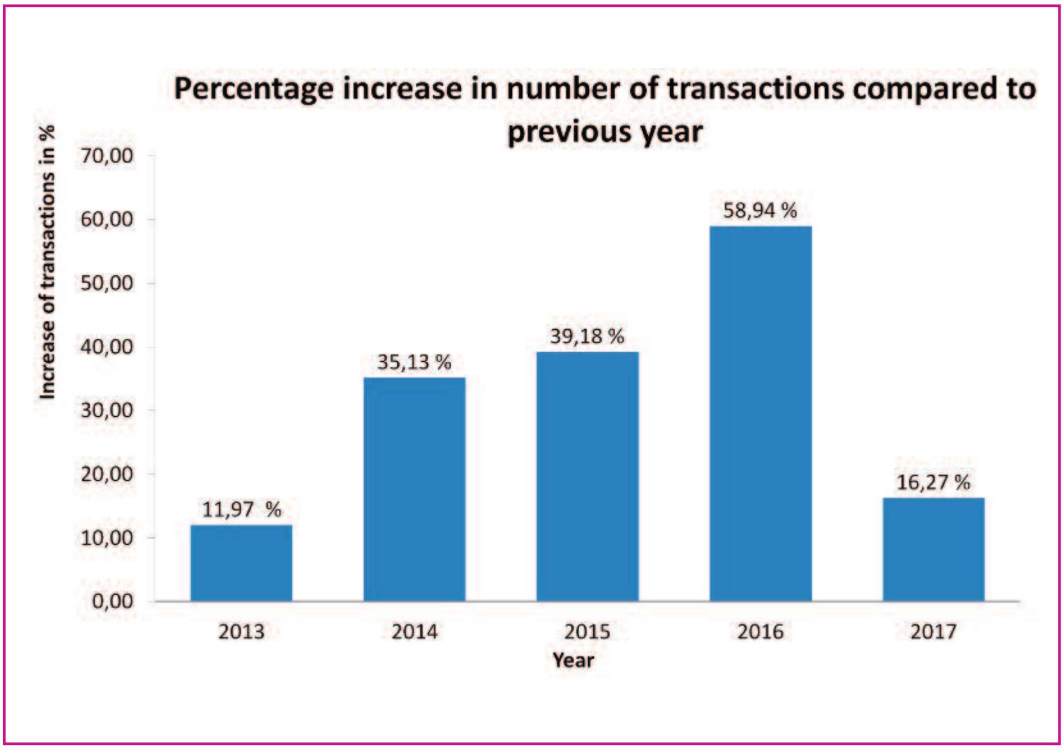
In the graph "Number of transactions in the months of the year" one can see the almost traditional March peak, which has been much more pronounced since 2016 than in 2013, 2014 and 2015.



The expansion and use of the system of basic registers is evident from the graph "Total number of transactions in the years 2012–2017". The greatest increase in number of transactions was in 2016, namely 166 779 679 transactions.

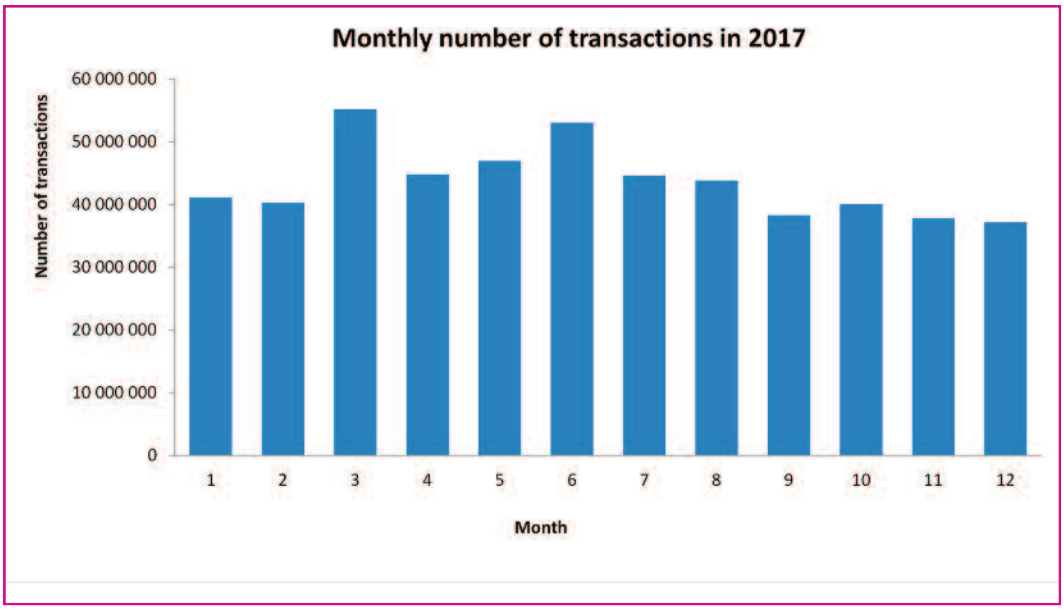


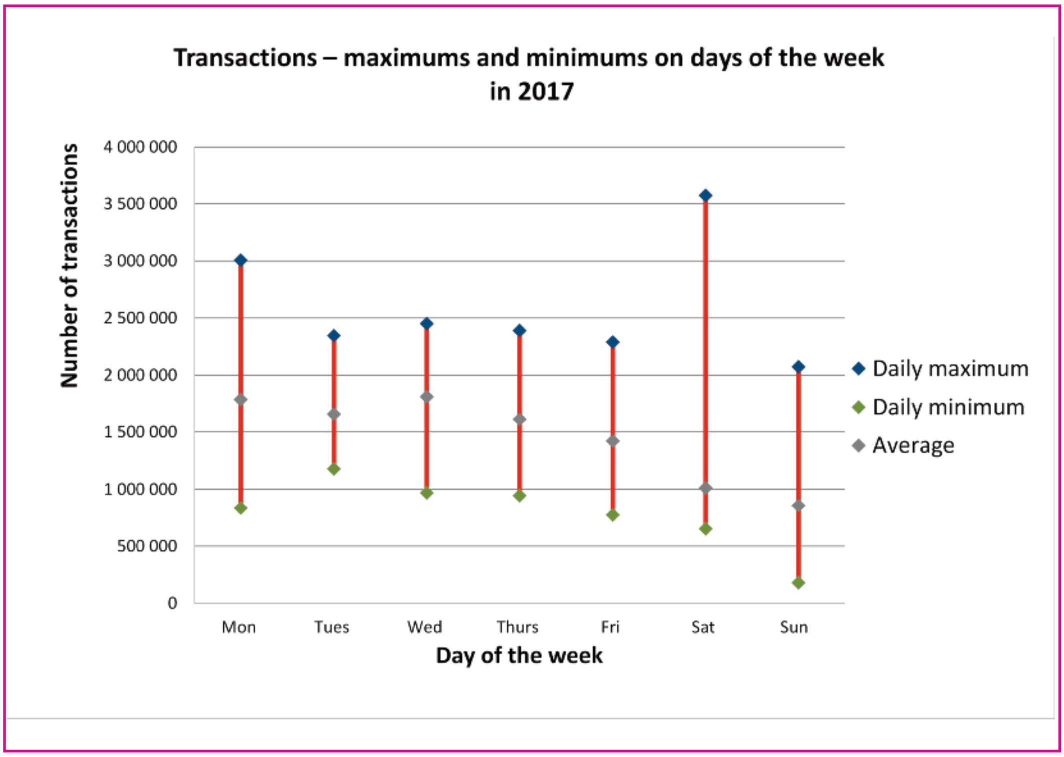
A depiction of the growth in number of transactions compared to the previous year in percentages is given in the graph "Percentage increase in number of transactions".



The distribution of requests to the system of basic registers over the course of the year can be seen in the graph "Monthly number of transactions in 2017". The maximum load was 10 June 2017 with a number of transactions of 3 573 612. The minimum was 19 August 2017 with a number of transactions of 654 069.

The next graph shows the load on the system during the week. Here the maximum and minimum values for number of transactions on each day are shown. It can be seen here that the maximum load on the system on 10 June 2017 was on a Saturday. In all likelihood this was due to maintenance of the databases and whole system.





Office Personnel

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

In 2017 the total number of systemised positions was 109.

Staff fluctuation in 2017 compared year-on-year over the previous year from 9.8% to 16.6%.

Individual processes of HR management at the office continued smoothly in connection with the development of the Civil Service Act and other relevant legislative changes.

At the start of 2017 a service evaluation of civil servants assigned to serve at the Office was conducted. Based on these evaluations one employee was assessed as adequate. No civil servant was evaluated as inadequate.

Six employees were brought in to serve, while 11 employees ended their se-rvice. Ten new employees were employed, with six employees terminating their employment.

Seven applicants were tested as part of the civil service exam for the field of service in "personal data protection" provided by the Office, of which six completed it successfully.

As of 1 January 2017, the records showed 99 employees at the Office; as of 31 December 2017 this number was 100.

The average registered number of employees for 2017 was 98.5.

A further 34 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. Many of them have been 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 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 required even increase them. It allows its employees to visit language courses. Employees can then 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. In this way it supports their interest in the issue of personal data protection while at the same time seeking out new potential employees.

Breakdown of Office Employees by Age and Sex – as of 31 December 2017

Whole set	men	women	total
up to 20	0,00	0,00	0,00
from 21 to 30	6,00	4,00	10,00
from 31 to 40	5,00	12,00	17,00
from 41 to 50	7,00	11,00	18,00
from 51 to 60	13,00	20,00	33,00
61 and over	13,00	9,00	22,00
Celkem	**44,00**	**56,00**	**100,00**

Breakdown of Office Employees by Education and Sex – as of 31 December 2017

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	2	4
L – Technical complete secondary + vocational certificate	1	2	3
M – Complete technical secondary	3	14	17
N – Higher technical education	0	0	0
R – Bachelor's	0	1	1
T – University	37	34	71
Total	**44**	**56**	**100**

Economic Management of the Office

The Office budget was approved by Act No. 457/2016 Coll., on the State Budget of the Czech Republic for 2017.
Drawing of state budget under Heading 343 – Office for Personal Data Protection

in CZK thousands

Summary indica	
Total income	1 394,27
Total expenditures	153 794,88
Specific indicators – income	
Total non-tax. capital income and accepted transfers	1 394,27
of which: total income from EU budget not including CAP	0,00
other non-tax and capital income and accepted transfers in total	1 394,27
Specific indicators – expenditures	
Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	153 794,88
Cross-sectional expenditure indicators	
Employee salaries and other payments for work performed	56 666,97
Mandatory insurance premiums paid by the employer*)	19 092,86
Contribution to the Cultural and Social Needs Fund	1 106,64
Salaries of employees in an employment relationship except those in service positions	11 029,90
Salaries of employees in service positions under the Act on Civil Service	34 063,10
Salaries of employees derived from salaries of constitutional officials	10 089,05
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		13 736,90	

*) 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 2017.The income budget for Heading 343 – Office for Personal Data Protection was fulfilled with an amount of CZK 1 394 270.

This primarily concerned:
- 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 relating to 2016 (payment of remainder of deposit account for paying salaries and contributions to the Cultural and Social Needs Fund for December 2016).

2. Expenditures

Expenditure drawing of CZK 153 794 880 includes:
- all costs for salaries and associated expenditures,
- capital expenditures associated with the Office building, renewal of information systems, both for the Office itself and the IS ORG,
- other 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 and maintenance,
- expenditures associated with non-investment purchases.

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

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 76 866 480 corresponds to the qualification structure and meeting of the employee plan.

As of 31 December 2017 there were **100 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", and Programme 043V10 “Development and Renewal of Material and Technical Base for Office for Personal Data Protection from 2017” a total of **CZK 13 736 900** was drawn.

Overview of budget drawing in 2017

Budget structure type	Name of indicator	Approved 2017 budget in CZK thousands	Final 2017 budget in CZK thousand	Reality as per accounting statemens as of 31 December 2017 in CZK thousands	Actual final budget in%
2211, 2212, 2324, 3113, 4132	Other non-tax income	0,00	0,00	1 394,27	
	Total income	**0,00**	**0,00**	**1 394,27**	
501	Salaries	55 003,89	56 023,67	55 182,05	98,50
5011	Salaries of employees in employment relation-ship with exception of employees in servise	10 251,05	11 160,81	11 029,90	98,83
5013	Salaries of employees in servise positions under the Act on Civil Service	34 400,45	34 510,45	34 063,10	98,70
5014	Salaries of empl. derived from salaries of const.	10 352,40	10 352,40	10 089,05	97,46
502	Other payments for work performed	1 495,99	1 792,18	1 484,93	82,86
5021	Other personnel expenses	1 495,99	1 792,18	1 484,93	82,86
5024	Severance	0,00	0,00	0,00	0,00
503	Mand. insurance paid by employer	19 209,96	19, 657,39	19 092,86	97,13
5031	Mand. social security premiums	14 124,97	14, 453,96	13 997,85	96,84
5032	Mand. public health insurance	5 084,99	5 203,43	5 095,02	97,92
513	Purchase of material	1 576,00	1 900,80	1 693,38	89,09
514	Interest and other fin. expenses	65,00	50,00	27,21	54,43
515	Water, fuel and energy	2 110,00	1 712,00	1 593,60	93,08
516	Purchase of services	16 236,00	65 057,01	52 113,61	72,77

517	Purchase of other services	41 993,83	8 268,79	4 796,02	58,00
518	Provided deposits, principal, quarantees	480,00	480,00	0,00	0,00
519	Exp. assoc. w/non-invest, purchases, contributions	2 913,20	2 920,62	2 790,81	95,56
534	Transfers to own funds and in relation to bodies without full legal personality	1 100,0	1 120,47	1 106,64	98,77
5342	Transfers to Cultural and Soc. Needs Fund and soc. funds of municipalities and region	1 100,08	1 120,47	1 106,64	98,77
536	Other non-inv. transf. oth. budg. tax payments and other	11,00	12,00	10,24	85,33
542	Compensation paid. to pop.	90,00	170,00	166,63	98,02
5424	Compensation during illness	90,00	170,00	166,63	98,02
	Total current expenditures	**142 284,95**	**159 164,93**	**140 057,98**	**88,00**
611	Acquisition of fixed intangible assets	7 600,00	7 054,20	2 940,82	41,69
612	Acquisition of fixed tangible assets	9 800,00	13 822,10	10 796,08	78,11
	Total capital expenditures	**17 400,00**	**20 876,30**	**13 736,90**	**65,80**
	TOTAL EXPENDITURES	**151 648,58**	**180 041,23**	**155 189,15**	**86,20**

Numerical data used from reports drawn up as of 31 December 2017.

INTERNAL AUDIT

The internal audit plan for OPDP for 2017 entailed three audit investigations; over the course of the year the following audits were performed on the basis of notification letters and audit programmes:

01/17 Audit

Audit of accounting for trips by service cars

The objective of the audit was to check and evaluate the costs for individual vehicles owned by the Office in terms of 3E as per Act No. 320/2001 Coll., on Financial Control in Public Administration, as well as checking and evaluating the procedural method for requests for assigning a service vehicle, the approval thereof, usage and also in accordance with other records (travel orders, ride log, GPS records). Furthermore, a verification of the accuracy of reports in the ride log, starting and ending odometer readings, checking of annual summaries and individual accounting documents, accuracy of kilometre reporting in connection to the vehicle routs, inspecting the receipts for fuel during vehicle operation in light of the permitted and approved routes.

According to the investigations carried out during the audit, the procedures listed in the directive on car operation corresponded to the facts kept in the individual records relating to service vehicles, all tested operations were in line with the directive in terms of vehicle requests, vehicle assignment and returning. The information kept in the individual ride logs corresponded to the information on the travel orders of those persons who used the vehicles.

In terms of compliance with the 3 Es (economy, efficiency and effectiveness), no errors in the individual acts of vehicle maintenance took place.

It was found that the system of car operations is set up and functions properly and does not need to be interfered with. It is however necessary to re-evaluate the overall efficiency of operating six vehicles for the needs of the Office.

02/17 Audit

Audit of publishing of contracts in register of contracts

The objective of the audit was to evaluate the procedural method of publishing contracts in the register of contracts with a particular focus on whether no systematic errors are taking place in determining which contracts are to be published in the register of contracts; also checking whether contracts earmarked for publishing comply with the law, with a focus on the declared metadata, format of the attachment and information stated in the published contracts, as well as checking and evaluating the efficiency of the process of publishing in the register of contracts in terms of its connection to related processes at OPDP and checking whether any duplicate or superfluous activities are taking place.

The audit found that publishing in the register of contracts was introduced as a process when determining which contracts are to be published in the register there is no systemic or conscious violation of the law; in checking whether the contracts are published in accordance with the law it was found that no systemic violation of the Act on the Register of Contracts was discovered.

03/17 Audit

Audit of internal oversight system

The objective of the audit was to evaluate the situation in the audited area in terms of the adequacy and effectiveness of the internal oversight system and its compliance with the applicable legislation, in particular the relevant provisions of Act No .320/2001 Coll., on Financial Control in the Public Administration (hereinafter the Financial Control Act) and implementing Decree No. 416/2004 Coll. Also checking and evaluating the ability of the internal control system to determine, evaluate and minimise the operating, financial, legal and other risks arising in connection with the fulfilment of the approved plans and objectives of the Office in time (Section 25 (1) b) of the Financial Control Act). Also part of the audit was checking fulfilment of the recommendations from previous audits and proposing recommendations for remedying the determined shortcomings and eliminating possible risks in the OPDP environment.

The audit was completed with the statement that in terms of the internal oversight system, the internal regulations of the Office are in compliance with the Financial Control Act and the other generally valid legal regulations and in practice they fulfil the role the Financial Control Act lays down and orders in terms of the effectiveness of the internal control system, the internal oversight system properly fulfils the function laid out by the Financial Control Act.

The procedures governing oversight laid down by the Financial Control Act and implementing Decree No. 416/2004 Coll. are set up in accordance with these regulations at the organisation and are actually used in practice.

The Office's accounting system fully reflects and applies into oversight management procedures that are prescribed for the public sector by the Financial Control Act; all tested operations were realised in accordance with the signature rules.

The strategy for OPDP's auditing activity is focused primarily on the economic side, with the goal of achieving maximum economy. From a long-term strategy it focuses on risks (in accordance with the strategy of the Ministry of Finance) with the objective of catching them early and rapid minimising them.

Also drawn up were the following:

- Annual Office Internal Audit Plan for 2017
- Medium-term Internal Audit Plan for 2017-2018
- Summary Report on IA Activity for 2016 for the Office President
- Report on Results of Financial Inspections for 2016 as per Annex 1a to Decree No. 416/2004 Coll. for the Ministry of Finance

FINANCIAL STATEMENT

Approval of the final financial statement for 2017 and information on its transfer will take place by the standard deadline of 31 July 2018 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., OPDP 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 2017 a total of 30 requests for information were addressed to the Office concerning its jurisdiction. Information was provided in full in 24 cases. In three cases OPDP completely refused to provide the information and in three cases the information request was partially rejected. The reason for partial or complete rejection was the protection of the personal data contained in the requested documents, or the fact that it was a request for information that cannot be provided under Section 11 of Act No. 106/1999 Coll. on Free Access to Information. No complaint from the applicants was registered against the Office's procedure in refusing or partially refusing to provide information. In one case OPDP received a complaint on the form of information provided, which was dealt with by providing information to the applicant in the requested form, i.e. in a machine-readable format.

In their requests for information, the applicants focused primarily on the Office's decision-making and inspection activity, i.e. on the results of administrative proceedings (administrative decisions) and the results of inspections (inspection reports). OPDP also recorded an inquiry concerning its systemisation under Act No. 234/2012 Coll., on Civil Service, or the number of inspections conducted in recent years, including individual months and broken down by inspector.

The provided information was published in accordance with Section 5 (3) of Act No. 106/1999 Coll.

Annual Report of the Office for Personal Data Protection for 2017
Office for Personal Data Protection Pplk. Sochora 27, 170 00 Prague 7
E-mail: posta@uoou.cz Internet address: www.uoou.cz
On the basis of the obligations laid down by Act No. 101/2000 Coll.,
on the Protection of Personal Data, Section 29 d) and Section 36,
the Office published this annual report on its website in February 2018.

Editor: Mgr. Tomáš Paták, telephone no. 234 665 286
Editing: Mgr. Vojtěch Marcín
Graphic design: Eva Lufferová
Proofreading: Mgr. Eva Strnadová
Printing: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno
Published for the Office for Personal Data Protection by Munipress Brno, 2018

ISBN 978-80-210-8914-3