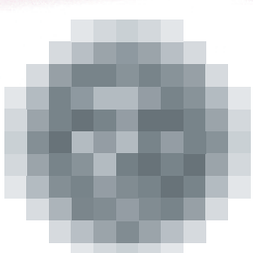
Annual Report Summary 2018



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-9224-2
ISBN 978-80-210-9225-9 (online: pdf)

Foreword by the President

Ladies and gentlemen,

You have just opened the Annual Report of the Office for Personal Data Protection for the year 2018, which for all of us here was dominated by the General Data Protection Regulation, widely known as the GDPR. In our interconnected and globalised world, this set of rules for the processing of personal data is becoming a global standard. Important economic partners of the European Union – the United States of America and Japan – are beginning to approximate it. This means one thing – that the principles and rules that the GDPR demands meet the needs of society and are also practicable in the diverse legal systems of democratic states. The Office takes part in fulfilling this standard not only with its "domestic" activities, but also through its thematically quite varied participation in the European Data Protection Board and further collaboration tied to this.

Our contribution to fulfilling the potential of the General Regulation is also connected to our involvement in audits in the mechanism of cooperation between the supervisory authorities of EU Member States, which are an important single point of contact for both data subjects and for controllers. Within this we twice found ourselves in the role of the lead supervisory authority.

Over the last two years we have been devoting a lot of energy to consulting and information support for those subject to obligations due to personal data processing – sometimes the only way is by debunking certain claims and advice. In this, as well as in our supervisory jurisdiction in the strict sense, the consent of subjects to data processing was the phenomenon of the year in 2018. This institution, which fulfils the constitutionally enshrined sovereign right of each person whose personal data are processed by someone else to be protected against unlawful activity, is very frequently misunderstood or abused. In the last year, this related in particular to what was called "re-consenting" which, with rare exceptions, was either completely unnecessary or even manipulative and helped form a distorted image of the GDPR. Here the Office naturally supports people affected by such an approach within the limits of its jurisdiction and, in addition to individual cases, has also helped them through an information campaign.

Preparation for the entry into force of the GDPR on 25 May and the anticipation of national adaptation legislation associated with continuous involvement left a significant mark on the year 2018 and thus also the content of this annual report. The Office's tasks do not however begin or end with the General Regulation. Protection of personal data is still "running down" under the Personal Data Protection Act, which as of the day when I am writing these lines continues to be an active part of the Czech Republic's legal code and fully applies for areas that are not covered by the GDPR.

The Office also upholds the protection of personal data under other laws. All forms of supervisory activity – from consultation to warnings to audits, administrative proceedings and issuing of fines – are brought to bear in the field of unsolicited electronically distributed commercial communications that the recipients legitimately perceive as a nuisance. Half of all fines handed out in the past year were for violations of the law in this area.

The Office also operates a significant part of the electronically conducted public administration in the Czech Republic, known under the acronym ORG, which is literally invisible to citizens, but which is of key importance for personal data protection in the public administration system. Within the basic registers, the ORG system contributes considerably to security and is of strategic significance.

The report that you have before will also inform you that the year 2018 was undoubtedly a breakthrough one for protection of privacy in the era of digitisation, which is omnipresent and is a constant focal point of the government's policy declarations.

I trust that these words will frame your picture of the work of the Office for Personal Data Protection in the last year.

Dr Ivana Janů
President of the Office for Personal Data Protection

Contents

THE OFFICE IN NUMBERS 2018 8

SUPERVISORY ACTIVITIES 11

I. SUPERVISORY PLAN 14
II. FINDINGS OF INSPECTORS FROM SUPERVISORY ACTIVITY 15
Leaking of personal data from HR files of the company CHRIST CAR WASH s.r.o. 15
Observation of the obligations of a controller by the company Lidl Česká republika v.o.s. 16
Internet Mall, a.s. – notification of security breach in management of personal data 18
INTER - IVCO, s.r.o. – observance of the obligations of a personal data controller 19
Inspection of mobile operator concerning consent request 20
Checking the sufficiency of personal data security at the General Financial Directorate (EET) 21
Processing of personal data in the CERD system at www.centralniregistrdluzniku.cz and www.cerd.cz (copying of public registers, publishing of false information, encroachment on private life and failure to inform data subjects) 22
Eltodo, a. s., - inspection of camera system in vehicles monitoring parking zones 24
Processing of client personal data during provision of loans by the company BNP Paribas Personal Finance SA, branch 24
Processing of personal data on the website of the company Mladá fronta, a.s. 26
Inspection of the company NaturaMed Pharmaceuticals s.r.o., concerning controller obligations 27
Regular inspection of the Schengen Information System 28
Prague City Hall Department of Transport Adminsitration – unauthorised divulgence of personal data to other data subjects 29
Mixing up of tax entities of the same name and data of birth by General Financial Directorate in delivering documents 31

OTHER SUPERVISORY ACTIVITIES 33

SUPERVISORY ACTIVITIES ON COMMERCIAL COMMUNICATIONS 33

COMPLAINTS, NOTIFICATIONS OF PERSONAL DATA BREACHES, AND CONSULTATIONS 37

IMPOSING OF SANCTIONS 40

FINDINGS FROM JUDICIAL REVIEWS 43

CERTIFICATION OF PERSONAL DATA PROTECTION 47

TRANSFERS OF PERSONAL DATA ABROAD 48

SCHENGEN COOPERATION 50

ANALYTICAL ACTIVITIES 54

LEGISLATION 64

HANDLING OF COMPLAINTS UNDER SECTION 175 OF THE CODE OF ADMINISTRATIVE PROCEDURE 69

INTERNATIONAL COOPERATION 69

CODES OF CONDUCT 71

MEDIA AND COMMUNICATION TOOLS 73

ORG INFORMATION SYSTEM 75

PERSONNEL 79

ECONOMIC MANAGMENT 81

PROVISION OF INFORMATION PURSUANT TO THE ACT ON FREE ACCESS TO INFORMATION 87

The Office in numbers

Questions and consultations	questions total	4161
	telephone consultations GDPR line	2800
	telephone consultations on camera systems	1900
	prior consultation pursuant to Article 36 of GDPR	0
	other consultations	20
Submissions and complaints	submissions received	3616
	dealt with by notifying controller of possible breach	462
	passed on for inspection or other proceedings	193
	matters passed on from criminal and administrative authorities	57
	notification of a personal data breach pursuant to Article 33 of the GDPR	260
	providing cooperation with criminal authorities	10
Supervisory activities (excluding inspections concerning unsolicited commercial communications)	commenced	76
	completed	89
	from previous years	36
	corrective measures imposed	28
	contested by objections	16
	objections upheld	2
	rejected	11
	partially upheld	3
	fines for failure to cooperate with inspection	4
	predealt with without commencing inspection (deferred, passed along)	27
Unsolicited commercial (communications (jurisdiction under Act No. No. 480/2004 Coll.)	total submissions	2901
	inspections commenced	22
	inspections completed	17
	from previous years	6
	contested by objections	5
	objections upheld	0
	rejected	5
	partially upheld	0

	sanction proceedings	26
	fines for failure to cooperate with inspection	10
	dealt with without commencing inspection by notifying entity of possible breach of obligations	414
Administrative punishment (with exception of proceedings concerning nsolicited commercial communications)	sanctions proceedings held with legal entities and natural persons engaged in business	39
	sanctions proceedings with natural persons	17
	waiving of fine under Section 40a of Act No. 101/2000 Coll.	38
	deferred	17
Decisions of the Office President	decisions contested by an appeal	25
	rejected appeals	22
	overturned and returned for new proceedings	7
	decision overturned and proceedings stopped	4
	change of decision	3
Judicial review (Note.: * *total since 2001*)	court actions submitted	8 (155*)
	actions rejected by court	1
	decisions overturned by court	4
	completed/uncompleted court proceedings since 2001	133/22
Permits for transfer of personal data abroad	applications for transfer of personal data abroad received (under Section 27 of Act No. 101/2000 Coll.)	3
	decision to permit transfer	1
	decision not to permit	0
	proceedings suspended on procedural grounds	2
Permits for transfer of personal data abroad	applications for transfer of personal data abroad received (under Section 27 of Act No. 101/2000 Coll.)	3
	decision to permit transfer	1
	decision not to permit	0
	proceedings halted on procedural grounds	2
Complaints under Section 175 of the Administrative Procedure Code	complaints received	12
	resolved as justified	2
	resolved as partially justified	0
	resolved as groundless	7
Requests under Act on Free Access to Information	requests received	56
	fully obliged	45
	partially rejected	7

	rejected applications	2
	requests for reimbursement for cost of exceptional information retrieval	2
	of those, number paid	0
Comments on drafts	planned laws	8
	acts	68
	implementing regulations	85
	draft government orders	17
	draft decrees	68
	non-legislative documents	63

Supervisory activities

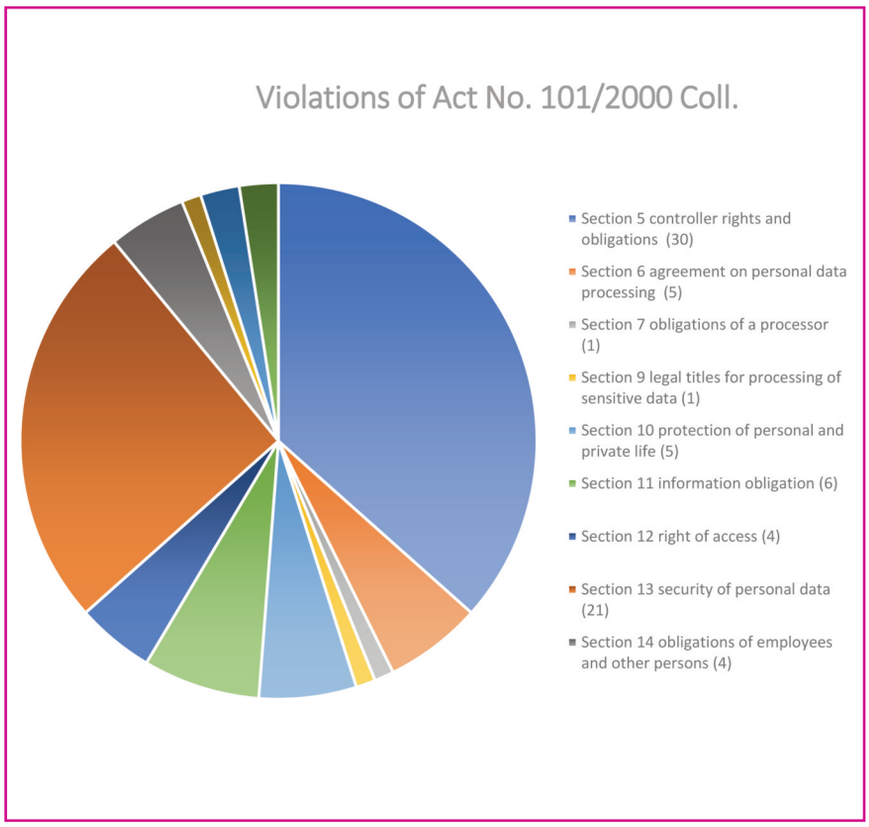
In 2018 the Office's supervisory activities were considerably impacted by the entry into force of the General Data Protection Regulation.[1] For the practical execution of supervision, this fact meant that the particular inspections over the course of the year took place under different regimes.

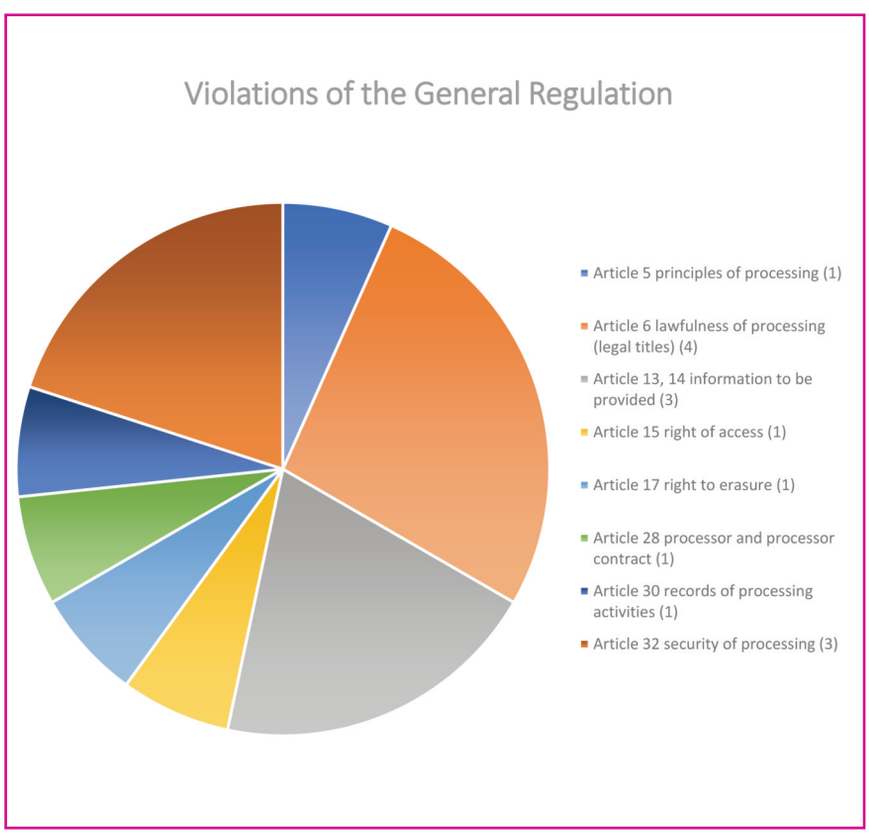
This primarily concerns inspections that were completed before 25 May 2018, i.e. before the General Regulation took effect. The facts found in these inspections were assessed solely according to the rules laid down by Act No. 101/2000 Coll.

The other main group were inspections that were carried out (even partially) once the General Regulation had taken effect. In these cases, the key factor for deciding which legal regime was used for the assessment was when the processing that was the subject of inspection took place. If processing that took place before 25 May 2018 was to be assessed, or an incident that occurred before this date, it was also judged primarily according to Act No. 101/2000. At the same time, however, the applicable provisions of the General Regulation were also taken into account where the inspectors found that they would have come to the same conclusions even if the regulation were already to be applied. In the case of differing conclusions, they provided a specific explanation of the differences. The last group of inspections were then those that were assessed solely in relation to the General Regulation.

The following graphs provide a more detailed overview of what specific violations of the individual provisions the Office found in the inspections conducted:

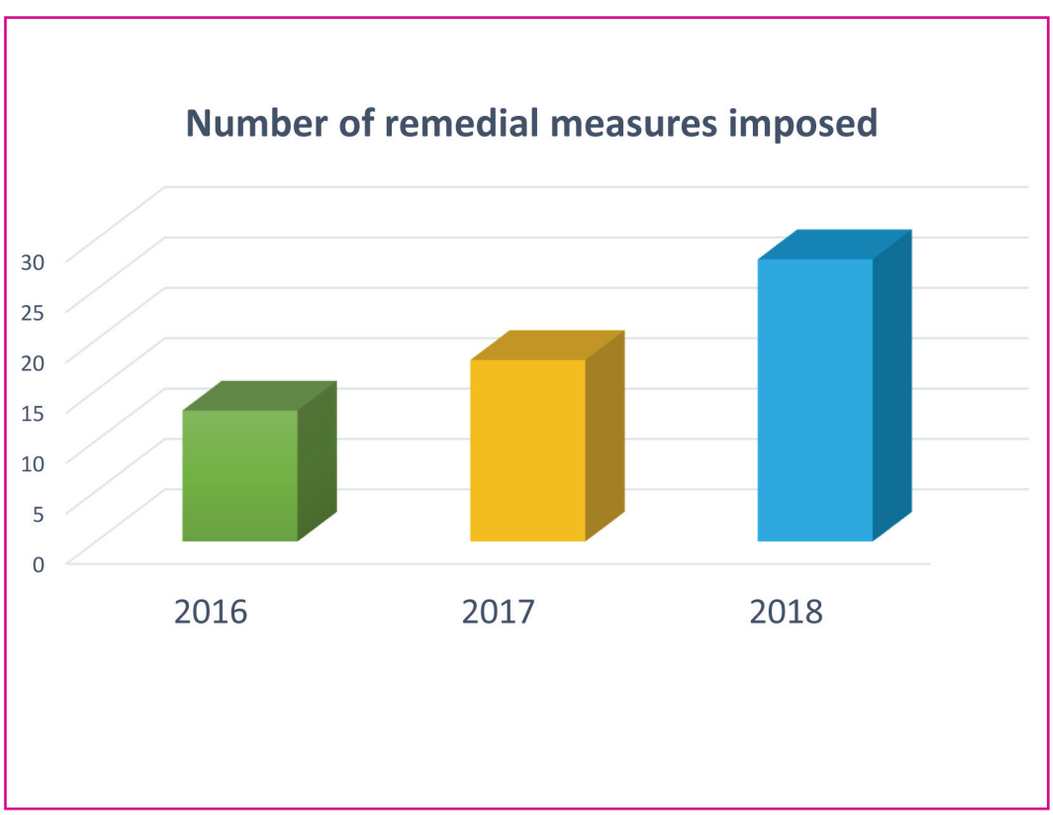
[1] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC).


Violations of Act No. 101/2000 Coll.
Section 5 controller rights and obligations (30)
Section 6 agreement on personal data processing (5)
Section 7 obligations of a processor (1)
Section 9 legal titles for processing of sensitive data (1)
Section 10 protection of personal and private life (5)
Section 11 information obligation (6)
Section 12 right of access (4)
Section 13 security of personal data (21)
Section 14 obligations of employees and other persons (4)


Violations of the General Regulation
Article 5 principles of processing (1)
Article 6 lawfulness of processing (legal titles) (4)
Article 13, 14 information to be provided (3)
Article 15 right of access (1)
Article 17 right to erasure (1)
Article 28 processor and processor contract (1)
Article 30 records of processing activities (1)
Article 32 security of processing (3)

Among other things, the General Regulation placed fundamental emphasis on cooperation between the supervisory authorities of Member States, which is meant to lead primarily to uniform assessment of conducted processing. Also part of this system is the "one-stop-shop mechanism" for cases of cross-border processing of personal data. Under this mechanism, one authority has the role of lead supervisory authority (the authority for the main or single establishment of the controller or processor) and other authorities can under certain conditions be "supervisory authorities concerned" (e.g. if the processing significantly affects data subjects based in the Member State of that authority). In terms of the inspections launched in 2018, the Office fulfilled the role of lead supervisory authority in two cases. As soon as these inspections have been completed, the Office will inform the public of the results thereof.

One of the basic tools, the goal of which (generally based on inspection results) is to rectify a situation that the inspection found to be a breach of the legal regulations on personal data protection, is the imposition of remedial measures. It must be emphasised that such measures are not imposed in cases where the relevant controller or processor rectifies the situation voluntarily in a timely manner. In such cases, proceedings to impose measures would not be cost effective, nor would they safeguard the rights of affected persons. With regard to the General Regulation coming into effect, it should be stated that no fundamental changes to the imposition of remedial measures took place compared to the process under Act No. 101/2000 Coll. The following graph shows the development in the number of remedial measures imposed over the last three years (note: one decision generally contains multiple remedial measures and the graph shows the number of measures imposed, not decisions issued).



• SUPERVISORY PLAN

The Office's Supervisory Plan was set up in 2018 to reflect the fact that significant changes to the effective legal treatment would be taking place before the first half-year was over. The commencement of individual inspections as per the Supervisory Plan was thus not determined by the particular quarters, as had been the standard previously, but by the legislation that was to be complied with for specific cases of processing.

The Supervisory Plan for 2018 included two inspections that the Office is obliged (on the basis of the applicable EU legislation) to conduct regularly. These are an inspection of the processing of personal data in the Customs Information System (CIS) and an inspection of personal data processing in the national part of the Visa Information System (VIS). The audit of VIS, along with the previously conducted inspection of the national part of the Schengen Information System (SIS) is also crucial in terms of the fact that in 2019 the Czech Republic is to undergo a "Schengen evaluation", i.e. an inspection of the functioning of the Czech national SIS, including the protection of personal data.

Findings from the Office's prior supervisory activities were also the subject of inspections carried out on the basis of the Supervisory Plan. For this reason (in connection with an inspection conducted on the company SOLIDIS s.r.o. and subsequent sanctions proceedings) an inspection was carried out for example on a company engaged in trading in databases used for marketing purposes and that processes personal data utilised for marketing purposes. An inspection on a company that collects personal information obtained by the financial advisers with which it works was also conducted to follow up on previous activities. Also subject of inspection was the processing of personal data by a recruitment agency, for one thing in connection to prior inspection findings and also with regard to the tightening of conditions for such entities as a result of changes to Act No. 435/2004 Coll., on employment. An inspection of a provider of services known as "hybrid post" was carried out at the urging of the Ombudsman.

Certain inspections were incorporated into the Supervisory Plan in direct connection to the General Regulation[2] coming into effect. Though it is based on the same general principles of personal data protection, it does differ in individual details. One of the more minor details is the fact that the General Regulation does not explicitly state as a legal grounds (title) for personal data processing that rightfully published personal data can be processed without the consent of the data subjects concerned (cf. Section 5 (2) d) of Act No. 101/2000 Coll.). An example of such a case was the inspection of the publishing of personal data on the internet in "clones" of public registers.

In September 2018, the Supervisory Plan was supplemented primarily with inspections of the processing of systems that use biometric data (dynamic biometric signature, voice biometrics, FaceId technology).

More can be learned in the following section of this annual report on certain cases that were the subject of inspection on the basis of the Supervisory Plan. Some of the inspections that were launched on the basis of the 2018 Supervisory Plan were not completed within the calendar year. The Office shall report on them in the standard manner on its website.

---

[2] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).

• FINDINGS OF INSPECTORS FROM SUPERVISORY ACTIVITY

Inspector Jana Rybínová

Leaking of personal data from HR files of the company CHRIST CAR WASH s.r.o.

The Office conducted an inspection of the company CHRIST CAR WASH s.r.o., of registered address Koterovská 534/175, Koterov, 326 00 Plzeň (hereinafter "ChCW" or the "inspected entity").

The inspection was launched on the basis of complaints the Office received over the course of December 2017 from ChCW employees and files passed on from the Police of the Czech Republic in January 2018. The content of the complaints was the fact that personal data had been leaked from the employee files of ChCW, in particular that ChCW employees had repeatedly received e-mails with copies of documents from their HR files attached. The object of the inspection was observance of the obligations of a personal data controller laid out by Act No. 101/2000 Coll. in connection with the processing of personal and sensitive employee data that a company processes as part of its employment relations, and also with a focus on observance of the obligations of a personal data controller within the meaning of Section 13 of Act No. 101/2000 Coll.

The Labour Code does not state any definition, or list of data, on what a personnel file should contain. The scope can thus be inferred from the legislation. In accordance with the Labour Code, a personnel file can only contain documents with personal data that is essential for performance of employed work, i.e. the scope of which is also in accordance with the provisions of Section 5 (1) d) of Act No. 101/2000 Coll.

It was found that the inspected entity was keeping copies of various documents in its HR files – e.g. a copy of the employee's ID card, a copy of their birth certificate, a copy of their health card, a copy of their health insurance registration card, a copy of their criminal record check, a copy of the client's bank card with their bank account number.

It was also stated in the inspection report that it is not possible to keep records of all the listed documents and keep copies of these documents in the HR files. It is the obligation of the employee to substantiate the accuracy of certain facts (e.g. a criminal record check) so that the employee can fulfil its legal obligations. To this end however it is sufficient for the employer to state in the HR file that the information in question has been confirmed and state who, when and on the basis of what document this has been verified (according to a document, contract, birth certificate, etc.).

It was also found that the inspected entity was keeping copies of the birth certificates of the children of certain employees, as well as scanned photographs of the employees. It was also keeping copies of ID cards, contravening the obligation laid down under Section 15a (2) of Act No. 328/1999 Coll., on Identity Cards. Even if inspected entity did have and provide the data subject's consent to the procuring and keeping of a copy of their ID card (which would satisfy the provisions of Section 15a (2) of Act No. 328/1999 Coll.), making a copy of the ID card with an employee's consent is only possible under the condition that all personal data listed on the ID card are being collected and thus also further processed in accordance with the purpose that the personal data controller has designated. If the inspected entity does not have a designated

purpose for collecting the other data on the ID card (the employee's photograph, the name of a potential spouse, their birth number, the names and surname of children and their birth numbers), it is not entitled to collect such personal data. Similar rules also apply for the purpose of an employer employing someone and keeping personnel records of the employee.

It was stated in the inspection report that the inspected entity processes personal data in its HR records contrary to the obligations laid down for it as a personal data controller in the provisions of Section 5 (1) d) of Act No. 101/2000 Coll. The reason for this is the collection of personal data that do not correspond solely to the stated purpose and to the extent necessary for fulfilling the stated purpose, and which is also in conflict with the obligations of a personal data controller under Section 5 (2) of Act No. 101/2000 Coll., as it does not have any legal title to process personal data in this manner.

In addition, in some undiscovered manner there was a "leak" of the personal and sensitive data of 62 ChCW employees. The data were then sent back to 28 employees by an unknown sender. The inspected entity had thus not adopted such measures as to prevent the disclosure of personal and sensitive employee data from the HR files, thereby violating the obligation imposed on it as a personal data controller under Section 13 (1) of Act No. 101/2000. The Office also found that the automated systems that the inspected entity was using to process personal and sensitive data for HR purposes was not equipped with a log function, thus it was not possible to determine and check when, who and for what reason personal data were recorded or otherwise processed. This meant that the inspected entity was not making electronic records of access (log-in) to the personal data being processed for HR purposes, thus failing to fulfil the obligation laid down by Section 13 (4) c) of Act No. 101/2000 Coll.

The inspected entity filed objections against the findings stated in the inspection report. In light of the fact that the deadline for submitting objections was not observed, they were rejected by the President of the Office for being late.

Proceedings on the imposition of measures to rectify the found shortcomings were subsequently conducted with ChCW on the matter and a fine of CZK 180 000 was issued.

Observation of the obligations of a controller by the company Lidl Česká republika v.o.s.

Based on the Supervisory Plan for 2018, the Office conducted a comprehensive inspection without having received a complaint at the company Lidl Česká republika v.o.s., which comprised an inspection of the HR, payroll, customer relations and surveillance systems, where it was not possible to anticipate what specific conditions for processing will have been put in place by the inspected entity. The object of the inspection was observance of the obligations of a personal data controller as laid down under Chapter II of Act No. 101/2000 Coll. in processing the personal data of company employees and customers.

Under the inspection, the inspected entity submitted a summary of all its databases. In these, it processed the personal data of customers and employees with stated purposes of processing, means and manner of process, including a summary of fulfilment of all conditions applicable to the individual instances of processing. For the purposes of a more detailed inspection, the inspectors selected the following systems: camera system with recording; database of electronic access cards, and database of incidents processed in specialised software applications.

It was found that the inspected entity had installed a camera system with recording in several of its buildings, through which the personal data of employees, customers and other persons

found in the areas monitored by this camera system were being processed. The purpose of the camera system is protection of life, health and property of customers; protection of life health and property of employees and protection of property of the inspected entity.

It was also found that the period of retention of the records from the camera system has been set up in accordance with the provisions of Section 5 (1) e) of Act No. 101/2000 Coll., with the retention period corresponding to the purpose of processing; use of the camera system is fully in line with the stated purpose; the camera system is not monitoring the activity of employees during the course of their work, aside from a minimised extent, and areas intended for their "private" activities, such as change rooms or break rooms, are not monitored.

The inspected entity has concluded an agreement with the processors of personal data in accordance with the provisions of Section 6 of Act No. 101/2000 Coll., lives up to its obligation to inform data subjects within the meaning of Section 11 (1) of Act No. 101/2000 Coll., and accepted and during the inspection documented the adopted technical and organisational measures for ensuring protection of the processed person data, and all operations with the camera system are logged in the sense of Section 13 (4) c) of Act No. 101/2000 Coll.

During the inspection of the processing of employee personal data through the electronic entry system, it was found that it is conducted automatically, with data on the electronic access card and employee entry to the premises of the inspected entity being kept in a separate database, with the database itself not recording any entries. Access to the database is recorded on the remote server located at the headquarters of the inspected entity, through which the database is accessed. The retention period has been established in accordance with the provisions of Section 5 (1) e) of Act No. 101/2000 Coll. and is in line with the purpose of processing. The inspected entity keeps the database of electronic access cards itself on its own server and also manages it itself. For this reason it does not have any agreement on personal data processing with a third party.

It was found that the inspected entity has adopted sufficient technical and organisational measures to ensure the protection of personal data processed under the given system; access to the system is logged in accordance with the provisions of Section 13 (4) c) of Act No. 101/2000 Coll.

For the purpose of keeping records and dealing with individual loss incidents, the inspected entity keeps a database of such, which aside from data on the individual events such as amount of damage, loss ratio, etc., also contains the personal data of customers as damaging or damaged parties. The retention period for the personal data has been set by the inspected entity in keeping with the provisions of Section 5 (1) e) of Act No., 101/2000 Coll. and corresponds to the purpose of processing.

On principle the inspected entity does not pass along personal data kept as records of and dealing with loss incidents to third parties, with the exception being passing on the whole incident for assessment to a specialised insurance broker, with whom the inspected entity has concluded a processing agreement in accordance with the provisions of Section 6 of Act No. 101/2000 Coll.

The inspected entity has adopted and documented sufficient technical and organisational measures for ensuring the protection of personal data processed under the given records. The Office found no violations of obligations by the inspected entity as a personal data controller pursuant to Section 13 (4) c) of Act No. 101/2000 Coll.

Inspector František Bartoš

Internet Mall, a.s. – notification of security breach in management of personal data

The Office received a written Notification of Security Breach in Management of Personal Data from the company Internet Mall, a.s. (hereinafter "Internet Mall"). The content of this message was the fact that the company, which under its line of business operates the internet shopping mall MALL.CZ, was reporting that on 25 August 2017 it recorded a security breach in management of personal data.

On some unspecified date between 31 December 2014 and 23 July 2017, an unknown person or persons stole an electronic database of the client user accounts from the servers of Internet Mall. The database contained the personal data of clients in the scope of e-mail contact, password (in encrypted form), name, surname and telephone contact. According to the statement, a total of 766 421 electronic records were stolen, of which 735 956 contained a unique e-mail address. In total around 20 percent of the total records in the customer database were stolen and around 350 000 of the records were also active in 2017 when the theft was discovered.

An inspection found that Internet Mall was alerted to the access to its database of clients (user accounts) by a natural person by an electronic message. An investigation and comparison of the accessed data identified the divulged database as the database of own clients from 2014 (internet servers operated by the company Internet Mall in 2014: www.mall.cz, www.korunka.cz,www.azelektro.cz and hfishop.cz).

After receiving the information, the company requested that the operator of the web portal www.ulozto.cz, the company Uloz.to Cloud, a.s., remove access to the database. That same day, Uloz.to Cloud, a.s. secured deletion of the aforementioned database. Following this, Internet Mall sent its customers information by e-mail on the possible leak of their personal data, with a recommendation that they change their log-ins and passwords.

The inspection also reported that a database of 766 421 records on customers of Internet Mall took place in the period from 31 December 2014 to 23 July 2017 by an unknown perpetrator or perpetrators. The database contained 735 956 unique customer addresses including name, surname, user name, e-mail address and telephone number, which it had stored in its ICT systems. Not only did Internal Mall, as a personal data controller, fail to prevent the unauthorised access and theft of the user database, it did not even register or discover it. It thus breached the obligation of a personal data controller laid down by Section 13 (1) of Act No. 101/2000 Coll., as it failed as a controller to adopt such measures as to prevent the unauthorised theft of the aforementioned database of customer records. The consequence of this failure was the database of 766 421 records on Internet Mall customers containing 735 956 unique customer addresses in the scope of name, surname, user name, e-mail address and telephone number being made public on the publicly accessible web portal www.ulozto.cz for the period of 27 July 2017 to 25 August 2017.

At the same time it was not possible to determine how many people were given access to the database of stolen personal data, who currently holds a copy of it, and how many copies were made. In the subsequent administrative proceedings the company was issued a fine of CZK 1.5 million.

INTER - IVCO, s.r.o. – observance of the obligations of a personal data controller

Based on complaints and the Supervisory Plan, the Office conducted an inspection at the company INTER – IVCO, s.r.o. (hereinafter the "inspected entity") on the matter of compliance with the obligations of a personal data controller laid down by Act No. 101/2000 Coll. in processing the personal data of data subjects in the register of debtors found on the website www.rejstrikdluhu.cz, with a focus on the legal title for processing the personal data, including the disclosure and publishing thereof.

It was found that the inspected entity was processing false information on the website www.rejstrikdluhu.cz. This concerned the person of the complainant, who learned that he was in debt for a large amount from his partner, who was alerted to this fact by an anonymous e-mail. The inspection found that the inspected entity had not adopted any rules for the entry, maintenance or even correction of false entries. It was found that anyone could enter information on an unpaid debt or receivable for payment of a fee and confirmation of agreement with the general terms and conditions. The operator did not however verify the entered information or the identity of the person making the entry. It is also did not check in any way the identity of persons who contacted it with requests for false entries to be deleted. The investigation showed, for example, that the site operator changed the content of published information on the basis of a simple phone call. For this service it also demanded a fee be paid.

During a local inspection during the investigation it was found that there were a total of 779 items from 431 submitters on the website www.rejstrikdluhu.cz. This set of data contained the personal data on a large number of natural persons, legal persons and natural persons conducting business.

It was found that in the case of the complainant's personal data, they were listed on the website www.rejstrikdluhu.cz in the scope of name, surname, address and information on the alleged amount of debt and fictitious creditor, this for a period of at least nine months without the complainant having been notified in any way. The operator deleted the untrue entry on the basis of a telephone complaint from the complainant.

The inspector found the processing and publishing of personal data of "debtors" in the register www.rejstrikdluhu.cz to be an unacceptable encroachment on the privacy and personal life of the persons in question. The disclosure of personal data in the register of debtors, which was obtained on the basis of a private law relationship, without the consent and awareness of the debtor, caused damage to the reputation of individuals who were entered into the debt register by accident or in some cases through the intent to harm. Considering that the company did not verify the documents on the basis of which a natural person was entered into the register of debtors at www.rejstrikdluhu.cz, this could damage their rights in many other relationships, both under private law as well as public law. Divulging personal data without the debtor's consent is only possible to authorised entities (e.g. the Police of the Czech Republic). A personal data controller may only publish or divulge data with the debtor's consent.

It was found that the inspected entity was a personal data controller and is fully liable for the processing, publishing and acquiring consent with processing of personal data of natural persons in the debt register at www.rejstrikdluhu.cz within the meaning of personal data controller obligations laid down in Act No. 101/200 Coll. In no case can this responsibility of the inspected entity be transferred to the creditor. Under Section 5 (4) of Act No. 101/2000 Coll., a personal data controller must be able to demonstrate consent to personal data

processing for the whole duration of this processing, which the inspected entity was not able to do.

The inspected entity did not have the consent of the complainant or any other consent of the other persons to processing of their personal data in the register of debtors published on the website www.rejstrikdluhu.cz, nor any other legal grounds for processing personal data within the meaning of Section 5 (2) a)–g) of Act No. 101/2000 Coll.

The inspected entity processed the personal data of 477 data subjects on its website in the form of its "debt offer" without having the consent of the individual data subjects or other legal grounds for disclosing them. The inspected entity processed personal data in violation of the provisions of Section 5 (2) of Act No. 101/2000 Coll.

It was found that the inspected entity breached the provisions of Section 5 (2) of Act No. 101/2000 Coll. in connection with processing the personal data of the complainant and publishing them in the debt register www.rejstrikdluhu.cz without his consent.

In the following administrative proceedings, a fine of CZK 90 000 was issued. In light of the fact that the inspected entity shut down the website www.rejstrikdluhu.cz during the inspection, it was not necessary to hold proceedings to impose remedial measures.

Inspector Daniel Rovan

Inspection of mobile operator concerning consent request

On the basis of complaints, the Office conducted and completed an inspection of a mobile operator. The complainants consistently stated that the environment of an electronic application is set up so that the client's access to the contracted services of the company is conditioned on provision of consent to the processing of the personal data of customers of the operator's services for commercial purposes. The client need not provide consent right away, but at an unspecified time in the near future. The complainants stated that the impression is convincingly made that consent must be granted one way or the other; in contrast there is no option for refusing the processing of personal data for commercial purposes. Another type of complaint was the complainant drawing attention to the processing (transfer) of personal data as part of the processing of Telcoscore. In light of the fact that the inspection was commenced after the General Regulation took effect, its Articles 4 (definitions), 5 (obligations), 6 (lawfulness), 7 (consent) and 28 (processors) were checked and assessed.

In practical terms the inspection dealt with two areas – the consent and option of withdrawing consent, and the transfer of personal data within the service of Telcoscore. The inspection findings showed that the inspected entity prepared and submitted to its clients for signature a new consent form.[3] The old consent was valid up until 24 May 2018, the new one from 25 May 2018. In light of the large number of clients, the inspected entity began "collecting" new consents in February 2018. The situation thus arose that some clients had two signed consents. This was confusing for them and thus they decided to withdraw one of the consents. If this was the "new" consent, they received the information that it could only be withdrawn once the General Regulation took effect, i.e. after 25 May 2018. The inspector evaluated this interpretation as incorrect, as a data subject has the right to withdraw consent at any time.

[3] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).

In the inspection of the processing (transfer) of personal data within the Telcoscore service, it was checked, and substantiated by the inspected entity, that scoring was conducted by the inspected entity in a two-part legal regime, specifically:

- on the basis of consent from the data subject for the purposes of the Telcoscore service provided via a different company under the contractual provisions of the parties involved. For certain providers of financial services, this service replaces an assessment of credit history for clients without any financial history (young people, in particular students) in light of their age. This service is provided in the interest of the applicant and with their written consent.
- on the basis of the interest of the inspected entity, consisting of an evaluation of the customer's behaviour in using its services (telcoscoring), including the customer's payment behaviour, for the needs of the inspected entity in deciding on offers to its clients. This case concerned the internal matters of the inspected entity and no personal data was transferred to third parties.

The inspection did not show that the inspected entity passed on the results of telcoscoring to third parties. In this part of the inspection the Office did not find any violations of the General Regulation.

Checking the sufficiency of personal data security at the General Financial Directorate (EET)

On the basis of the Supervisory Plan for 2017, the Office conducted and completed an inspection of the General Financial Directorate in connection with the processing of personal data by the Financial Administration of the Czech Republic (hereinafter the "inspected entity") with a focus on the processing of personal data under Act No. 112/2016 Coll., on Registration of Sales under what is known as EET (the electronic registration of sales). The Office also received a submission on suspected insufficient personal data security, which it investigated during the inspection. The tax administrator publishes the conditions and procedure for access to the shared technical equipment of the tax administrator by remote access, which allows the taxpayer to manage the certificate for registration of sales and data for managing registration of sales. Communication takes place via the tax portal, see http://adisspr.mfcr.cz/adist/idpr_pub/dpr/uvod.faces. The tax portal serves in general for communication with the Financial Administration of the Czech Republic and to obtain information as part of tax administration, with the operator of the tax portal being the General Financial Directorate.

The inspected entity operates an automated tax information system. In the analytical space, which is not an application in the true sense of the word, the data are stored on a database server. The automated tax system has been designated as an IS of the critical information infrastructure under Act No. 181/2014 Coll., on Cybersecurity, and the related Decree No. 316/2014 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures and Setting the Requirements for Submissions in the Field of Cybersecurity. The requirements of these documents refer to security measures. Among these are technical measures, inter alia measures for the user interface of the information system and its immediate systemic environment (operating systems, databases, web services).

In light of the fact that the inspection took place before the General Regulation took effect, the controller obligations were checked according to Act No. 101/2000 Coll., specifically those

arising under Section 5 (1) b), d), and e), Section 5 (2), Section 6, and Section 13. The inspection findings showed that the powers under the Act on Registration of Sales are executed by the authorities of the Financial Administration of the Czech Republic, i.e. the General Financial Directorate. The automated tax information system that processes the data was designated an information system of critical information infrastructure under Act No. 181/2014 Coll., on Cybersecurity, and the related Decree No. 316/2014 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures and Setting the Requirements for Submissions in the Field of Cybersecurity. This fact automatically dictates the standards for its security. The inspection checked compliance with this.

A physical inspection was conducted of the data storage and application server rooms at the data centre, the services of which the inspected entity utilises. The inspectors also focused on a physical inspection of one of the inspected entity's IT worksites focused on managing the information system, specifically the Department of Tax Information Systems, as well as an inspection of a worksite that makes use of the information system for its activities, specifically the Financial Office for the City of Prague. At all worksites it was checked whether the employees of the inspected entity had been trained and informed on security measures, whether they knew their responsibilities and complied with them. Secure access to protected worksites was also checked, as was whether access to the site matched the documentation submitted by the inspected entity.

The complaint concerned the fact that the inspected entity had implemented the commercial product reCAPTCHA from the company Google Inc. in connection with processing of applications of the electronic registration of sales (EET) into the automated tax information system operated by the financial administration. The inspection findings showed that this product was only included in the system as a supplementary one. Moreover, the inspected entity replaced this commercial product during the inspection with their own solution. The inspection did not find any violations of Act No. 101/2000 Coll.

Inspector Josef Vacula

Processing of personal data in the CERD system at www.centralniregistrdluzniku.cz and www.cerd.cz (copying of public registers, publishing of false information, encroachment on private life and failure to inform data subjects)

On 31 March 2016, the Office commenced an inspection of the company CSR & Protikorupcnilinka.cz s.r.o. in connection with a large number of complaints received. Generally speaking, the complainants had discovered that their personal data had been published on the aforementioned websites, with false information assigned to their personal data, e.g. that they have outstanding debts or that they are still the target of insolvency proceedings. The amount of such complainants numbered in the dozens.

In gathering background documents for the inspection proceedings, the Office worked with open sources, primarily commercial registers. These were the Czech Commercial Register and the commercial register of several US states. The inspection found that foreign companies are also involved in the processing of personal data within the CERD system: e.g. CERD SYSTEM LLC, CENTRAL REGISTER OF DEBTORS INC. or CERD LLC, REGISTRY LLC). The Office also worked with publicly available information on those who registered the domain names.

Based on a thorough analysis of the information obtained from these sources, the inspection found that the entity that founded and controlled all the companies involved in processing the personal data on the aforementioned websites was a natural person. It turned out that this person created an intricate structure of Czech and foreign legal entities that were meant to conceal the true personal data controller, i.e. this natural person. In addition, this person listed false information on the aforementioned websites, e.g. that confirmations of no debt issued that they issue are completely valid and universally accepted, or that state authorities work with this register of debtors.

Following a careful evaluation of the information obtained, the Office drew up the conclusions of its inspection activity, stating that the aforementioned company CSR & Protikorupcnilinka.cz s.r.o. is in the position of a personal data processor within the meaning of Section 4 k) of Act No. 101/2000 Coll., while the personal data controller in the meaning of Section 4 j) of Act No.101/2000 Coll., and thus the entity responsible for all activities associated with the processing of personal data, is the natural person. In this inspection the Office furthermore found several serious breaches of Act No. 101/2000 Coll. Selecting one at random we can mention violation of the provisions of Section 5 (2) of the introductory part of Act No. 101/2000 Coll., as specific natural persons could be listed on the website without any control or verification and listed as debtors, including the amount owed, without these people actually being debtors or even knowing that a record is being kept of them in this context. The inspection also found violation of Section 11 of the Act in question, in that the personal data controller informed data subjects insufficiently or untruthfully about the processing of their personal data; or the provisions of Section 10 of the cited Act, wherein the inspection found that the actions of the personal data controller severely encroached on the privacy of the data subjects, having not only initiated and facilitated false publishing of debtors (see above), but also copying the official insolvency register kept and managed by the Czech Ministry of the Interior and then failing to keep the contents thereof up-to-date, thus listing on their website inaccurate (false) information on the data subjects. Such information could then have an impact on the subjects' personal life, particularly in the case of natural persons conducting business. In such cases this information also had an effect on their business activity.

It must be emphasised that for the whole duration of the proceedings, the inspectors met not only with very difficult communication with official foreign sites, but with cooperation that bordered on obstruction on the part of the inspected entity, and above all with personal attacks including insults and abuse from the natural person against the members of the inspection team. Despite these difficulties, the inspection proceedings were successfully wrapped up on 30 July 2018. The decision of the Office President on submitted objections rejecting them across the board was delivered to the inspected entity.

The importance of these inspection proceedings and dangerous nature of this natural person's activities are also underscored by the fact that the European Commission also received complaints against the aforementioned websites. It requested that the Office, as the authority that managed to resolve this problem, give a paper on how this Europe-wide issue was resolved at a conference on consumer and data protection.

Eltodo, a. s., - inspection of camera system in vehicles monitoring parking zones

The Office commenced an inspection of the aforementioned company on the basis of the Supervisory Plan for 2018, reacting to a great number of inquiries over the "little car with the cameras". The inspection was thus focused on the processing of personal data in connection with monitoring conducted by automobiles operated by the inspected entity to check parking fee payment in the paid parking zones within the City of Prague as part of the project www.parkujvklidu.cz.

The general function of the camera vehicles can be described in that the vehicles drive around a predetermined paid parking zone at ten-minute intervals. During the first trip the four cameras located on the vehicle monitoring these zones take a picture of the registration plates of parked vehicles. The pictures of the vehicles' registration plates are checked online in the central information system, where it is determined whether the given vehicle (or rather the registration plate) has paid the parking fee. If it is determined that the registration plate has paid its parking fee, this picture is not saved, but is immediately deleted. If a registration plate has not paid its parking fee however, the images from the camera are saved and when the vehicle next drives by, photo documentation of the vehicles that have not paid their parking fee are also made in order to procure proof for potential administrative proceedings. This photo documentation is made with two other cameras. Subsequently the aforementioned website published information on the processing of personal data in the scope of registration plate, location data (GNSS coordinates, information on the location of the monitoring vehicle and photographed vehicle), time the photographed vehicle was parked there, identification of the section of the paid parking zone in relation to the parking session, ID of parking session and information on the existence of a long-term parking permit.

In order to assess the position the inspected entity holds in relation to the personal data, the inspectors requested the contract documentation. On the basis of an analysis of the relevant agreements they came to the conclusion that the personal data controller within the meaning of Section 4 j) of Act No. 101/2000 Coll. is the City of Prague and the personal data processor within the meaning of Section 4 k) of Act No. 101/2000 Coll. is the City of Prague Technical Administration of Roads, with the relevant processing agreement having been concluded in accordance with Section 6 of Act No. 101/2000 Coll. The inspected entity, i.e. the company Eltodo, a.s., was found to have the position of a person processing personal data on the basis of an agreement with the personal data processor pursuant to Section 14 of Act No. 101/2000 Coll.

Inspector Božena Čajková

Processing of client personal data during provision of loans by the company BNP Paribas Personal Finance SA, branch

The Office launched an inspection on the basis of the Supervisory Plan for 2018, which included a complaint concerning suspicion of unauthorised processing of the complainant's personal data by the inspected entity, in particular processing of personal data after the deadline for the destruction thereof.

The inspectors focused on compliance with the obligations incumbent upon BNP Paribas Personal Finance SA, branch (hereinafter "BNP Paribas" or the "inspected entity") under Act No.

101/2000 Coll., on Personal Data Protection and Amending Certain Acts, in connection with the processing of client personal data when providing a loan.

The inspection found that the loan agreement with clients is concluded in hard copy or electronic form. Clients can apply for a loan in person, at the inspected entities branch, or also when purchasing goods in instalments with a contractual partner of the inspected entity (hereinafter "retailer") at a branch of the retailer, or online through the web portal of the inspected entity or retailer. In the case that a contract is signed in hard copy at a branch of the retailer, the retailer holds the position of a personal data processor. In other cases (online or in person in electronic form) the retailer does not keep the client's personal data. The providers of information technology ("providers") also have the role of personal data processor in connection with provision of loans. With both the retailers and the providers BNP Paribas signed agreements on personal data processing that meet the requirements of Section 6 of Act No. 101/2000 Coll. The scope of information on clients required in connection with arranging the loan is the same regardless of whether the application is made in person at a branch or online. In connection with providing loans, BNP Paribas processed personal and sensitive data of clients, sensitive data (the client's biometric signature) being only in the case of signature in electronic form. Client personal data are processed on the basis of BNP Paribas fulfilling its legal obligation and client consent, sensitive data (biometric signature) on the basis of their explicit consent. The purposes of the processing are, in particular, the fulfilment of the company's legal obligations under special legislation, assessment of the applications for provision of a financial service, concluding and performing the agreement with the client, protection of the company's rights and legitimate interests, activities in the insurance business, creating an information file as part of the registers of client information on financial standing, reliability and payment history, and marketing purposes.

The inspection found a violation of Section 5 (1) d) of Act No. 101/2000 Coll., consisting of the processing of clients' biometric signature even though the processing of this data is not essential for fulfilling the purpose of processing, which according to BNP Paribas is simplifying identification of the client. In light of the scope of data collected in connection with providing a loan, the inspectors consider it evident that the clients are identified in a sufficient manner. In addition, it is possible to conclude a loan agreement with BNP Paribas in paper form, which binds the company and client in the same manner and to the same extent as the electronic agreement with the client's biometric signature.

The inspection also found that BNP Paribas was retaining sound recordings of telephone conversations with clients with whom a contract had been signed for a period of ten years after the agreement had ended. In connection with this a violation of Section 5 (1) e) of Act No. 101/2000 Coll. was found, as the blanket ten-year period for keeping records of all telephone calls with clients with whom a contract was signed is not essential. In this regard the Office is of the opinion that in the case of recordings of telephone conversations (assuming they are evaluated as truly necessary to fulfil a legal purpose), the various types of conversations must be distinguished along with the corresponding purpose of their further retention. The given period of retention is only relevant in the case that a transaction order is made during the call. In contrast, in the case of service advice, for example, such a period is clearly disproportionate. As far as ordinary conversations of an informative character go, it is necessary to

consider whether recordings of such calls are necessary, or at least properly adjust the period for their further retention.

The inspectors also found violations of Section 5 (1) e) of Act No. 101/2000 Coll. in connection with the complainant's submission delivered to the Office. In it, the complainant stated that BNP Paribas was processing their personal data acquired in connection with an application for a current account for longer than the period specified for the data to be destroyed. PNB Paribas confirmed this fact, stating that the state of affairs (likely caused by switching to a new internal information system) had already been rectified and that at the time the complaint was submitted, the complainant's personal data were no longer being processed.

During the inspection and subsequently after the inspection report was handed over, the inspectors were already informed about measures BNP Paribas was preparing in connection with the violations noted in the report. The changes concerned measures related to the retention period of sound recordings and measures to check the disputed processing of the client's biometric signature. In light of this it was therefore not necessary to impose measures to rectify the shortcomings found on the inspected entity.

Processing of personal data on the website of the company Mladá fronta, a.s.

On the basis of the Supervisory Plan for 2018, which laid out an inspection of the publishing of personal data on the internet in "clones" of public registers, an inspection was commenced focused primarily on determining the legal grounds for such processing of personal data in connection with the legal treatment under the General Regulation and with regard for Section 60 (3) b) of Act No. 455/1991 Coll., on Trades (hereinafter the "Trade Act").

It was found that the inspected entity, through information listed on the website www.finance.cz, specifically on the web portal rejstriky.finance.cz, offered users (portal visitors) a service in the form of information on legal entities and natural persons conducting business compiled from public registers kept by the competent authorities of the Czech Republic, including historical information.

According to Section 60 (3) b) of the Trade Act, four years after the day an entrepreneur's last trade licence has been terminated, information on the entrepreneur is transferred from the public part of the Trade Register to the non-public part. After this transfer has occurred, the given personal data can no longer be considered published data, and application of Article 6 (1) f) of the General Regulation is no longer possible. At the same time, none of the other legal grounds defined in Article 6 (1) of the General Regulation can be applied to such processing either, with the exception of consent of the data subject. Thus the inspected entity has no legal title to these personal data.

The inspected entity also violated the obligation under Article 5 (1) d) of the General Regulation, as it processed the personal data of the entrepreneurs without ensuring they were kept up to date. In connection with the cited provision, the inspected entity was obliged to adopt appropriate measures to ensure regular updating of the source database.

Over the course of the inspection and also after it was completed, it was determined that the inspected entity was gradually adjusting the state of affairs in connection with a technical recalibrating of the parameters for the source database of entrepreneur personal data. A complete update of the data of all persons was set up, which meant that the personal data reclassified into the non-public part of the Trade Register were removed completely.

In light of the conclusions of the inspection, administrative proceedings to impose a fine were commenced.

Inspector Jiřina Rippelová

Inspection of the company NaturaMed Pharmaceuticals s.r.o., concerning controller obligations

In 2018 the Office conducted an inspection of the company NaturaMed Pharmaceuticals s.r.o. (hereinafter "Na¬turaMed"), which dealt with the offer and subsequent sale of dietary supplements. This company offers its goods through coupons, which are distributed, placed in mailboxes or inserted into magazines. Potential clients are also contacted via e-mail and by telephone through a call centre. In all these cases (coupons, e-mails and telephone calls), not only do they use contacts for previous NaturaMed customers, but also contacts from the databases of other entities, which the company either purchases or hires for this purpose.

The inspection focused on NaturaMed on the basis of a large number of complaints received. Generally these complaints concerned situations where the person in question was not a former customer of NaturaMed and thus did not know how the company had acquired their personal data. Another group were former customers of the company that had however explicitly refused to receive any more offers of goods, i.e. who withdrew their consent to personal data processing yet continued to be contacted.

As was already mentioned, the inspection found that NaturaMed not only makes use of the contact info of its former customers to offer its goods, but also data acquired from other entities in the form of purchasing or rental of databases. When the people in question ask about the legal title for (further) processing of their personal data or wish to withdraw their consent or exercise their right to erasure, it refers them to these entities. Thus although the company obtains contact data and clearly uses them for the purpose of promotion and offering of its own goods (and is thus in the position of a personal data controller), it does not accept any responsibility in relation to the data subjects. The sources of contact information (i.e. those who sell or lease the databases) to which NaturaMed redirects people often tend to be uncontactable. The people affected thus generally have no redress in this manner either.

The inspection was thus wrapped up with the conclusion that the company had violated the obligations of a personal data controller, in particular the obligation to process personal data solely on the basis of legally anticipated grounds (in this case primarily consent). This conclusion applies to the personal data acquired or taken from the databases of other entities. This occurred without the company ensuring or checking that consent to personal data processing that the people in question provided also applies to the transfer or personal data and further use thereof.

Violation of obligations in the processing of personal data was also found in relation to former NaturaMed customers. For such persons, the legal grounds for further use of contact information for offering goods in the future is generally provided up until the data subject in question expresses their disagreement with this approach. At the same time the scope of personal data that can be utilised for this purpose is limited (to name, surname and address, to which e-mail can also be added with regard for the development of communication technology, as this piece of data has the same character as address in electronic communication). The company nevertheless also retained and made use of the telephone number of former

customers for marketing purposes, as well as of other persons whose data it acquired by purchasing or renting a database.

The inspection also found a violation of the duty to inform. NaturaMed informs data subjects of the processing of their personal data in different manners (depending on the manner the personal data were obtained), but always insufficiently. What is primarily missing is a list of all the personal data it is actually processing, and an indication of the legal grounds on which it is doing so. NaturaMed also fails to properly inform data subjects of their rights.

NaturaMed filed objections against the inspection conclusions, but the Office President did not uphold them. Liability for the described breaches of obligations in processing personal data was the subject of subsequent administrative proceedings, in which a fine of CZK 30 000 was imposed on the company for unauthorised processing of the personal data of at least five persons.

Regular inspection of the Schengen Information System

In 2018 the Office conducted a regular inspection of the Schengen Information System. The power to conduct such inspections stems from Article 44 of Regulation (EC) 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) and also Article 60 of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System. According to the cited provisions, the Office is also obliged to conduct an inspection of the processing of personal data in the national component of SIS II (N.SIS II) at least once every four years in keeping with international auditing standards. The subject of the inspection was both the fulfilment of obligations laid down by the cited EU regulations by personal data controllers (Police of the Czech Republic) or processors, as well as the exercise of rights that persons concerned (data subjects) have in relation to SIS II.

SIS was established by the Convention of 19 June 1990 implementing the Schengen Agreement on the gradual abolition of checks at common borders (the Schengen implementing convention). Currently, Member States are using the second generation of SIS (SIS II), the establishment and operation of which are governed by the aforementioned EU legislation. The Czech Republic has been taking part in Schengen cooperation since 21 December 2007.

The purpose of SIS II (the second generation of the system being used since April 2013) is to secure and maintain a high level of security within the Member States (with regard for the absence of checks at the Schengen area's internal borders) by utilising information communicated via this system. It is thus a fundamental tool compensating for the abolition of police checks at internal borders.

The SIS II technical infrastructure is defined under the aforementioned regulations as consisting of a central component, a national component and communication infrastructure.
Responsibility for operation of the central SIS II database and the communication infrastructure lies with the European Union and EU-LISA (European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice). Member States are responsible for the establishing and functioning of the national component and for connecting it to the National Uniform Interface. All information is fed into SIS II and searched for using the national component of SIS II, which is a copy of the SIS II central database. Access to the national part of SIS II of other Member States is not possible.

From the perspective of Act No. 101/2000 Coll., which for the processing of personal data in SIS II is an auxiliary legal regulation to Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA, the controller of personal data processed in the national component of SIS II is the Police of the Czech Republic, which conducts the processing in question and is also responsible for it. The purpose of this processing is defined by the legislation and internal regulations of the Police of the Czech Republic.

Other entities also participate in the processing of personal data in SIS II from the position of personal data processors. These are: the General Directorate of Customs, the Czech Ministry of the Interior (Asylum and Migration Policy Department), the Ministry of Foreign Affairs, and the municipal authorities of municipalities with expanded jurisdiction.

The scope of personal data processed is relatively broad and is again laid down by the cited legislation. Aside from personal data, sensitive data are also processed, for example fingerprints or any special objective and unalterable physical characteristics. Through an internal regulation, the Police of the Czech Republic has established an overview of the records and associated source information systems, including requirements for a record to be entered. It has also set out the detailed procedures for processing personal data in SIS II (entry, search, access, updating and deleting). This includes the activities of the SIRENE headquarters with requirements for ensuring operation of SIS II in a manner that corresponds to the requirements of the legislation.

The inspection found that the necessary measures had been adopted to ensure proper receipt and processing of data subject requests to execute their right to access to personal data. Specific cases were also evaluated over the course of the inspection. There was no evidence that the adopted measures were not followed in practice.

Once again in the field of measures the Police of the Czech Republic had adopted in order to ensure the security of personal data processed in the national component of SIS II (the scope of which is generally dictated in EU legislation), the Office did not find that the Czech Police had failed to adopt or uphold measures to ensure the security of personal data processed within the scope required under Article 10 of Regulation (EC) No 1987/2006 and Article 16 of Council Decision 2007/533/SV.

Inspector Petr Krejčí

Prague City Hall Department of Transport Administration – unauthorised divulgence of personal data to other data subjects

The Office conducted and completed an inspection at the Department of Transport Administration at Prague City Hall at Na Pankráci 1685/17-19, 140 21 Prague 4. Among other things, the inspected entity keeps current records of vehicle operators/infractions.

The object of the inspection was compliance with the obligation of a personal data controller/processor laid down by Act No. 101/2000 Coll. in connection with divulging personal data in the call to pay a fine for a traffic infraction.

A number of complaints were received over time by the Office pointing out that it may have contravened the Act on Personal Data Protection when on 3 January 2018 calls to pay a certain amount concerning vehicle operators were sent to the addresses of other recipients. This led to divulgence of personal data in the scope listed in these fines, which contained the name, surname, date of birth, address of permanent residence, registration plate number of the

vehicle, the place and time the infraction took place, a description of the infraction, the amount of the fine, a description of how it could be paid, the day the call was made out, the file number, the reference number, and on the reverse side information on what would happen if the vehicle operator failed to pay the designated amount. Some of the complaints also included these letters, including the envelope, and/or links to or print-outs from websites of media outlets describing the events in question.

It was ascertained that the procedure followed by the inspected incident in connection with an agreement concluded with Czech Post concerning the delivery of mail through hybrid post was as follows: On 3 January 2018 the inspected entity handed a data file over to Czech Post containing two and a half thousand calls to pay a certain amount for a traffic infraction in PDF format, and a text file containing the addresses to which the fines were to be delivered. It demonstrated this fact with a screenshot with a list of all the files handed over on CD and a screenshot of the text file listing in the PID the fines and addresses to which they are to be sent, including the specific fine, and the set of data sent to Czech Post according to the order sent by form, or to the address on the Czech Post internet portal. This is logged into by the provider of the software providing for processing of the fines and handing the data over to Czech Post for processing. The inspected entity provided evidence of the security of the sending of the data sent to Czech Post hybrid post in an attachment to the agreement concluded between the inspected entity and Czech Post.

The inspected entity also provided evidence of the sending of the electronically properly paired contents of the fines with the addresses of the vehicle operators. It also documented the method by which registration of the order is automatically sent by Czech Post to Prague City Hall and the software company confirming receipt of the hybrid post order.

After only a few days, representatives of Czech Post notified the public that the error in the sent post was truly on their end and stated how the mistake took place.

The inspection found that Czech Post, on the basis of the data it received from the inspected entity, conducted machine processing of the order on 5 January 2018, i.e. on the basis of the received calls it printed them out and placed them in envelopes, sending them to the recipients stated on the envelopes by registered post marked addressee only. The whole process of printing out the fine notices received from the inspected entity and placing them in envelopes, including printing the name and address on the envelopes, is machine automated and takes place on the Czech Post packing line. If the notices of 3 January 2018 were mistakenly delivered to the addresses of recipients other than those stated in the notice, this allegedly occurred, according to the repeated statement of Czech Post at a meeting 31 January 2018 between the inspected entity and Czech Post, due to a technical error (the lines of the fine notification and allocated address being shifted). This was taken up with the Czech representative of the foreign supplier.

The inspected entity ruled out that the mistake could have taken place on its end, i.e. that a specific employee could have made an error. The first complaint was delivered to the inspected entity on 9 January 2018 and it began talks to redress this with Czech Post, to which e-mail correspondence between them testifies, including urging for a statement on the incident, minutes of the meeting of 31 January 2018 and a report with Czech Post's statement on the incident of 30 January 2018.

An inspection was also made of the electronic security of personal data, in particularly in terms of the requirements for automated processing, i.e. logging, at the worksite of the Transport Administration Department, with the applications used meeting the given requirements. The inspected entity issued a public promise regarding the notifications of 3 January 2018 that were improperly delivered that the recipients are not in danger of any sanctions from these, i.e. that the wrongly addressed people are not to pay anything, can consider the notifications groundless, and that misdirected documents cannot lead to any legal consequences, including distraint.

The explanation of the improper delivery was communicated to all affected data subjects, a total of 2 500, via a statement in the media, including information published on the website of Prague City Hall, and the notifications were delivered again, this time to the proper addresses. The inspection unequivocally refuted claims that the Prague City Hall Transport Administration Department was responsible for the errors in this case. The inspection confirmed that the error in the case of the misdirected letters, i.e. the notifications of 3 January 2018 to vehicle operators, was the sole liability of Czech Post. The inspected entity did not violate any provisions of Act No. 101/2000 Coll. in the matter under inspection.

Czech Post adopted measures to prevent such incidents in the future. For the infringements described above the company was issued a fine of CZK 250 000.

Mixing up of tax entities of the same name and data of birth by General Financial Directorate in delivering documents

The Office conducted an inspection of the General Financial Directorate, Financial Office for the Ústí Region, District Office in Louny, Rybalkova 2376, 440 01 Louny, Reg. no.: 72080043.

The inspection was launched on the basis of a submission in which the notifier pointed out an evidently systematic error and requested it be rectified so that cases are not repeated whereby natural persons are not identified by a unique identifier such as birth number or place of birth or place of business, adding that this could lead to an error in the inspected entity demanding an obligation be fulfilled by a person other than the obliged data subject, the consequences of which could even lead to distraint against the wrong tax entity. The notifier cited the repetition of the case of a specific tax entity, which the inspected entity had fined CZK 2 000 for filing their 2015 tax return on a paper form and not by data mailbox, even though they had not set up the latter. In this manner the inspected entity also delivered other documents to a data mailbox, i.e. to a different tax entity with the same name and date of birth. On the basis of improper delivery, i.e. failure to identify the tax entity according to an address or birth number, the inspected entity issued several documents (decisions) that were delivered to a different person. In fact, however, they should not even have been delivered to the proper tax entity, as the latter did not own a data mailbox, and thus had no obligation to file a tax return in this manner. As a result of this mix-up, the matter was only rectified on the basis of the resulting administrative proceedings, in which the tax subject in question had to obtain their rights on the basis of an appeal filed against the inspected entity, with the inspected entity admitting its error and cancelling the payment order for the fine.

During the inspection, the inspected entity confirmed that the error took place as a result of the existing systematic solution in the financial administration information system shared by all financial offices, adding that with manual processing and checking, the proper selection of

data mailbox is dependent on the accountability and attentiveness of the employee who has all the information necessary to match natural person entities – name, surname, date of birth and address – in the electronic system used by the inspected entity.

The inspected entity's information system is set up so that the relevant employee checks whether the addressee of a document has an active data mailbox based on name, surname and date of birth. This is then used to deliver the document in question. In the given case there was a match in the name, surname and date of birth, and thus the data mailbox offered by the information system was incorrectly assigned to the tax entity for sending correspondence. It was an error that the document containing personal data of a different tax entity was sent to one other than the one for which it was intended, that is to say divulged to another addressee due to an identical name, surname and date of birth. The dispatch containing the notification on the amount of back payment and the payment order for the fine sent to the data mailbox of the other tax entity contained the following personal data, inter alia: name, surname, residence, birth number, amount of back payment and the reason for the assessment.

After discovering the mix-up of tax entities, the inspected entity took measures directly with the employee who is responsible for sending documents, i.e. for divulging the document to a different tax entity's data mailbox. This employee was made aware of the improper delivery and also briefed on the cause of the improper entry of the data mailbox in the addressees of the document. An informative meeting was held at the inspected entity's District Office in Louny, where the specific case was described and analysed. Employees were explicitly notified in written form as well with the sending of an e-mail message on the possibility of an incorrect data mailbox being entered when checking the existence of a data mailbox for the addressees in the document records. A notice was placed in the file of the tax entity on this matter.

When a violation of Section 13 of Act No. 101/2000 Coll. was found and stated in the inspection report, the following was ordered of the inspected entity: "to promptly complete systemic measures for the whole financial administration so that mistakes in the delivery of documents cannot occur anymore, not even at other locations of the inspected entity. Until such a time the inspected entity shall ensure that in the case of any doubt or discrepancies as to a tax entity that its employees make a check when sending documents, in particular verifying the permanent residence address, including comparing and verifying in the case of a same name, surname and date of birth so that the personal data of data subjects are not divulged to an unauthorised person, i.e. documents are delivered to a different recipient/tax entity than that for whom they are truly intended.

The inspection form clearly demonstrated that another error of the same type was made in the inspected entity's system (dealt with by the Office in 2015 at a different district location), and thus the measures declared by the inspected entity were evidently not sufficient.

For violating the obligations under Section 13 of Act No. 101/2000 Coll. (the obligation of a controller to take such measures so as to prevent authorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data), the Office issue a fine of CZK 5 000 in administrative proceedings.

Other Supervisory Activities

• SUPERVISORY ACTIVITIES ON COMMERCIAL COMMUNICATIONS

As a result of the Regulation (EU) 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) taking effect, certain changes took place within the Office, with individual inspectorates dealing with supervisory activity in the realm of personal data protection. Supervisory activity in the realm of unsolicited commercial communications, which was previously performed by one of the inspectorates, was then entrusted to a separate newly created unit starting 1 August 2018.

This unit carried out all actions associated with unsolicited commercial communications. This primarily concerned analysing individual submissions, for which a special form has been created on the Office website. By analysing the header of e-mail messages and the text of the communication itself, the sender of the commercial message or person on whose behalf the commercial message is being distributed is determined, as is whether it is truly a commercial message.

The most important and most extensive activity of this unit is carrying out inspection and administrative proceedings. As can be seen from the included graph, this unit dealt with a total of 30 inspection proceedings in 2018 and conducted administrative proceedings that resulted in fines with 26 entities. The total amount of fines issued by this unit for distributing unsolicited commercial communications was CZK 3 464 360.

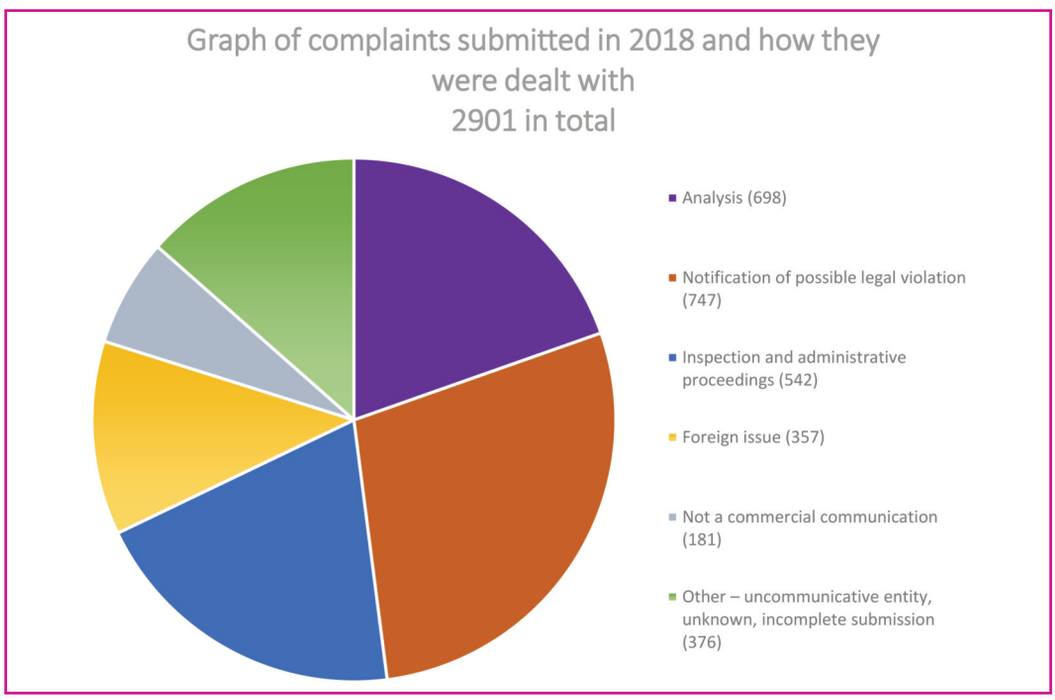
In ten cases administrative proceedings were also conducted for issuing a disciplinary fine for failure to cooperate during the conducted inspection, with the total amount of fines issued being CZK 905 000.

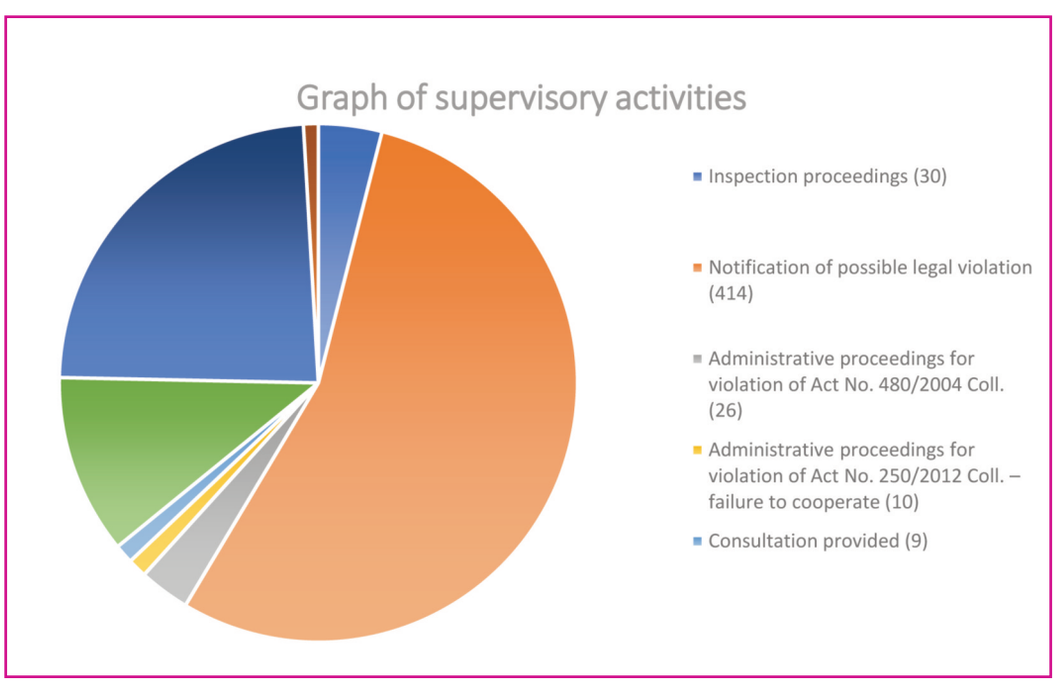
No less important however were the tasks associated with notifying individual entities of possible violations of the law, which is performed in cases where the Office receives only a few complaints against a single entity in a given period and the encroachment on privacy in electronic communication is thus not significant. This notification primarily fulfils a preventive function and also includes a proper explanation of the individual conditions under which the sending of commercial communications is allowed. Other activities of this unit also fulfil

a preventive and educational or public-awareness function, such as providing consultation in this area and dealing with individual written or telephone inquiries, or generalising the results of inspections and administrative proceedings in the form of press releases and position statements.

In terms of international cooperation, this unit passes along individual complaints where a foreign subject located in the European Union is found to be responsible to the competent foreign supervisory authority.

Last but not least it compiles various statistics, which it also depicts in the form of graphs.





Inspection of Widder Gilde, s.r.o.

An inspection of this company was launched on the basis of complaints received. Its aim was to assess compliance with Act No. 480/2004 Coll., on certain Information Society Services and on Amendments to certain Acts, in connection with the sending of unsolicited commercial communications.

During the inspection operations, the Office found that the inspected entity had concluded an agreement with the Ukrainian company POLITEKS LTD., with the contractual obligation of this company being the promotion of the inspected entity's products. These included, inter alia, "*the sending of messages on the products and services of Widder to e-mail addresses, to which the Partner (note: POLITEKS LTD.) has the consent of the persons in question*". The inspected entity thus did not send the commercial communications itself, but concluded an agreement for this purpose with POLITEKS LTD., which distributed the commercial communications. The actual sending of the commercial communications took place at the wishes of Widder Gilde on the basis of an issued distribution order.

The inspectors thus found that the entity responsible for distribution of commercial communications was both the inspected entity and the company POLITEKS LTD. It came to this conclusion on the basis of the applicable provisions of Act No. 480/2004 Coll., in which the legislation assumes that a propagator can distribute commercial communications not only on its own behalf, but also via a different entity. According to the provisions of Section 7 (4) b) of Act No. 480/2004 Coll., *a contrario* every commercial communication must contain information on who is sending it and on whose behalf the communication is taking place, i.e. to whose benefit the commercial communication is being distributed. Only such an interpretation is EU-compliant and in accordance with the purpose of the law.

During the inspection the inspectors primarily investigated whether the responsible entity has the legal title to send commercial communications. On the basis of the inspection operations conducted and findings, the conclusion was come to that the inspected entity did not make sure in any way that its contractual partner had valid consents to send commercial communications as it declared in Article 3.5 of the agreement.

The Office thus found that the inspected entity had violated Section 7 (2) of Act No. 480/2004 Coll., as it distributed commercial communications without the prior demonstrable consent of the addressee, and a further violation was found in relation to Section 7 (4) a) of Act No. 480/2004 Coll., as the distributed commercial communications were not clearly and distinctly marked as commercial communications. The inspected entity filed objections against the conclusions of the inspection report, and these were rejected by the Office President.

Administrative proceedings were then held against Widder Gilde. On the matter of these proceedings it is necessary to add that Section 11 (1) of Act No. 480/2004 Coll. is designed on the basis of strict liability, i.e. liability for the legal state, with it not being necessary to investigate culpability for the resulting unlawful situation in relation to a legal entity. It is for this reason and for the reason of fulfilling the will of the legislature – i.e. protecting privacy to the greatest possible extent – that those entities who gave the order, concluded an agreement or otherwise de facto initiated the sending of commercial communications must also be considered disseminators of commercial communications. For this reason, it is necessary for disseminators of commercial communications, whether they are the ones who ordered it or the actual distributors, to always sufficiently check whether the addressees of commercial communications

have given consent for such, or more generally whether distribution is taking place in a legal manner. On the basis of the aforementioned inspection proceedings, the administrative authority considers it proven that the accused company did not have the legal title for distributing commercial communications for the addressees in question, nor did it check in a sufficiently demonstrable manner that the partner with whom it concluded a contract for the purpose of distributing commercial communications had access to such legal titles. In relation to the liability of the accused company and its partner it can be added that each of these entities bears its only portion of the responsibility for its actions, which meet the grounds for an offence. A disseminator in the position of the one making an order thus bears its own liability regardless of the obligations of other entities, and within the meaning of Section 11 (1) of Act No. 480/2004 Coll. it is thus possible to punish a disseminator in the position of a client for these actions, i.e. Widder Gilde, s.r.o.

Under these administrative proceedings this company was thus fined CZK 80 000. The accused company first submitted a protest, then an administrative appeal, which was rejected by the Office President, and the contested decision was confirmed. The subject of the submitted objections, as well as the protest and administrative appeal was above all that the accused did not agree with its responsibility for the sending of the commercial communications.

On this matter it is necessary to present in more detail the further arguments that were used in the decision on the administrative appeal. Attesting to conclusion on the accused's liability is the broad logic and purpose of Act No. 480/2004 Coll., whereby the provisions of Section 7 and Section 11 of Act No. 480/2004 Coll. must be viewed not separately, but in context alongside Act No. 101/2000 Coll., on Personal Data Protection and Amending Certain Acts. It is evident from the file documentation in the inspection proceedings that the commercial communications were not intended exclusively for legal entities, and thus with respect to judgment of the Supreme Administrative Court no. 9 As 34/2008-68 the details of electronic contact must be viewed as personal data. It follows from the agreement on marketing cooperation that the accused entrusted the partner with promoting its products and services, inter alia by sending messages to e-mail addresses. The accused thus determined the purpose and the methods for personal data processing, thus fulfilling the definition of a personal data controller in the sense of Section 4 j) of Act No. 101/2000 Coll. In light of the fact that it is the primary responsibility of the controller to ensure compliance of processing with the legal conditions, it is the controller who bears primary liability in the case of a potential legal violation. We can also point out one of the central principles of personal data protection, which is the right of a data subject to access information. This right is applicable in particular against the personal data controller, as it is the controller who is responsible for the legality of processing and who has access to the personal data of a specific subject. For this reason, it is necessary to be aware of the identity of the controller. Only in this way can right to access to personal data and to change or destroy them be invoked. This is the reason that legislators enshrined the obligation to state in every commercial communication the identity of the sender – the one on whose behalf the commercial communication is being distributed. If it were possible to transfer liability for illegal distribution of commercial communications to another entity, including entities outside the jurisdiction of state authorities, the aforementioned rights and principles of personal data protection, including of privacy in a general sense, would be completely annulled, while also profiting the sender of the commercial communications that de facto initiated and directed

the distribution. In the situation where Directive 2002/58/EC and Act No. 480/2004 Coll. were adopted precisely in order to increase the security and protection of personal data with regard for the special risks of the internet and electronic communication, such a conclusion would be absurd and go completely against the presumption of a rational legislature that intended to ensure the highest level of protection.

• COMPLAINTS, NOTIFICATIONS OF PERSONAL DATA BREACHES, AND CONSULTATIONS

En the second half of 2017, with the effective date of the General Regulation[4] approaching, there was a gradually increasing number of inquiries and then, due to the media attention the regulation was receiving, also an increase in the number of complaints from data subjects. For this reason, the Complaints and Consultations Unit, falling under the Public Relations Department, was divided from the start of 2018 into a Submissions and Complaints Unit and a Consultation Unit. This step allowed the heads of these units to devote themselves effectively to their agendas. At the same time the Public Relations Department was renamed the Department of Consultation Agendas. This title better captures its complex activities, to which the evaluation of received notifications of personal data security breaches and provision of prior consultations under the General Regulation were added with the latter coming into force.

COMPLAINTS AGENDA

The complaints agenda was significantly influenced by the turning point of the General Regulation taking effect. In this period a great proportion of complaints were directed against the actions of personal data controllers in obtaining the consent of affected data subjects whereby they

- improperly conditioned provision of service (concluding an agreement) with consent to the sending of commercial communications or other non-essential marketing activities
- obtained consent in a manipulative manner, e.g. that expression of consent was not intelligibly separated from the controller-provided information on personal data processing or the contract provisions themselves

Once the General Regulation, one of the pillars of which are the rights of data subjects, had entered into force, the Office recorded an increased number of complaints against failure of controllers to live up to these rights. This concerned in particular the right of access to personal data, wherein the data subjects were often not provided with information upon request, or the application of this right was made difficult by excessive requirements for the method of verifying their identity. Exercising of this right becomes increasingly important for example in terms of the frequent complaints against unsolicited telemarketing, as it allows data subjects

[3] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).

not only to obtain a copy of the personal data being processed, but also information on the source of the personal data. This allows them to decide effectively on further action.

Once the General Regulation had taken effect there was also an increase in complaints about copies of public registers on the internet run by private entities. In general, these were republishings of data on the business activities of natural persons or data from the insolvency register. In connection with this, among other things, the Office put a guide for persons concerned on its website of how to exercise the rights granted by the General Regulation with the operator of the databases in question.

Complaints in 2018 also concerned the publishing of personal data on the internet and the associated right to be forgotten, where the relationship between the right to information and the right to privacy had to be weighed for selecting the right approach. A traditional portion of the complaints agenda was complaints over cameras, most frequently those used as part of neighbourly (civil) disputes, by an employer, or to protect public property.

From a procedural standpoint, in cases of less serious violations or suspicions of violations of both Act No. 101/2000 Coll. and following 25 May 2018 the General Regulation, the Office elected to apply the tried-and-true informing of controllers on possible violation of the rules on personal data protection. In the vast majority of cases the situation was rectified in this stage without ex officio steps having to be taken. In 2018 the Office sent out nearly five hundred such informative letters to controllers, which helped cultivate the environment to a large extent.

A large part of these informative letters related to the publication of address data of applicants for information under Act No. 106/1999 Coll., on Free Access to Information. This primarily applied to municipalities, which in order to make this agenda easier often publish the document with the provided information without removing the address data of the applicants. In connection with this the Office has even encountered abuse of the General Regulation, whereby an applicant, knowing that municipalities often take this incorrect step, sends hundreds of municipalities an information request with the intent of evoking this mistake. Then the person requests financial compensation under the General Regulation.

NOTIFICATION OF PERSONAL DATA BREACHES

With the General Regulation coming into force, controllers ended up with a new obligation of notifying the Office of high-risk breaches of personal data security. What could be observed first and foremost under this new agenda was that, since it was a new obligation for controllers, they often failed to reflect the requirements of the General Regulation on the content of the notification. Notifications often lacked a description of the likely consequences of the incident for the persons concerned, and as well as a description of measures the controller had adopted in order to resolve the given incident. These are highly important elements, essential for assessing the received notification.

A recurring subject of notifications of breach of personal data security was being attacked by ransomware, which illegally encrypted information. The perpetrator then demanded a ransom. The other frequent notifications included loss of devices or documents containing personal data. Most frequently these were cases of human error or theft.

CONSULTATION

The General Regulation taking effect also considerably impacted the consultation agenda. Its educational significance in connection with this new piece of legislation became even more

important, as it was often necessary to assuage the panic that arose around the General Regulation. In suitable cases the Office emphasised to advice-seekers the fundamental continuity between the rules and the previous Act No. 101/2000 Coll. The start of the year and the period around the General Regulation taking effect saw an extreme onslaught of inquiries from the general public. For several months the Office faced double the number of inquirers as in previous years. For this reason, to increase efficiency, during the year it markedly updated its FAQ, dividing it up for better orientation into areas that the questions applied to. Information materials were also gradually added on the Office's website so that the public could find all the relevant information on the General Regulation without having to pose written questions.

On the day the General Regulation took effect, a telephone information line began to be operated every day, intended to provide quick and simple information on the General Regulation to the public, especially small and medium enterprises. A telephone line for questions concerning cameras and camera systems also began to be available twice a week. Both lines were served exclusively by qualified employees (lawyers).

The largest part of the consultation agenda was traditionally responding to written inquiries which, given that the issue of personal data protection twines through all aspects of human life, concerned highly diverse issues.

Both before and after the General Regulation took effect it was often necessary to clarify in what cases the obligation to name a Data Protection Officer does or does not arise, for example at what kinds of publicly funded organisations.

For questions on the exercising of data subject rights, it was necessary in several cases to explain that even the General Regulation does not institute any changes where a certain procedure is laid down by specific legislation, i.e. for example the right of erasure cannot be applied if the law stipulates that data must be retained for a longer period.

It was also necessary to explain the stricter interpretation of Working Group 29 (after the General Regulation took effect it was replaced by the European Data Protection Board) on the obligation to keep records on processing activities, which even in the case of smaller businesses applies to every constantly performed processing of personal data. This provides the controller with a useful overview of the activities they perform.

In some cases the questions focused on whether the controller is supposed to conduct a data protection impact assessment as per Article 35. In this case they were informed that the decision to draw up an impact assessment is up to the controller, which should only consult with the Office on potential remaining high risks pursuant to Article 36 of the General Regulation.The Office did not however receive any qualified request for prior consultation under this article in 2018.

Another integral component of the consultation agenda was the provision of personal consultations to associations of controllers, controllers themselves or their Data Protection Officers. For example, the Office provided personal consultation to representatives of the banking sector, an important representative of the automotive industry, and to a number of central state authorities or state bodies.

In order to increase public awareness, seminars were organised at the Office in cooperation with various Office bodies for officers named under Article 37 (1) a) to c) of the General Regulation, which were received very positively and were of great informational value for all those present.

• IMPOSING OF SANCTIONS

In 2018 the Office imposed fines for offences (or for violations of the General Regulation)[5] totalling CZK 7 202 360, of which CZK 3 464 360 was for unsolicited commercial communications. A summary of statistics on the proceedings the Office conducted in 2018 can be found in the section of this annual report entitled "The Office in Numbers".

The protection of personal data in the Czech Republic, and indeed the whole European Union, was tied to the General Regulation in 2018. The main topic associated with the General Regulation for the general public (and part of the professional public) was undoubtedly fines. The reason for this is that under the General Regulation, administrative fines can be issued of up to EUR 20 million or, in the case of a business, up to four percent of the total global turnover for the previous financial year, whichever is higher. At the same time the General Regulation explicitly states that administrative fines must be effective, proportionate and dissuasive. In light of these requirements, and also taking into account the established case law of the highest Czech courts, according to which imposed sanctions may not be decimating (cf. for example the finding of the Constitutional Court plenum under file no. Pl. ÚS 3/02 of 13 August 2002), it cannot be expected that the fines imposed for violating the obligations laid down by the General Regulation will normally reach the millions or even tens or hundreds of millions of CZK. When issuing fines under the General Regulation it is necessary to take into account many circumstances, which are listed under Article 83 (2) of the regulation. Of these circumstances we can name for instance the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement, or the manner in which the infringement became known to the supervisory authority, in particular whether the controller or processor notified the infringement.

In this context it is also necessary to remember that the highest fine imposed by the Office under Act No. 101/2000 Coll. over its 15 years of activity in this area was CZK 3 600 000 (with the upper limit under this legislation being CZK 10 000 000). It was thus a fine at a level of over one-third the legally stipulated maximum. In general fines of over CZK 1 000 000 have been rather exceptional.

Although the General Regulation took effect in 2018, the proceedings on infringements that the Office conducted applied to unlawful activities that took place under Act No. 101/2000 Coll. The following cases in particular (in addition to some of the cases presented in the part of this annual report entitles "Findings of Inspectors from Supervisory Activity") can be considered significant, not just in terms of the amount of the fine:

[5] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).

PROCESSING OF PERSONAL DATA IN ORDER TO CREATE DATABASES TO BE RESOLD

On the basis of an inspection conducted in 2017, the Office launched proceedings on an offence with the company Solidis s.r.o., in which a fine of CZK 800 000 was imposed.
In the proceedings the Office stated that the company processed personal data without legal grounds of an unspecified number of persons numbering in the hundreds of thousands, including at least the name, surname, address and telephone number, which it had obtained from third parties. It thereby violated the obligation laid down under Section 5 (2) of Act No. 101/2000 Coll., i.e. the obligation to process personal data with the consent of the data subjects or in the cases laid down by Section 5 (2) a) to g) of this act.

In its business activities the company made further use of the collected personal data (from other companies or from its own activities) to create tailor-made databases for its clients. It thereby determined the purpose and means of personal data processing, and was thus a personal data controller. This is not changed in any way by the fact that the personal data it provided for payment to its clients were structured according to the demands of individual clients, nor that their source was other entities. It is also the case that the fact that the company is a controller in relation to one instance of personal data processing it conducts does not rule out it being in the role of a processor in the case of other specific cases of processing.

The company acquired the personal data on the basis of licensing agreements, or orders, according to which consent to being contacted is guaranteed by the provider, or they were to have been data rightfully made public. This cannot however be considered an expression of consent fulfilling the necessary requirements (i.e. a free and informed indication of the will of the data subject, the content of which is the consent of the data subject to personal data processing). Under Section 5 (4) of Act No. 101/2000 Coll., the data subject must additionally be informed when giving consent on the purpose of processing and for which personal data the consent is being provided, to which controller and for which period. The controller must be able to provide evidence of the data subject's consent to personal data processing for the whole duration of processing.

It is evident from the above that the company as controller did not have consent for further processing of the personal data (creation of databases used to offer goods and services). Here it must be once again emphasised that these would have to be consents in which the company itself was listed as the personal data controller. A controller may not free itself of its liability to provide evidence of legal grounds for processing personal data by referring to contract documentation that is supposed to guarantee that the legal title in question (in this case consent) exists. It is the controller's responsibility to verify this fact with its contractual partner and ensure that it will be able to provide evidence of these consents, even if they happen to be stored with the other party.

The Office President rejected the administrative appeal submitted by the company against the decision of a first-instance administrative authority.

PURCHASE OF ILLEGALLY ACQUIRED DATABASES OF PERSONAL DATA

In the summer of 2016, the Office issued its highest fine to date for violation of the rules for personal data processing. This was the fine of CZK 3 600 000 levelled against T-Mobile Czech

Republic a.s. The Office found that the company had not adopted sufficient measures to secure the personal data stored in its internal electronic database, which contained the personal data of roughly 1.2 million natural person customers.

In October 2016 the Office noted reports in the media about the fact that the client data stolen from T-Mobile Czech Republic a.s. had been purchased by the company STEM/MARK, a.s. Following up on this information it immediately commenced an inspection of this company. During the inspection however the company refused to provide the necessary documents so that it could be performed, citing the fact that criminal proceedings were underway on the matter. So that the statute of limitations for potentially imposing a fine would not run out, in January 2017 the Office began proceedings for suspicion of an administrative offence. These proceedings had to be suspended in July 2017 however in light of the fact that the Police of the Czech Republic was performing an investigation of all the facts necessary to decide on prosecuting on the same matter. In August 2018 the Office reopened its proceedings, as copies of part of the police files were passed along to it and the matter was passed along for investigation of an administrative offence.

In September 2018 the Office issued a decision imposing a fine of CZK 400 000 against the company STEM/MARK, a.s., as in the period from March to May 2016 it wrongfully processed the personal data of customers of T-Mobile Czech Republic a.s. This concerned the personal data of two thousand natural persons (name, surname, residence address, sex, age and telephone number) as well as the personal data of roughly 81 000 natural persons conducting business (name, surname, telephone number, number of SIM cards in use, payment method for operator services and name of bank from which the payments come). The company thereby violated the obligation laid down in Section 5 (2) of Act No. 101/2000 Coll., i.e. the obligation to process personal data with the consent of the data subject or in the cases stipulated in Section 5 (2) a) to g) of the same act, as it did not have any legal grounds for processing these data.

The case file showed that the company was approached during February 2016 with an offer to buy a database, and it expressed an interest. All it wanted from the seller (in terms of extent of the database) was postal codes and telephone numbers. The seller was not able to modify the database in this manner, thus it purchased the whole thing. The database contained two thousand natural persons and 260 000 legal persons and natural persons conducting business. The Office's findings showed that the database contained the personal data of roughly 81 000 natural persons conducting business. The company did not make further use of the purchased data, because it did not need it at that time, and subsequently it was confiscated by the Police of the Czech Republic. The company paid an amount of approximately CZK 120 000 for the database.

The company submitted an administrative appeal against the decision, with the primary reasoning being that it is not liable for the unlawful actions committed by its employee (at the time the deputy director and member of the supervisory board).

The Office President rejected the appeal against the decision and the decision on the fine thus entered into force in December 2018. In her decision the President stated, among other things, that liability for unlawful actions must be attributed to the company as it was not an evident case of excess by its employee.

• FINDINGS FROM JUDICIAL REVIEWS

As in previous years, several decisions of the Office were the subject of judicial review in 2018. A number of other Office decisions are still awaiting judicial review. In terms of specific findings from the judicial practice in question, several rulings can be referred to, in particular concerning the following:

- publishing of personal data
- the scope of collected personal data necessary for concluding a private contract
- installation of camera systems by an employer

1. The public interest in publication of information on the tapping and recording of telecommunications and information obtained from the tapping and recording of telecommunications by the press and publicly accessible computer network outweighs the right to privacy in the case of informing the public on relevant influencing of the decision-making powers of the Prime Minister by a person for whom such behaviour is not formally appropriate.

The Supreme Administrative Court, in its judgment of 3 May 2018 in proceedings on the "cassation" appeal of the company MAFRA, a.s. against the judgment of the Municipal Court in Prague of 9 August 2017, stated above all that, in agreement with the Office and the Municipal Court in Prague it considers it to be sufficiently demonstrated that the information published by MAFRA is information acquired from wiretaps and from recordings of telecommunications obtained in the manner supposed under Section 8c of the Criminal Code, with none of the persons it concerns having given consent to publishing and it not being information already used in proceedings before a court. Furthermore the Supreme Administrative Court stated that: "*The interdiction laid down in Section 8c of the Criminal Code was breached and the information was published via the press and publicly accessible computer network. Thereby the formal merits of an administrative offence under Section 45a (1) of the Act on Personal Data Protection were fulfilled. This is not however an offence if the conditions of Section 8d of the Criminal Code have been met, in the given case the condition of public interest in the information being published, if this outweighs the right to privacy of the person concerned, or each of them. Here an assessment of the proportionality between the right to information and right to privacy of those affected by the publishing has a place.*"

The Supreme Administrative Court likewise agreed with the Office and Municipal Court in Prague that the fact that the persons affected by this administrative offence did not in any way object to the subsequent publishing of the information cannot be considered consent. Complete publishing of the wiretaps and recordings of the telecommunications was, according to the Supreme Administrative Court, problematic and it would have been appropriate to limit the scope of the published information. The public interest of publishing the information cannot however be denied where such information informs the public of the fact that the Prime Minister was relevantly influenced in his decision-making powers by a person for whom such behaviour was not formally appropriate. This person however nevertheless communicated with employees of the intelligence services in their own private interest concerning the Prime Minister.

The Office fully reflected these conclusions of the Supreme Administrative Court in new proceedings on the given case.

2. The name, surname, date of birth and address of a passenger is fully sufficient for concluding an agreement on provision of transport with that passenger. These data are generally sufficient in concluding all private contracts. Technical realisation of performance of the concluded agreement cannot justify unlawful collection of personal data. A personal data controller must treat each set of collected personal data and the applicable consent to processing thereof individually and must therefore be able to terminate the processing thereof and destroy the data once the relevant consent to processing has been withdrawn, or if the legal grounds for the processing of personal data without consent have lapsed.

The Municipal Court in Prague, in its judgment of 7 December 2017, which was delivered 8 January 2018, dismissed the court action of the company ČSAD Karviná a.s. against the decision of the Office President of 30 July 2015. In the decision in question, the Office President confirmed the first instance decision, by which the Office imposed a fine of CZK 60 000 against ČSAD Karviná a.s. as a personal data controller for violating the obligations laid down under Section 5 (1) d) and Section 5 (2) a) to g) of Act No. 101/2000 Coll. These legal obligations were breached in that the controller processed personal data contained in a cancellation request/agreement on issuing of an electronic money instrument (EM CARD). In doing so the company ČSAD Karviná a.s. committed an administrative offence under Section 45 (1) c) and e) of Act No. 101/2000 Coll. The subject of dispute in the given matter was solely the Office's legal assessment, not the actual facts of the case.

Regarding the administrative offence under Section 45 (1) c) of Act No. 101/2000 Coll., which ČSAD Karviná a.s. disputed having committed, the Municipal Court in Prague agreed with the argument of the Office as to the redundancy of including the birth number, being of the opinion that the name, surname, date of birth and permanent address of an applicant for an EM CARD is completely sufficient. The Municipal Court in Prague also stated that it considers the Supreme Administrative Court judgment of ref. no. 7 A 58/2002–40 of 22 October 2013, from which one can infer a relatively broad range of uses for the birth number where a person must be uniquely identified, to be outdated, as it comes from a time when the birth number was not considered a special category of data within the meaning of Article 8 (7) of Directive 95/46/EC and to which the legal treatment under Section 13, or 13c, of Act No. 133/2000 Coll., on the Population Register and Birth Numbers and on Amendment to Certain Acts (the Population Register Act), implemented only after amendment by Act No. 53/2004 Coll., effective from 1 April 2004, did not apply. In the opinion of the Municipal Court in Prague, the birth number serves to identify citizens in relation to the state and its authorities. Use of certain means of technical implementation cannot justify the illegal collecting of personal data. The company in question should thus have technically ensured that the system worked so that the electronic processing equipment and relevant card or other technical means for its operations did not require a birth number. As the Municipal Court in Prague further stated: "*With regard to the development of the legal treatment, whereby it can be inferred that since 1 April 2004 it has been necessary to view the collecting of birth numbers restrictively, the plaintiff has had more than 10 years to properly adjust its system. The Court concludes with the fact that the*

plaintiff indeed already issues an ODIS card that does not require a birth number, which attests to the technical feasibility of a system that does not use the birth numbers of passengers."

Regarding the merits of an administrative offence under Section 45 (1) e) of Act No. 101/2000 Coll., the Municipal Court in Prague also agreed with the Office, stating that "*...one and the same personal data controller can collect identical personal data of the same person for the same purpose multiple times if each collection is based on a separate action, whereupon each individual collection of personal data and consents to processing thereof must be treated separately.*" A new application for a new card to be issued is thus a collection of personal data separate from previous applications for a card, and consent to personal data processing can be withdrawn separately, which shall not affect in any way the prior consent, even if the subjects involved, personal data and purpose are exactly the same. In addition the Municipal Court in Prague pointed out that "...in the case of cancellation of an application for an EM Card from a completely new applicant whose personal data it did not have from an earlier time, the plaintiff would evidently have proceeded methodologically in the same manner, i.e. despite the objection of the data subject it would keep the request containing the personal data if already labelled with a number until shredding, in which case it could not even use its argument as to the purely formal handling of data that had already been legally collected and processed before." Although the Act on Personal Data Protection does not explicitly state a deadline for when personal data should be destroyed, according to the Municipal Court in Prague it can be inferred that personal data must be destroyed without undue delay, otherwise the relevant provisions of the act aiming to protect against unauthorised collection of personal data would lack any sense.

3. The operation of automobile transport in and of itself does not constitute a highly dangerous workplace as per Section 316 (2) of the Labour Code. Application of Section 5 (2) e) of Act No. 101/2000 Coll. requires the criteria of suitability and necessity to be met.

The Supreme Administrative Court, with its judgment of ref. no. 10 As 245/2016–41 of 20 December 2017, which entered into force on 15 January 2018, rejected the cassation appeal of the company STUDENT AGENCY k.s. and upheld the decision of the Municipal Court in Prague of ref. no. 5 A 107/2013-38 of 18 October 2016.

The company STUDENT AGENCY k.s. planned to install a camera in the front part of their buses that would only make a visual recording of the driver and steward in order to protect its property, employees and transported persons, including protection of their health. The recordings were to be used when dealing with traffic accidents or passenger complaints. The company saw this as grounds for an exemption for processing personal data without the consent of data subjects under Section 5 (2) e) of Act No. 101/2000 Coll. The Office did not however permit registration of such personal data processing pursuant to Section 17 (2) of Act No. 101/2000 Coll.

STUDENT AGENCY k.s. therefore brought a court action to the Municipal Court in Prague, which however entirely concurred with the test of proportionality conducted by the Office, stacking up the interests of the employer, i.e. protection of its property and the life and health of employees and passengers, against the right of employees to privacy in the workplace. On the basis of the conducted test the Office stated that a camera monitoring the driver and

steward and their immediate surroundings is an unjustified and disproportionate encroachment on their privacy, and thus Section 5 (2) e) of Act No. 101/2000 Coll. cannot be applied in this case. The Municipal Court in Prague also stated that the justifications for the decisions of the administrative authorities of both instances of the Office are "*very rigorous, precise and logical*" , delivered in accordance with the law and the established case law. It therefore dismissed the action as groundless under Section 78 (7) of the Code of Administrative Justice.

STUDENT AGENCY k.s. filed a cassation appeal against the judgment of the Municipal Court in Prague ref. no. 5 A 107/2013-38 of 18 October 2016. The Supreme Administrative Court then stated in its decision on the cassation appeal that the decisions of the Office and the Municipal Court were correct, as in the given case the criterion of necessity for personal data processing was not met, solely the criterion of suitability. According to the Supreme Administrative Court, camera systems are not a guarantee of avoiding unwelcome events, though they do have a significant influence for example on the possibility of damaged parties making claims and preventing such actions from being repeated in the future, as well as constituting a deterrent from any unlawful behaviour from occurring. The criterion of necessity comes of the impossibility of using less invasive means to achieve the objective pursued by the personal data controller, as well as the existence of a real threat to the legally protected values of the personal data controller, which STUDENT AGENCY k.s. did not substantiate.

"*With regard to the above, the Supreme Administrative Court found that "it did not come to the conclusion that the nature of bus transport as such entails that the situations described by the complainant could take place with a high degree of probability from the nature of the matter. This can be the case for certain highly dangerous operations, i.e. situations referred to by Section 316 (2) of the Labour Code, which speaks of the special nature of an employer's activities. It can be agreed that errors in bus driving can endanger a sizeable number of persons and property. If however the court agreed that this circumstance alone constitutes a special nature of the employer's activities, it would have to profess this is the case for all automobile transport, as by violating the obligations of a road user, any driver can cause damage both to health and third party property, and to a considerable extent.*"

The Supreme Administrative Court therefore came to the conclusion that the nature of bus transport alone cannot predicate a constant increased risk for which it would be essential to monitor the interior of the bus for the whole ride.

• CERTIFICATION OF PERSONAL DATA PROTECTION

The General Regulation[6] introduces mechanisms for the issuing of personal data protection certificates, seals and marks for the purpose of demonstrating compliance with the Regulation (Articles 42 and 43). A personal data protection certificate is a document issued by a certification body, by which an entity (controller, processor, manufacturer, etc.) demonstrates that it has ensured compliance with the requirements of the General Regulation.

Issuing of certificates concerns:

1. personal data processing operations (one or more personal data processing operation)
2. products (HW, SW) and services (Recital 100)

According to the General Regulation, certificates can be issued by:

1. accredited certification bodies
2. the Office for Personal Data Protection, with the following able to issue accreditation (authorise the issuing of certification):
   1. the Office for Personal Data Protection
   2. the Czech Accreditation Institute
   3. the Office for Personal Data Protection and the Czech Accreditation Institute at the same time

Following thorough consideration and analysis, the Office placed responsibility for issuing accreditation in the hands of the national accreditation body, which is the Czech Accreditation Institute (in accordance with Regulation (EC) 765/2008 of the European Parliament and of the Council and the standard ČSN EN ISO/IEC 17065 and the requirements laid down by the competent supervisory authority). According to the proposed provisions of Section 15 of the Act on Personal Data Processing, the Czech Accreditation Institute is to be the accreditation authority by law. After the law is approved therefore, activities in issuing accreditation will be entrusted to it automatically. The main reason for this are the institute's long years of experience with this activity, its independence and the possibility of EU-wide recognition of such issued certificates.

The Office began talks with the Czech Accreditation Institute on cooperating in preparing the system for issuing personal data protection certificates so as to meet the conditions of the Regulation.

According to the General Regulation, it is essential for creating the conditions for issuing certificates for the Office to produce two fundamental documents:

- the requirements for accreditation of entities for issuing certificates
- the criteria for issuing certificates

[6] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).

The Office commenced work on preparing the draft criteria for issuing certificates (accreditation and certification criteria), which it presented for public discussion, with potential comments to have been submitted by January 2018. On the basis of the comments the text was adjusted and is prepared for being sent to the European Data Protection Board for its opinion.

It is the Board that has a significant role in influencing the creation of criteria. It is currently preparing a document concerning the implementation of certification and forming of criteria. The practice is that as soon as its instructions are complete and approved, the Office will take them into account in preparing the relevant documents.

It is important to add that submitting an application for a certificate under the Regulation is the voluntary decision of a controller, the goal of which is to demonstrate compliance with the Regulation. It is thus not a new obligation of a controller or processor. Currently it is not yet possible to apply for accreditation or a certificate.

• TRANFERS OF PERSONAL DATA ABROAD

In the first half of 2018, transfers of personal data abroad also wound down in the regime 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 the free movement of such data. This required a permit from the Office for each transfer of personal data to a country with an insufficient level of protection. The number of such requests was minimal however. To be exact, the Office received three requests for a permit to transfer personal data to third countries under Section 27 (4) of Act No. 101/2000 Coll. in the period from 1 January to 25 May 2018.

Of these three requests, one was set aside because it was a case of transfer to Israel, which is a country with an adequate level of personal data protection according to the Commission's decision of 31 January 2011. Another set of proceedings was stopped because the applicant withdrew their request following consultation with the Office. Thus in the given year the Office issued only one permit, the last under Directive 95/46/EC. Specifically this was the transfer of personal data of a travel agency's clients to the countries where they were to stay on the basis of the legal grounds laid down by the provisions of Section 27 (3) e) of Act No. 101/2000 Coll. whereby the data transfer was essential for performance of an agreement to which the data subject was a party.

The reduced number of applications can be explained by the fact that controllers were already intensively adapting to the new legal framework for personal data protection. In the provisions of Articles 44–50, the General Regulation[7] shifted the whole area of personal data transfers to third countries to a self-regulatory regime. In general it is thus the case that a personal data controller no longer need apply to the Office for a permit to transfer personal data to third countries, nor must it inform it ahead of time of such transfer.

---

[6] The General Personal Data Protection Regulation, also know as the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).

An Office permit is now only necessary in cases where the controller intends to transfer personal data to third countries with an insufficient level of protection on the basis of non-standard instruments for creating appropriate safeguards pursuant to Article 46 (3) a) and b) of the General Regulation (non-standard contractual clauses; non-binding administrative arrangements between public authorities or public bodies including enforceable and effective rights of data subjects). Even in these unconventional cases, it is less a transfer permit than approval of a non-standard instrument for the transfer of personal data that requires full application of the mechanism of consistency including a positive opinion from the European Data Protection Board. Considering the nature of such permits, it is not surprising that not only has such a permit not yet been issued in the Czech Republic, but nor has it in the whole European Union.

With the General Regulation the focus of the Office's work in the realm of data transfers shifted from permitting individual specific transfers to approving own instruments ensuring the legal transfer of data to third countries with an inadequate level of personal data protection, called appropriate safeguards under Article 46 (2) of the General Regulation. What were primarily taken under consideration were binding corporate rules, which the General Regulation promoted to one of the standard legal instruments for creating appropriate safeguards of personal data transferred to third countries.

For this reason the Office decided to actively get involved in advance in the demanding work of those supervisory authorities helping realise specific approval procedures for binding corporate rules (BCR), which to date had included almost exclusively the supervisory authorities the major "old" EU Member States. Over the course of 2018 the Office commented in the role of co-reviewer on revised BCR proposals under the three approval procedures that were still conducted under Directive 95/46/EC. In one case the Office was involved in the same role in an approval procedure already being held under the Regulation.

In this work the Office gained experience that applicants for approval of binding corporate rules are very accommodating in reacting to the recommendations and comments of co-reviewer authorities and generally amend their BCRs to the maximum recommended extent. On the basis of this it can be stated that the meticulous work of the co-reviewer contributes significantly to the quality of the resulting approved binding corporate rules, thereby increasing the global level of personal data protection overall.

At the level of the Working Group for Article 29 of Directive 95/46/EC (hereinafter "WP29"), later the European Data Protection Board, the Office took active part in the work of the International Transfers sub-group in preparing interpretative statements and other auxiliary materials for the field of personal data transfers to third countries. In the realm of BCRs, a number of guidance documents were finalised and issued for the General Regulation regime for the groups of companies that choose to formulate their own binding corporate rules:

- Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors under the General Regulation (WP263)
- Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data (WP264)
- Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data (WP265)
- Working Document setting up a table with the elements and principles to be found in Controller Binding Corporate Rules for controllers (WP256)

- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP257)

In addition to these practical documents, the principles for evaluating an adequate level of personal data protection in a third country "Adequacy Referential" were also finalised (WP254). The validity of all the aforementioned documents was confirmed at its first session of 25 May 2018 by the European Data Protection Board.

It also approved two more important explanatory documents. These were the Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 and Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). The latter document was submitted for public discussion at the end of 2018.

The Office also volunteered to help formulate the Board's position on the Commission's draft decision on an adequate level of data protection in Japan, taking part in consultations with Commission representatives and representatives of the Japanese supervisory authority (the Perso¬nal Information Protection Commission, PPC) and many other personal meetings and teleconferences of the working team. On this team the Office was assigned with the responsibility of evaluating the correctness of the Commission's steps in applying the principles of integrity and confidentiality, minimising the retention period, and transparency.

The working team identified several weak points, above all however it had to deal with a fundamental issue concerning the nature of the Commission's proposed decision – an adequate level of data protection in Japan is not declared in the Commission's decision for the whole Japanese legal system, but is limited to private entities that abide by the Japanese Act on the Protection of Personal Information (APPI) and to European data. For these a special regime of protection has been created, guaranteed with Supplementary Rules by the PPC, which are an annex to the Commission's decision. It can thus be stated that the system of adequate protection does not apply to the whole country, but to certain sectors, or is in fact more similar to the personal data safeguards under Article 46 of the General Regulation. The situation was similar in the case of the Commission's decision on adequate protection provided by the EU-USA Privacy Shield.

The Office will also push for a deciding role in formulating the interpretation of the relationship between application of Article 3 and Chapter V of the General Regulation, with nothing less at stake than the explicit definition of personal data transfer to third countries, among other things.

• SCHENGEN COOPERATION

Great emphasis is placed on the protection of personal data processed under 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 national supervisory authority overseeing compliance with the applicable regulations, thus contributing to the protection of fundamental rights of persons whose personal data are the

subject of processing within the Schengen area. Additionally, an authorised Office representative regularly attends the coordination groups that have been established for the individual systems. These also include the specially created Europol Cooperation Board, which has been functioning since 2017.
Aside from standard supervision and inspection associated with the requirements for lawful processing of personal data by the controllers of the aforementioned systems, in the past year the Office also took on extensive inspections of the national components of SIS II, CIS and VIS, as well as commenting on the newly emerging legislation for certain systems.

ACTIVITIES OF INDIVIDUAL COORDINATION GROUPS IN SCHENGEN, VISA AND CUSTOMS COOPERATION

The following topics were pervasive across all groups in 2018:

- interoperability of information systems
- positions and opinions on legislative changes
- the issue of future supervision in light of extensive legislative changes in personal data protection

In the realm of interoperability, the three coordination groups (SIS II SCG, VIS SCG, Eurodac SCG) sent out a joint letter supporting the critical position of the European Data Protection Supervisor (*EDPS*), Working Party 29 (*WP29*) and the European Agency for Fundamental Rights (*FRA*). The addressees were the European Commission, Parliament and Council.

Recommendations were regularly updated on the basis of assessments of Member States carried out on application of the Schengen acquis (for SIS II SCG and VIS SCG).

Certain long-term projects and studies were also completed under the groups. For example, the joint plan for conducting inspections of the Customs Information System (the Office had taken part in drafting it in the past as lead rapporteur), studies concerning logging at the national level in SIS II and a study on implementation of Article 41 of Regulation (EC) No 767/2008 of the Council of 9 July 2008 concerning the Visa Information System and the exchange of data between Member States on short-stay visas, and a guide on data subjects exercising their rights within Europol.

CURRENT ISSUES BEING ADDRESSED IN THE CORDINATION GROUPS

The SIS II Supervision Coordinator Group (*SIS II SCG*) regularly updates the appropriate recommendations for Member States arising from Schengen evaluations. This activity is coordinated with the group for the VIS. Another regularly updated document is the guide for data subjects for accessing data processed in SIS II. Currently the group is working on a study that should provide an overview of national legislation and practices in Member States in entering alerts on persons and things for the purpose of discreet or specific checks according to Article 36 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

At the end of 2018, the Coordination Group for VIS (*VIS SCG*) completed preparation of a letter to the European Commission, Parliament and Council reflecting the group's position on the new legislation governing VIS. The group identified major points of concern that could

raise certain doubts from the perspective of personal data protection. No less intensely was it occupied with a study that is to map out data protection training for authorised employees of authorities with access to VIS. The final document draft is expected at the next meeting in June of 2019.

At the end of the year the Eurodac Supervision Coordination Group (*Eurodac SCG*) finalised a case document dealing with the premature erasure of data in the case the person in question acquires citizenship of a Member State, and a study concerning the exercising of data subject rights with respect to Eurodac. The final form will be voted on at the next meeting in June 2019.

The Supervision Coordination Group for the Customs Information System (*CIS SCG*) updated its guide for data subject access to information in CIS. The joint format for CIS inspection, to which the Office contributed in the past as lead rapporteur, and the module for inspecting data security were also updated. A questionnaire has been prepared for inspection of the security policy of AFIS (Anti-Fraud Information System).

The Europol Cooperation Board (ECB) drew up a opinion on the monitoring mechanism of Europol in the context of Article 39 of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol). Among the other main activities of the group were drafting a practical guide for national Europol units and an information pamphlet for data subjects.

NUMBER OF SUBMISSIONS, COMPLAINTS AND QUESTIONS AND HOW THEY WERE DEALT WITH

Another of the Office's obligations is dealing with received submissions from data subjects concerning the processing of their personal data in SIS II. In 2018 the Office received a total of 22 submissions, in three cases reviewing the actions of the Police of the Czech Republic in processing personal data. In one case it also took part in cross-border cooperation among supervisory authorities in connection with the right of access to personal data processed in SIS II.

The Office furthermore received 19 submissions in which 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 the Office, the individual petitioners were referred to the Ministry of Foreign Affairs, and in one case to the Police of the Czech Republic. 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 regularly conducted in each state of the Schengen area. Among these are the Schengen Information System, the visa policy, police cooperation, external borders, returns and protection of personal data. The evaluation teams are always formed ad hoc for the individual evaluations. They are made up of representatives of the European Commission and experts from Member States, or representatives of the European

Data Protection Supervisor (EDPS). On the basis of submitted documents and a subsequent inspection, the evaluation team prepares a report summarising its findings on the compliance of practice in the given Member State with the requirements of the Schengen acquis. This inspection generally includes a visit to the police body that provides for operation of the national component of the Schengen database, the data protection authority, and other affected i nstitutions.

In November 2018, an Office employee took part in an evaluation mission in Lithuania as a national expert. In 2019 an evaluation is to take place in the Czech Republic.

Analytical Activities

The Analytics Unit has been performing tasks assigned within the jurisdiction of the Office for Personal Data Protection (the Office) since mid-2016. After the General Data Protection Regulation (General Regulation)[8] entered into force in May 2018, the meaning of analytical work increased even further. Protection of personal data and privacy, which is the goal of the General Regulation, requires a reassessment of the existing approaches and new methodological procedures in applying the right to data protection. Although the General Regulation is based on continuity with the previous legislation, it is characterised by a number of changes, the purpose of which is to more effectively protect the basic rights that it governs, above all the right to protection of personal data and privacy. On the basis of the principle of proportionality however it also takes into account other fundamental rights.[9]

The starting point for working with the Regulation is application of its general principles. On top of this the Regulation contains new rights that must be implemented in data protection (right to portability, impact assessment, incident reporting). In this regard an important instrument for proper practice by controllers and processors are the positions and opinions of the European Data Protection Board (EDPB), previously the Article 29 Working Party (WP29).[10] Analytical analysis is the prerequisite for a deeper understanding of the issues and finding a balanced relationship between technological development and personal data protection. On this basis new specific solutions will emerge ensuring compliance with data protection. In searching for solutions, the dynamic development of new technologies must not be neglected, as this increases the demands on the expertise of all those who are to protect personal data and privacy.

---

[8] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[9] Recital 4 of the General Regulation.
[10] The Wokring Party of the protection of individuals with regard to the processing of personal data was established on the basis of Article 29 of Directive 95/46/Ec (the *Article 29 Working Party*, hereinafter WP29). After the General Regulation entered info force, its tasks were taken over by the European Data Protection Board (EDPB(.

In the past year, the Analytics Unit specifically provided statements or analyses on issues of data protection and privacy to state authorities and institutions including courts and took part in providing for the Office's educational and awareness activities, as well as providing consulting including cooperation in providing answers to questions from the public. In carrying out these tasks, it drew on the assumptions, principles and provisions of the currently valid regulatory framework for protection of personal data and privacy in the Czech Republic and the EU. On this basis it formulated its conclusions or recommendations in relation to the presented problems. Of the issues that the Analytics Unit dealt with systematically last year, we can mention the data protection requirements in relation to medical registers, to keeping DNA databases, and the retention of telecommunication records. The following text will address the significant aspects of personal data protection in relation to these topics.

MEDICAL REGISTERS

Generally speaking, the Office does not have objections to the establishment and existence of medical register systems, assuming their goal is to utilise the possibilities currently afforded by technological development to optimise medical systems and efficiently allocate funding collected under the health insurance system. It must however be taken under consideration that medical registers collect large amounts of data. If these databases do not contain personal information, they do not present a risk in terms of personal data protection. However the majority of currently generated data do contain personal data, and large data sets increase the risks for human privacy and personal data protection. The value of this information does not consist solely in its primary purpose, but also in its secondary application, i.e. processing for purposes other than those for which it was originally collected. The collection of a large volume of data can not only engender threats to personal data and privacy, but also to the neglecting of ethical questions, human dignity and human individuality. Large-scale data are also often mentioned as a potential risk in the already effective General Regulation. An instrument that is meant to comprehensively address serious issues of the relationship between technological development and protection of data and privacy and set criteria for considering the level of appropriate encroachment on privacy is the new regulatory framework for data protection in the European Union, in particular the General Regulation. At the same time, the legal framework for data protection based on general principles leaves more room for controllers (processors) to ensure compliance with the legislation compared to regulation based on detailed rules.

In terms of health data, the General Regulation considers these personal data and defines them as data related to the physical or mental health of a natural person. This includes data on the provision of health care services which reveal information about that person's health status. The General Regulation explicitly classifies these data in a special category of personal data for which there is a strict regime of treatment. It bases this on the fact that health data, which are by their nature sensitive and subject to ethical standards and the obligation of medical confidentiality, require an especially high level of protection. In terms of processing special categories of personal data, Article 9 of the General Regulation prohibits this unless there is a derogation under Article 9 (2). Since the General Regulation has taken effect therefore, a controller must carefully consider whether any of the ten exceptions in the aforementioned second paragraph apply. Processing of personal data in medical registers is generally not based on consent from data subjects, although the institution of consent is generally supreme and

primary in terms of fulfilling the right to informational self-determination. The legal grounds for processing in this case is legal obligation, though only assuming there are sufficient safeguards for protecting personal data.

In assessing whether health data can be processed at all, or what measures should be implemented to protect them, it is necessary to draw for one thing on the general principles of the General Regulation, and for another taking into account the structural principles on which the General Regulation is based. Practically speaking, proper application of the general principles of the Regulation means posing the question of whether there is legal grounds for processing, whether the data are minimised and whether they are being processed only for the requisite period. This also includes the fundamental requirement of transparency of personal data processing, to which the informative obligation of a controller is tied. Of the new institutions that the General Regulation brings to the table, it is important to emphasise the institution of data protection impact assessment. In the case of medical registers, which process sensitive data on a large scale, this should be a matter of course, which also follows from the recitals of the General Regulation. Also important is the principle of protecting privacy starting with the design (privacy by design), which requires the default settings to prevent threats to personal data from ever occurring. Of the structural principles of the General Regulation, we should mention for example a risk-based approach, which assumes more fastidious measures in the case of greater risk, and also a preventive approach, which means that approaches must be chosen that prevent threats to or breaches of personal data. Specifically, in many cases it is not necessary for controllers to collect personal data, it is sufficient to work with anonymous data, which the General Regulation does not consider personal data.

Protection of personal data and data subject rights must not be forgotten in the context of medical registers. The current legislation has certain shortfalls in this regard, because the principles and rules of data protection have not yet been sufficiently reflected in the legal treatment of medical registers. In this regard one guideline could be the finding of the Constitutional Court Pl. ÚS 1/12 of 27 November 2012,[11] which refers to the validity of general principles applicable to personal data processing and application of the principle of proportionality on the basis of the criteria of appropriateness, necessity and proportionality. The cited ruling intelligibly presents the principles that are to be applied to all medical registers.[12] At the same time it is evident from the purpose of medical registers, as the law lists under Section 70 (1) and Section 73, that anonymised data would often serve the same purpose. In this regard it would be sufficient if medical facilities passed along to the National Health Information System anonymised data, which could naturally not become the target of a leak. It must be added that if in the meantime from ruling Pl. ÚS 1/12 the General Regulation has increased the standard of personal data protection over the previous Directive 95/46/EC, the requirements for protection of personal data and privacy must also have grown, as these are fundamental rights protected by the constitutional order.

---

[11] http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-1 -12

[12] It would therefore be ideal if the legislature, when adopting the new legislation for the National Register of Medical Workers, carefully considered to what extent from these perspectives the other registers that make up the National Health Information System stand up, and with timely intervention rectify any potential shortcomings that could lead to the violation of the rights of patients, medical workers and other persons to informational self-determination.

DNA DATABASES

DNA databases have long been a topic in data protection. A systematic approach to the issue of genetic and biometric data can be found above all in the interpretational opinions of WP29.[13] DNA is discussed in the framework of personal data protection in connection both with genetic data and with biometric data, with which it shares characteristic properties. The aforementioned opinions contain collective points for the processing of biometric and genetic data in relation to protection of data and privacy. For example, the WP29 Working Document on Genetic Data from 2004 first stated that "*there is no doubt that genetic information content is cover by [the definition of personal data]*". It was also stated in this material that national authorities are becoming increasingly aware of the risks associated with the processing of genetic data, and thus it is necessary to couple genetic technologies with adequate safeguards to protect the right for privacy. A general trend towards new initiatives at the national level is anticipated.

WP29 Opinion 3/2012 highlighted both the affordability of the technology and the fact that the systems that analyse DNA can be highly effective in helping to fight crime and reveal the identity of an unknown person suspected of a serious crime. It also pointed out that the use of such systems on a large scale can produce serious side effects for the protection of privacy. In the case of DNA this is especially the risk that DNA technologies cannot ensure complete accuracy and there is always a risk of wrongful identification in the form of a false positive or false negative result, which affects the rights of the individual including possible discriminatory consequences. In the case of DNA there is also the risk they could reveal sensitive data on the health of the person or racial or ethnic origin. It also points out the danger of centralised storage of DNA, which could lead to the interconnection of databases (creating detailed profiles of an individual) and the specific dangers of the reuse of such data for incompatible purposes, especially in the case of unauthorised access.

Opinions on biometric and genetic data have gradually evolved, yet increasingly the approach has been advocated that with regard to the extremely unique nature of genetic data and their association with information that could reveal the state of health or ethnic origin, these data should be treated as "particularly sensitive". Discussion on the nature of these data continued for the whole duration of preparations of the General Regulation, and only in the final phase of preparations was it decided that for one thing genetic data would be defined as sensitive, and for another they would be defined in the General Regulation (and thus also in the directive on enforcement of rights) as a separate category. Article 9 (1) classified the "processing of genetic data for the purpose of uniquely identifying a natural person" under a special category of personal data which the General Regulation grants a special, i.e. stricter, regime in terms of protection. Specifically this means that their use is prohibited except in the case of an explicit exception under Article 9 (2).

Among the long-term serious problems of data protection in the Czech Republic are issues associated with the collection of DNA samples obtained by the police in connection with crimes or the investigation thereof. This area is governed by Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for

---

[13] Working Document on Biometrics adopted on 1 August 2003.
Opinion 3/2012 on developments in biometric technologies adopted on 27 April 2012.
Working Document on Genetic Data adopted on 17 March 2004.

the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Law Enforcement Directive). This directive reacts to the specific nature of police and judicial cooperation on criminal matters and contains special rules for the protection of personal data. The transfer of data to third countries and between organisations should be facilitated while ensuring a high level of data protection. The technologies that allow for personal data to be used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must therefore be accompanied by adequate measures.[14] The directive will be adopted into the national legislation in the Czech Republic through an adaptation of the Act on Personal Data Processing, which has not yet been adopted.

The principles for processing of personal data derive from Recital 26 and Article 4 of the directive. "Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review."[15]

The WP29 Working Party issued an opinion on some key issues of the Law Enforcement Directive (2016/680) on 27 November 2017, which contains some practical recommendations, for instance:

- National laws on data processing within the scope of the Directive always should foresee maximum storage periods as well as periodic reviews of the necessity to keep the respective data. The review proceeding should be documented and the decision to extend the data storage period should be duly justified.
- The principle of data protection by design should be specifically implemented within this context to promote compliance with the data quality principles. Existing and future databases should be (re-)organized in a way that ensures periodic reviews to take place automatically as well as automatic deletion of data after reaching the maximum storage period.
- The assessment on the need to further store the data, as well as the establishment of maximum storage periods should reflect the different categories of data subjects.

[14] Articles 3 and 4 of the Law Enforcement Directive.
[15] Recital 26 of the Law Enforcement Directive.

It can be summarised that the keeping of a DNA database undoubtedly encroaches on the right to data protection and privacy of individuals and measures must be adopted to protect them in accordance with the directive. In terms of the situation in the Czech Republic, no provision of the Act on the Police of the Czech Republic contains express authorisation to keep a database of DNA profiles. Also lacking in this act is addressing of stricter conditions for keeping a database, such as an exact delimitation of the time limits for retaining profiles, or a more detailed treatment of destroying personal data. In the opinion of the Office, the scope of crimes that allow for a sample to be placed in a database should also be narrowed. Currently the treatment of personal data records for the purposes of identification in the Act on the Police of the Czech Republic is highly fragmentary. The possibility of establishing such can only be inferred through interpretation. The lack of specific time limits for keeping records and more specific conditions for deletion are currently laid down in the police's internal regulations.[16] This has been the target of repeated criticism, as detailed rules are not set out by a generally binding regulation easily accessible to the public. In the opinion of the Office the aforementioned issues should be rectified.

RETENTION OF TELECOMMUNICATION RECORDS

Telecommunication operators (legal or natural persons providing a public telecommunication network or providing a publicly accessible electronic communication service) are obliged in the Czech Republic to retain the traffic and location data processed in providing their public service for six months. Traffic and location data are, in particular, data allowing the tracing and identification of the source and recipient of a communication as well as ascertaining the date, time, manner and duration of the communication, but not its content. Under the conditions laid down by the legislation, such data can be demanded by, in particular, the criminal authorities, the Police of the Czech Republic, the Security Information Service and Military Intelligence Service, and in some cases the Czech National Bank. The obligation to retain all traffic and location data was imposed on telecommunication operators in EU Member States in 2006 by a directive known as the Data Retention Directive.[17] Its purpose was to retain traffic and location data on the grounds of crime prevention and the fight against it. This directive was adopted after the terrorist attacks of 11 September in reaction to the increased need for security. Nevertheless after the directive was issued, opinions arose that the retention of telecommunication records represents a serious encroachment on privacy that should be set up with much greater sensitivity. This is illustrated by expert material from WP29, case law of the EU Court of Justice, and a ruling of the Czech Constitutional Court. The valid legislation on retention of telecommunication records should also take into account the criteria following from these materials listed below.

---

[16] Detailed rules on the basis of which the National DNA Database is kept are contained in the binding instruction of the police president No. 250/2014, on identification operations. This instruction not only governs the internal affairs of the Police of the Czech Republic, but also deals with issues of deleting data and the processing period for specific personal data. For example, the period for retaining a profile is automatically set up to 100 years of age of the person (Article 68 of the instruction).

[17] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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.

OPINION OF THE WP29 EXPERT GROUP ON THE ISSUE OF TELECOMMUNICATION RECORD RETENTION

Several materials of WP29 have expressed an opinion on the issue of retaining telecommunication records from the perspective of protecting personal data and privacy.[18] Even in the period of theoretical discussions and considerations on adopting the Data Retention Directive, it was WP29 who was the first to point out[19] the need for a balanced approach in the fight against terrorism. Specifically it stated that these measures have a direct and indirect impact on the protection of personal data. It pointed out the commitment of democratic societies to ensure respect for the fundamental rights and freedoms of the individual, with the right of an individual to protection of personal data being part of these fundamental rights and freedoms. Measures that are simply "useful" or "wished" may not restrict the fundamental rights and freedoms. WP29 also expressed concern over an increasing tendency to represent the protection of personal data as a barrier to the efficient fight against terrorism and called for the standard of human rights not to be lowered.

A further evaluation of the issue and proposal for practical steps to remove certain risks in Report 01/2010[20] pointed out that the Directive has far reaching consequences for all European citizens. Measures associated with the decision to oblige providers of telephone and internet services to retain traffic data of all their subscribers and users encroaches on the daily life of every European citizen and may endanger the fundamental values and freedoms that they enjoy. Any restrictions on individuals' rights of privacy and data protection must be necessary, appropriate and proportionate within a democratic society and serve specific public purposes such as national security, defence, public security, or the investigation, detection and prosecution of crimes. As a bare minimum, such restrictions must respect the rights, freedoms and principles laid down in the Charter of Fundamental Rights of the EU as well as the European Convention for the protection of human rights and fundamental freedoms. In terms of specific safeguards in relation to service providers, WP29 asked that safeguards be introduced at least with regard to purpose specification, access limitation, data minimisation, prohibition on data mining, judicial/independent scrutiny of authorised access, ban on the use by providers of the data that is retained solely for public order purposes under the DR Directive.

The cited report furthermore stated that the availability of traffic and location data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression. These scenarios are likely to occur both because of intentional activities and on account of negligent retention mechanisms. In light of these facts, implementation of the Data Retention Directive by electronic communications and internet service providers is associated with an inherently high risk level that requires appropriate technical and organisational security measures. For the above reasons it came to the conclusion that, inter alia, it is essential to give broad enforcement powers to supervisory authorities to protect personal

---

[18] This was an expert group comprised of representatives of supervisory authorities that deal with personal data protection that has now been replaced by the European Data Protection Board.

[19] *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism (adopted 14 December 2001).*

[20] *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive - WP 172.*

data, including the powers to demand access to business confidentiality and implement a number of auxiliary sub-measures. It was proposed that reducing the maximum retention period be considered along with setting a single, shorter term and ensuring appropriate technical and organisational measures to minimise the risk of accidental and/or unauthorised destruction or alteration of the data along with the risk of unauthorised access and/or processing. Providers must assess the risks of processing regularly and objectively. Also appropriate would be regular external audits which contribute to independent and objective risk assessment.

Case Law of the Czech Constitutional Court

In the Czech Republic, the Constitutional Court commented on the issue of telecommunication record retention in its ruling Pl. ÚS 24/10 of 22 March 2011,[21] in which it assessed the contested legislation from the perspective of constitutional requirements and found a number of errors. It stated that the contested provision of Section 97 (3) of the Act on Electronic Communication contains only a vague and imprecise designation of the obligations of legal and natural persons that retain traffic and location data. There is no clearly and precisely defined purpose for which the traffic and location data are provided to authorised authorities, which makes it impossible to judge the contested legislation in terms of its necessity. The contested legislation does not lay down clear and detailed rules containing the minimum requirements for security of retained data, in particular in the form of restricting third party access, setting procedures to protect the integrity and confidentiality of data, and the procedures for their destruction. The Constitutional Court also criticised the contested legislation in that the individuals concerned do not have sufficient safeguards against the risk of abuse and arbitrariness, and the time limit for data retention is unclear. The court also expressed doubts over whether the instrument of blanket and preventive retention of traffic and location data on nearly all electronic communication is essential in terms of the intensity of encroachment on the private sphere. For this reason the Constitutional Court annulled the provisions of Section 97 (3) and (4) of Act No. 127/2005 Coll., on Electronic Communication, and the related contested Decree No. 485/2005 Coll.[22]

Criteria for data retention stemming from EU Court of Justice case law

The judgment of the EU Court of Justice on the case Digital Rights Ireland (and Tele2 Sverige AB),[23] which invalidated Directive 2006/24/EC in relation to restricting monitoring of communication data (telephone, text messages, e-mail, internet communication) referred to the values of protecting fundamental rights and stated that Directive 2006/24/EC constitutes in itself an interference with the rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the EU. In addition, the access of competent national authorities to personal data constitutes another wide-ranging and particularly serious interference with those fundamental rights. Although it does not interfere with the essence of these fundamental rights, as the

---

[21] http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10

[22] The Act On Electronic Communications was amended on the basis of the Constitutional Court ruling with amendment no. 4680/2011 Coll. The Constitutional Court ruling was preceded by the judgment of the EU Court of Justice on Digital Rights Ireland.

[23] Judgment of the Court of 8 April 2014 in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd. and Judgment of the Court of 21 December 2016 in Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB."

directive does not apply to the content of communication, it is still an encroachment on these rights. The fact that the data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of persons concerned the feeling that their private lives are the subject of constant surveillance.

According to the judgment, in assessing interference with the rights guaranteed by Article 7 and 8 of the Charter of Fundamental Rights of the EU[24] it is necessary to follow the requirements of Article 52 (1) of the Charter, which provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. As regards the question of whether that interference satisfies an objective of general interest, the material objective of that directive is to contribute to the fight against serious crime and thus, ultimately, to public security. In this sense, the case law of the Court has confirmed that the fight against international terrorism in order to maintain international peace and security and the fight against serious crime constitute objectives of general interest of the EU.

Aside from the meeting the requirement of a general objective it is also necessary to respect the principle of proportionality, which according to the settled case law of the EU Court of Justice requires that acts of EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives. As for the requirement of limiting interference to fundamental rights to what is strictly necessary, Directive 2006/24/EC did not meet this in many regards, as stated by the EU Court of Justice judgment, for example:

- it did not require any relationship between the data whose retention is provided for and a threat to public security and was not restricted to a retention in relation to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved in a serious crime
- it failed to lay down any objective criterion for access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions
- it did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use
- it did not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued
- the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body

[24] Article 7 of the Charter of Fundamental Rights of the EU Respect for Private and Family Life reads: Everyone has the right to respect for his or her private and family life, home and communications.
Article 8 of the Charter of Fundamental Rights of the EU Protection of Personal Data reads:
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

- no distinction was made between the categories of data set out in Article 5 of the directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned
- retention was not based on objective criteria in order to ensure that it is limited to what is strictly necessary
- sufficient safeguards were not laid down, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data, and no specific obligation on Member States to establish such rules was laid down
- it was not ensured that a particularly high level of protection and security is applied by providers by means of technical and organisational measures
- the irreversible destruction of the data at the end of the data retention period was not ensured

It follows from the above summary of the shortcomings of Directive 2006/24/EC that clear and precise rules governing the extent of the interference with fundamental rights to protect personal data and privacy were not laid down and that the directive represented a far-reaching and particularly serious interference with fundamental rights in the EU legal code without such interference being limited to the essential minimum. Adoption of Directive 2006/24/EC thus surpassed the bounds laid down by the requirement to observe the principle of proportionality in terms of Article 7 and 8 of Article 52 (1) of the Charter, which led to the conclusion of the evaluated directive being invalid. The reasons for invalidity of the directive should naturally also be considered when considering the national legislation of EU Member States that were adopted on its basis.[25]

[25] Proposal of the Constitutional Court Pl. ÚS 45/17 to annul Section 97 (3) and (4) of Act No. 127/2005 Coll., on Electronic Communications and Amending Certain Related Acts, as amended; proposal to annul Section 68 (2) and Section 71 a) of Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended; proposal to annul Section 88a of Act No. 141/1961 Coll., the Criminal Code, as amended; proposal to annul Decree No. 357/2012 Coll., on the Storage, Transfer and Disposal of Traffic and Location Data.

Legislation

On 12 July 2018 the government received the confidence of parliament and the legislative process thus returned to its standard form. Amendments however continue to be favoured over legislative plans and new acts. The names of the amendments are in many cases formal instead of expressing what they actually do. The government asked for the Office's position on certain initiatives, generally deputy-initiated, and only sporadically draft laws. In 2018 the Council of the EU made 284 documents concerning personal data protection public out of 15 836 total.

Impact assessment of proposal on protection of privacy and personal data

A Data Protection Impact Assessment (DPIA) has been an obligatory component of explanatory memoranda or justifications since 1 January 2013, which is updated with Article 35 of the General Regulation. Unfortunately, despite the new requirements for DPIA quality laid down under the General Regulation[26], even after five years its form is still not optimal. The Office has thus prepared a guideline in which it explains what a DPIA in legislation should look like.[27] As a rule, assessments where the submitter has invited a Personal Data Officer to create them can be evaluated positively.

Implementation of the new EU regulatory framework

In 2018 the Office also dealt with implementation of the new EU regulatory framework for personal data protection (the General Regulation, JHAD[28] & PNRD[29]).

---

[26] The General Personal Data Protection Regulation, also known as the GDPR (Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC).

[27] https://www.uoou.cz/navod-k-posouzeni-vlivu-na-ochranu-osobnich-udaju-u-navrhu- pravnich-predpisu-dpia/ds-5344

[28] DIRECTIVE 2016/680 (EU) 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 competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[29] DIRECTIVE (EU) 2016/68 OF THE EUROPEAN PARLIAMENT AND 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

The draft Act on Personal Data Processing and the accompanying law have been significantly delayed. Only on 21 March 2018 did the government approve it and since that time the Chamber of Deputies spent the whole rest of the year discussing it.

The Office provided the cabinet with a broad opinion on the initiative draft amendment to the existing Act on Personal Data Processing, in which it primarily pointed out the unsystematic nature of exempting all local governments from administrative punishment under the General Regulation. Deputies then withdrew the draft from discussion.

Electronic public administration

The most major piece of news was the practical fulfilment of eIDAS[30] and Act No. 250/2017 Coll., on Electronic Identification. This was reflected as the launch of the NIA (https://www.eidentita.cz) and "Citizen's Portal" (https://obcan.portal.gov.cz). The Office supported the end of including birth numbers on ID cards. The Interior Ministry wants to develop e-government with the concept Registry 2.0.

The Office also took up the issue of electronic identification with the Czech Office for Surveying, Mapping and Cadastre and the Ministry of Health. From the start of 2018 the State Institute for Drug Control has been allowing each patient to view their pharmaceutical record. A new bill will also make it available to physicians, with data protection safeguards.

The draft plan for an Act on eHealth should bring a fundamental change to healthcare. Its essence is the indexing of medical records and a reform of the NZIS registers.

Private law

The Ministry of Justice has prepared a draft amendment to the new Civil Code that is to allow a change of sex without surgery. The Office rejected it as a whole due to it being premature and not well thought through. The Ministry of Justice also proposed extensive changes to the Act on Corporations, which was discussed in 2018 as parliamentary paper 207.

Transparency

The government asked the Office to comment on the initiative draft for partial transposition of the 4th AML[31] Directive in the wording of 5AMLD,[32] which is meant to make public the Ultimate Beneficial Owners – parliamentary paper 318. The Office recommended that the government not agree with the proposal, in particular due to insufficient DPIA and the absence of more privacy safeguards from the 5AMLD recitals; i.e. insufficient protection of personal data. The government took a neutral standpoint on it.

Privacy in electronic communications

The draft Regulation concerning respect for private life and the protection of personal data in electronic communications (CELEX[33]: 52017PC0010) is meant to replace the existing Directive

[30] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[31] Money laundering.

[32] DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

[33] Communitatis Europeae Lex

2002/58/EC. The most controversial issues with this proposal are data retention, processing of metadata and electronic communication content, cookie walls, browser settings and the relationship to the General Regulation. In light of the politically sensitive content and the impact of this proposal on other sectors, the Austrian EU Presidency decided not to continue on to the next phase – trialogue with the European Parliament and European Commission. At the December Telecoms Council, only a progress report was approved. Due to many unresolved issues, it is not expected that the proposal will have been approved by the end of the European Parliament term.

Progress is also taking place in the field of artificial intelligence and blockchain, i.e. technologies that have an impact on fundamental human rights such as the protection of privacy and personal data.

Disinformation campaigns

The proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament aims to improve protection against cybersecurity incidents in the fight against disinformation campaigns in connection with the European Parliament elections in May of 2019.

Directive 2013/40/EU of the European Parliament and of the Council harmonised the definition of crimes and adjusted the minimum and maximum level of sanctions in connection with attacks against information systems. In this context it stated that attacks against information systems are an aggravating circumstance.

The European Commission also recommends that every Member State establish a domestic election network. This would include all bodies that monitor online activities. Such a measure would facilitate the exchange of information and at the same time allow findings to be shared and rules to be enforced. At the end of the year the Office was approached to participate in the activities of this network.

Free flow of non-personal data

Following the general approach of the EU Council, at the start of October 2018 the European Parliament approved the regulation on the free flow of non-personal data. This is meant to help create a competitive data-based economy under the single digital market. It will also ensure the free movement of data across borders. Member States will be obliged to notify the European Commission of all remaining or planned restrictions concerning data localisation in specific defined situations during data processing by public authorities. This regulation will complement the General Regulation with the aim of facilitating the free movement of all data (personal and otherwise), thereby creating a single European data space.

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

The Code of Administrative Procedure allows those who are not satisfied with the results of administrative authorities, including the Office, to lodge a complaint under Section 175 of the Administrative Procedure Code.[34] Specifically, the persons concerned can approach the administrative authorities with their complaints on inappropriate behaviour by public officials or against the approach of an administrative authority. Complainants have this option if the Administrative Procedure Code does not offer them any other means of recourse, i.e. in particular an appeal or other due or extraordinary remedial means.

In 2018 the Office dealt with a total of twelve complaints submitted on the basis of Section 175 of Act No. 500/2004 Coll. In the majority of cases the complainants were dissatisfied with how their prior submissions concerning possible violation of the data protection legislation had been dealt with. Last year only two of the total of twelve complaints were found to be justified and seven were found to be unfounded. The Office will deal with three of the complaints, which it received at the end of 2018, in 2019.

Despite the fact that the Office recorded a marked increase in the number of complaints directed against personal data controllers or processors in connection with the General Regulation taking effect, the number of complaints under Section 175 dropped compared to the previous year.

---

[34] Act No. 500/2004 Coll. of 24 June 2004, the Code of Administrative Procedure

If we look at the individual complaints more closely, in ten cases the complaints were against the actions of the Department of Consultation Agendas, which methodologically manages the complaints and consultation agendas. Complainants predominantly submitted complaints due to disagreement with how their prior submission had been dealt with, having been set aside by the department without any measures taken. In such cases the manner in which the complainant's prior submission had been dealt with was investigated. In one case the complainant again did not agree with how their complaint was dealt with and turned to the Office President. In this case as well, the prior actions of the Office were found to be justified and the complaint was evaluated as groundless. When reviewing of a complainant's submission did uncover suspicion of a violation of Act No. 101/2000 Coll. or the General Regulation, the submission was passed along to either an Office inspector to conduct an inspection, or the Supervisory Department to commence administrative proceedings on suspicion of an administrative offence or misdemeanour. In two cases the complainants turned to the Office with a complaint against the conclusions of its inspection procedures or how Office inspectors ran an inspection. In both cases the complaints were found to be groundless.

In all the above cases the complainant was informed of the result of the investigation. The relevant Office department was also informed of how the complaint was deal with.

Of the twelve complaints that the Office received, none of them were for inappropriate behaviour by public officials. Overall it can be stated that in carrying out its mandate the Office acts professionally, responsibly and in accordance with the principles of good governance.

International cooperation

In recent years the scope of the Office has gradually expanded in the field of what is now the former WP29. Over the past year this trend has taken leaps and bounds and its role in the activities of the newly established European Data Protection Board (formerly WP29) has undergone a qualitative change. In four cases, Office employees have become members of proposal groups, specifically for the following tasks:

- Analysis of lists under Article 35(4) submitted to the Board – lists of processing operations subject to the requirement of a data protection impact assessment

On the basis of Article 35 of the General Regulation[35], the Office has prepared a list of types of operations that are subject to data protection impact assessment. In February and March of 2018, a public discussion took place on the proposed list and in June the draft list was sent to the European Data Protection Board. At the same time the Office volunteered for cooperating on analysing the lists sent by other Member States.

Analysis of the first 23 lists took place in July and August and the result was drafts of opinions prepared for the plenary session of the Board in September 2018. At its session the Board approved the opinions and presented them to the individual Member States to be dealt with as part of ensuring the mechanism of consistency. An evaluation of further lists (including Norway and Liechtenstein, which are members of the EEC) took place in October and November of 2018. The Office prepared a document addressing the comments and suggestions listed in the opinion on the list it had prepared and sent the modified document back to the Board, stating that the preliminary draft opinion showed that the modifications made were sufficient and that the list is thus compliant. After definitive approval by the Board it anticipates publishing the list on the Office website.

[35] The General Personal Data Protection Regulation, also known as the GDPR (Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC)..

- Preparation of guidelines on video surveillance

The European Data Protection Board began work on the next in a line of guidelines focused on a practical and thematically focused interpretation of the provisions of the General Regulation, this time on the field of surveillance by camera systems. The Office became a member of the research team. Aside from theoretical background, i.e. explaining the scope of application of the General Regulation and the legal basis, the document will have a practical focus on the needs of camera system users, as well as providing information to individuals as data subjects. Through a series of examples from practical life, the important aspects will be explained, such as transferring records to third parties, transparency and the information obligation, retention period for recordings and the obligation to delete them, technical measures, and processing of special categories of personal data.

- Preparation of an opinion on the Commission's draft decision on suitable data protection in Japan

The European Commission asked the European Data Protection Board for an opinion on the forthcoming decision stating that Japan provides data protection at a level corresponding to the current EU standard. The Office volunteered to work on formulating this opinion, attending consultations with Commission representatives, representatives of the Japanese supervisory authority for personal data protection, and many personal meetings and teleconferences within the close working team. The task of drawing up such an opinion follows from Article 70 (1) s) of the General Regulation. In the case of Japan the task was all the more of a responsibility because it was the first such Commission decision under the General Regulation, setting the standards for application of Article 45 of the General Regulation, not only for the work of the Commission and for evaluating supervisory authorities, but also for the approach of third countries who have an interest in convergence with the European system of data protection.

- Assessing the Questions and Answers document on the relationship between the Clinical Trials Regulation (EU 536/2014) and the General Regulation

The European Commission asked the Board for an expert opinion and advice in the interest of a consistent approach to data protection in this area. In total the Office has a direct employee representative in six subgroups of the Board:

- the subgroup for cooperation among authorities
- the subgroup for technology
- the subgroup for key provisions
- the subgroup for borders, travel and law enforcement
- the subgroup for international transfers
- the subgroup for e-government

In 2019 the Office plans to send out delegates to another two subgroups with a focus on financing and on issues of practical law enforcement (supervisory and surveillance activity).

The force of the General Regulation has also been reflected in other areas of activity. For example, there was a rise in the number of cases with a cross-border element, which the Office generally deals with in the role of a supervisory authority concerned, but also from the position of lead supervisory authority.

The Office has begun accepting and recording notifications of data security breaches under Article 33 of the General Regulation. More detailed information is available in the chapter "Complaints, Notifications of Personal Data Breaches, and Consultations"

Office employees travelled to annually held conferences and seminars, for example to the spring conference of data protection commissioners (with Europe-wide participation) or at the international conference of privacy and data protection commissioners (with global participation). Attendance of other conferences and seminars was limited in favour of trips to meetings of the Board working groups.

• CODES OF CONDUCT

FIRST EXPERIENCES AND FINDINGS OF THE OFFICE

In 2018 the Office noted great interest on the part of controllers and processors in dealing with General Regulation compliance through codes of conduct. The growing interest from various sectors and the early sending of draft codes of conduct for assessment led the Office to issue a methodology for codes published on the Office website providing the general public with basic information and procedures for those drawing up codes.

In 2018 the Office received eight draft codes of conduct or provided consultation for their preparation or monitoring. One of the entities even decided to publish its "code of conduct" on its website. On the basis of a call from the given entity, another roughly 50 joined it, this despite the fact that it had not been approved by the Office and no designated entity has been accredited to monitor it, thus the basic requirements so that a code can serve to demonstrate compliance with the General Regulation had not been met. The Office alerted the given entity to the fact that such an approach is inconsistent with the General Regulation and called on it in a letter to rectify the situation.

The basic findings from meetings with those who submitted codes can be generalised as follows:

- the draft code is aimed at a small group of controllers (problematic monitoring or economic parameters of such activity) and sometimes ignores other controllers with a similar or identical character of personal data processing
- the draft code to a large extent copies the text of the General Regulation provisions, thus it has a negligible added value over the General Regulation, which does not meet the requirements of a code
- the producer of the code (and its controller) demands actions from controllers to which it does not have the right under the Regulation
- here is a lack of sufficient analysis and justification in the preparation and content of the code
- there is a lack of evidence of the necessary talks before starting to produce the code demonstrating that there is a broad consensus in the given sector on the drafting of the code, its content, and the entity that drafted it

TASKS OF THE OFFICE

The tasks of the Office associated with the agenda of codes of conduct comprise two basic levels:

- the Office carries out approval of codes of conduct - Article 40 of the Regulation
- the Office must provide for monitoring of codes (either on its own or through a third party that the Office accredits for this purpose) - Article 41 of the Regulation

Media Communication Tools

From a media perspective, the central point of communication in 2018 was the entry into force of the General Data Protection Regulation in May.[36] Aside from this, media attention focused on the legislative process concerning the relevant adapted legislation, i.e. the Act on Personal Data Processing.

To an ever increasing extent journalists inquired about topics associated with possible sanctions arising from the General Regulation, as well as on possible limitations on their own activities that they claimed could occur without the relevant adaptive legislation.

To a lesser extent, due to the topic of the General Regulation, International Data Privacy Day drew attention, with Office representatives providing several media appearances.

As in the previous year, in 2018 the Office joined in the celebrations of Safer Internet Day, with the clear aim of supporting a safer internet and more responsible online behaviour.

Over the course of the year the Office continued with its outreach activities with the aim of raising awareness and interest in data protection. Similarly, it focused on topics associated with the General Regulation taking effect. It also continued to produce and publish its own unofficial translations of materials from the WP29 group with the goal of presenting different parts of the Regulation to the public. Over the course of the year it produced new information material for the general public on the given topic. To a considerably greater extent it provided consultation activities either directly on-site at the Office, electronically, or over a specially created GDPR telephone line, which was available from Monday to Friday. The line is operated solely by qualified employees (lawyers).

[36] The General Personal Data Protection Regulation, also known as the GDPR (Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC).

As part of an information campaign, Office experts gave talks at nearly 90 events, conferences and seminars in 2018. In addition, it organised seven meetings with DPOs on its premises, the goal of which was to pass along to participants the latest in good practice.

Overall it can be stated that 2018 differed quite markedly from previous years. Aside from the General Regulation, the media community took an increased interest especially in cases like the leaked client data from the Mall.cz internet shopping mall, or the parking fines sent to the wrong addresses by Czech Post. The Office also had to react frequently to misleading or mistaken information that was constantly repeated in the media in connection with the General Regulation.

In 2018 the Office got fully involved in the preparations and running of the Czech Secondary School Competition on Cybersecurity, the goal of which was to test the knowledge and skills of students in terms of security in cyberspace. Nearly ninety schools signed up for the competition and three thousand students took part in it.

MEDIA IMAGE

In their articles and reports, journalists did not take any particular attitude towards the Office and generally limited themselves to stating that entities that violate the General Regulation can receive a new maximum possible fine.

Once again in 2018 the Office repeatedly stressed to the media that it is necessary to honour the principle that everyone can adequately execute their rights if their legally protected interests have been encroached upon. Journalists have already fully accepted this approach from the Office and regularly bring it up in their reports on individual cases made public.

LIBRARY

The Office Library holds 2500 volumes, which is a year-on-year increase of 100 volumes compared to 2017, of those six being donations. Despite the somewhat more difficult situation caused by the planned renovations, the library fulfilled its standard function consisting of two pillars – an area for employees and a source of reference literature for the public. According to the approved plan, the library was moved into a separate, more suitable space on the ground floor.

WEBSITE

The website continues to be the primary communication channel through which the Office can inform most effectively about its activities and news from the field of personal data protection. The dominant topic on the Office website in 2018 was, quite expectedly, the General Regulation. The Office altered the structure of the website quite significantly, adding several sections and overall increasing the clarity of its internet presentation so that visitors could get to the most important information as quickly as possible. It provided access to the GDPR section, which was located in the first spot on the navigation menu, in the form of individual sections in the right navigation column as well. In connection with this, a special microsite was also created on the General Regulation for the general public that wants to learn more about the General Regulation. A link to the GDPR line was also placed on the front page with the goal of promoting this new communication channel further.

ORG information system

The ORG system, which the Office runs and maintains, is part of the system of basic registers. Since July 2012, the system of basic registers has been collecting and storing basic information on natural persons. Basic public administration registers are one of the key pillars of the expanding Czech e-government, i.e. the process of digitising and streamlining public administration. Public authorities, citizens and other entities can currently already take the system of basic registers of the Czech Republic as part of the modern functioning of public administration.

Among other things, basic registers contain reference data on citizens, legal entities, natural persons conducting business and public authorities, thus simplifying communication between citizens and the authorities.

In 2014, Act No. 181/2014 Coll., on Cybersecurity was adopted, and the ORG information system, as a part of e-government, was labelled as a critical infrastructure information system. The controller of such an information system is obliged to fulfil the technical measures laid down in Decree No. 316/2014 Coll., on Security Measures, Cybersecurity Incidents, Reactive Measures, and on Cybersecurity Reporting Requirements.

The ORG information system is an absolutely essential technical security component of the basic registers. It can be said that the individual systems of the basic registers are separated from each other, but through the ORG information system they can be connected. It is utilised every day by the state administration. A breakdown or long downtime would mean a considerable limitation on the operation of many authorities and organisations. If ORG was not functioning, the individual registers would become mere lists with meaningless content. Further funding of the ORG information system stems from Government Resolution No. 411 of 31 May 2017.

Meeting the demands placed on a system of critical infrastructure requires constant upgrading and introduction of new security features, both in the connection between individual parts of the system and in constant monitoring of the system's operation. Protection of the workplace of Office employees who are supervising the running of the system must also be constantly upgraded.

Since 2012 the system has only been maintained in terms of hardware by replacing damaged parts (disks, power sources, etc.) with new ones. Today it is evident that the system is technically and morally obsolete and outdated. For this reason it is necessary to consider replacing it. Likewise the software also needs new security versions and databases installed.

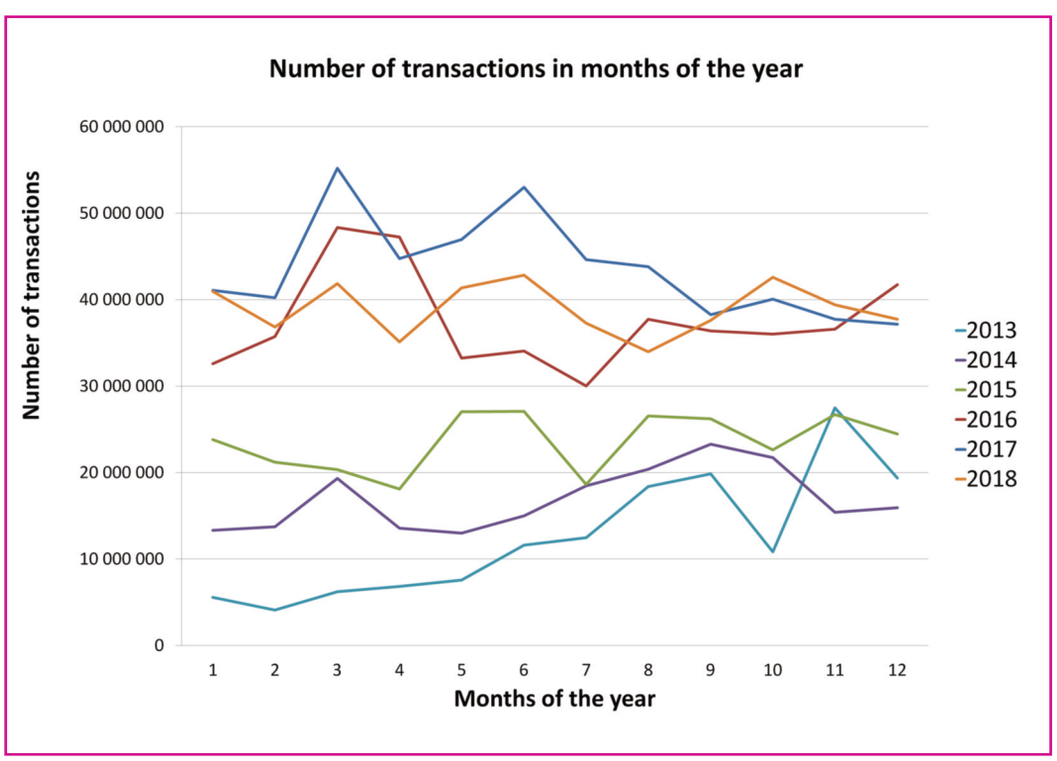
The creation of the system and its operation during the first five years was partially financed from fund provided by the EU under the assistance programme "Development of Information Society in Public Administration".

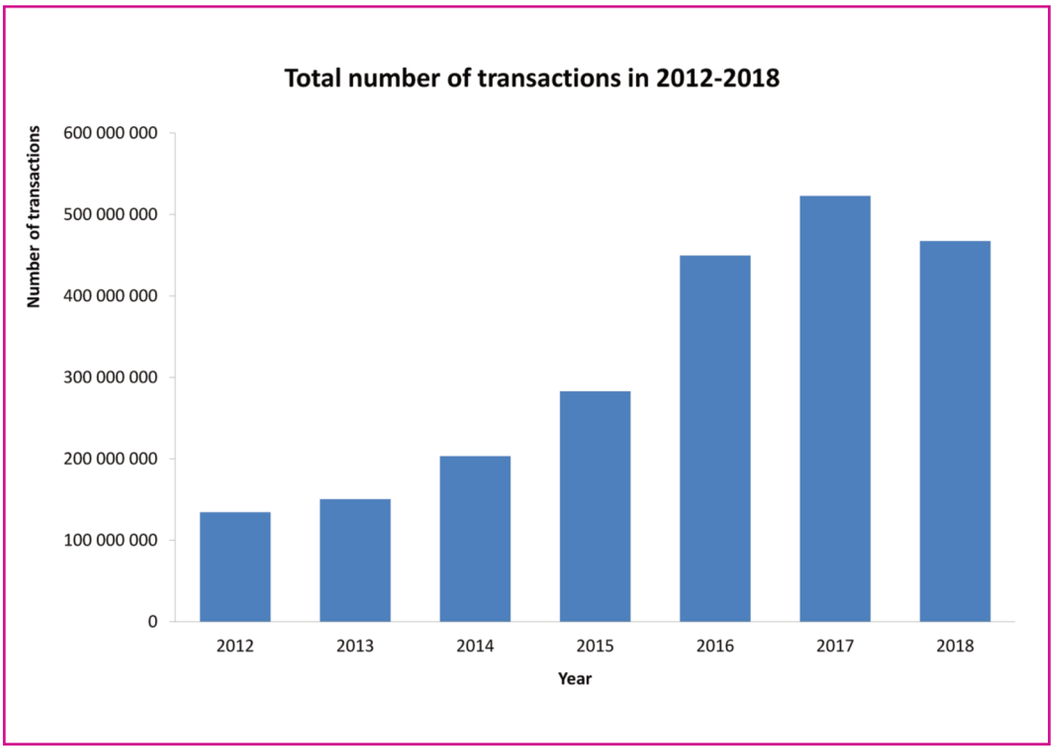
To ensure the necessary running and development in the near future, we foresee the following conditions being secured:

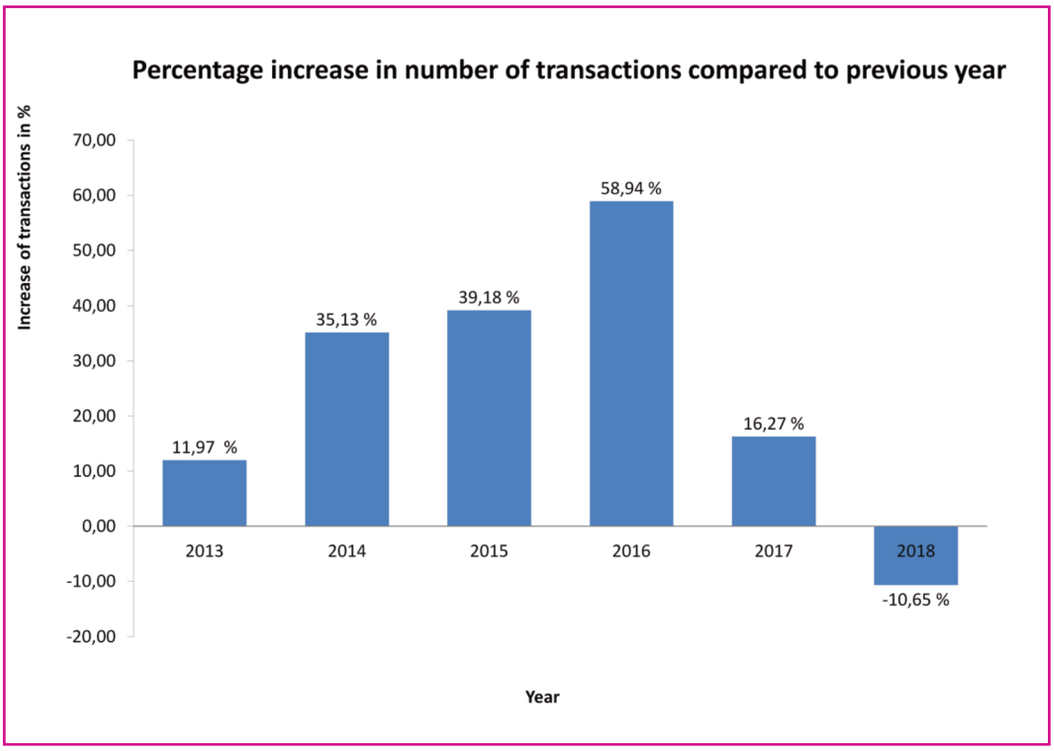
- continuing the transformation project dealing with renewing and expanding the basic registers of public administration and related systems
- operation of basic registers at the existing level of services provided (SLA)
- operating basic registers only on manufacturer-certified HW and SW
- annual 20% increase in basic register load through 2021

Another challenge will be ensuring cybersecurity, as in the original concept of the basic registers project no Cybersecurity Act was taken into account.

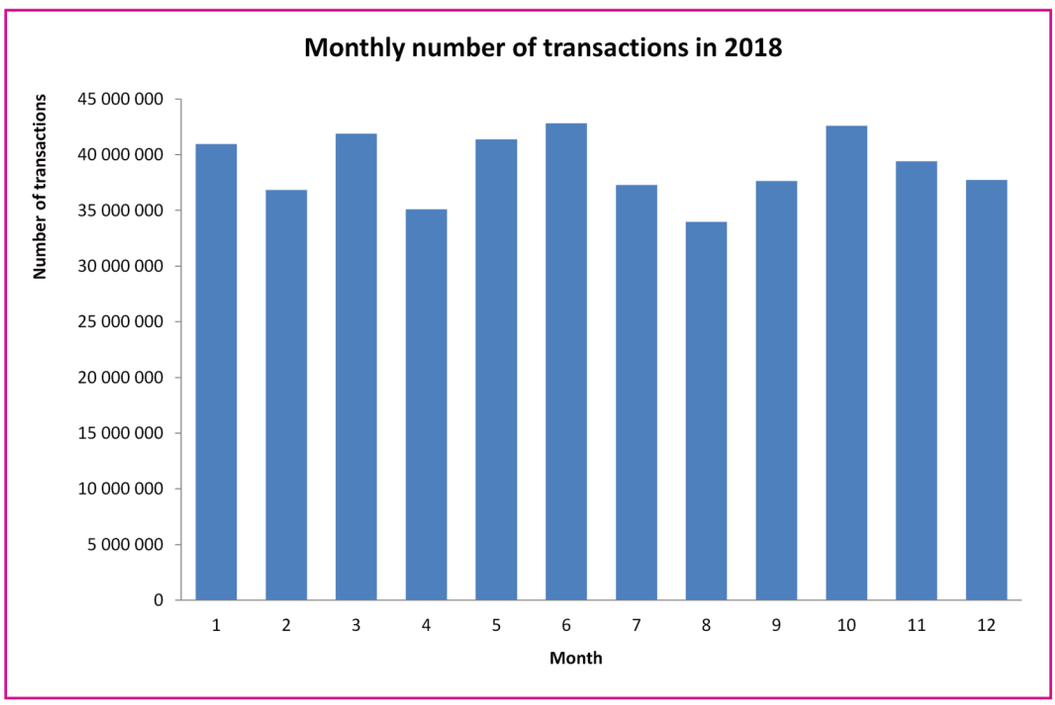
The graph "Number of transactions in the months of the year" shows the progression of numbers of transactions in the various years and months since 2013.



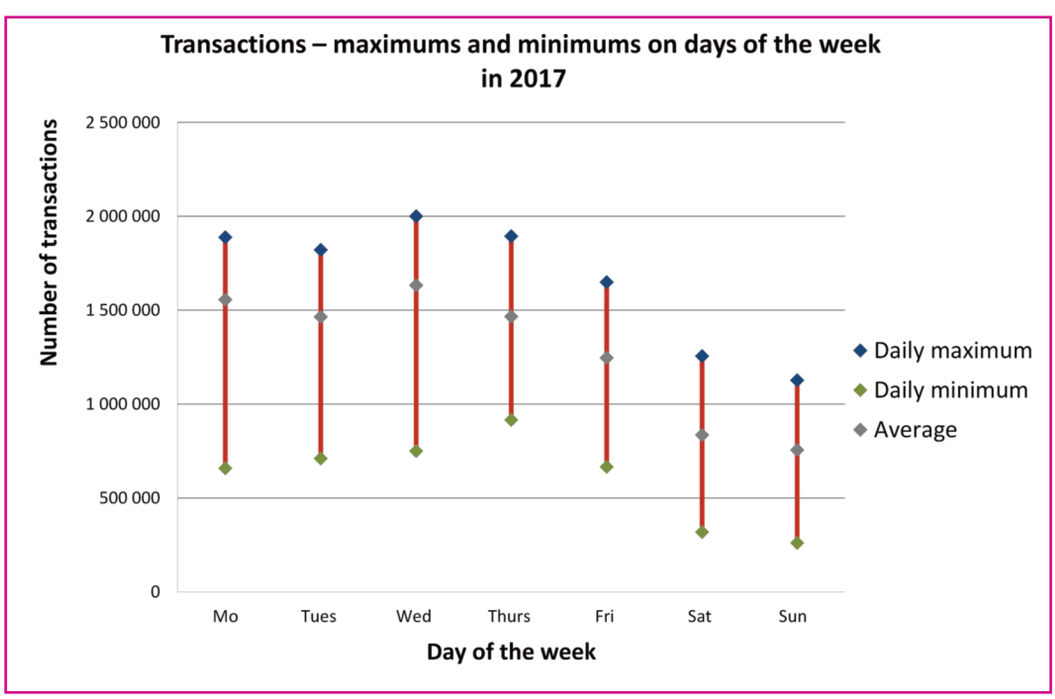

Total number of transactions in 2012-2018
Number of transactions
600 000 000
500 000 000
400 000 000
300 000 000
200 000 000
100 000 000
0
2012
2013
2014
2015
2016
2017
2018
Year


Percentage increase in number of transactions compared to previous year
Increase of transactions in %
70,00
60,00
50,00
40,00
30,00
20,00
10,00
0,00
-10,00
-20,00
11,97 %
35,13 %
39,18 %
58,94 %
16,27 %
-10,65 %
2013
2014
2015
2016
2017
2018
Year

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 2018". The maximum load was 2 July 2018 with a number of transactions of 2 000 795, which is 1 572 817 less than in 2017. The minimum load was recorded 5 June 2018 with a number of 260 631.



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. The highest load was recorded on Wednesdays.



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 2018 the total number of systemised positions was 109.

Staff fluctuation in 2018 fell compared year-on-year from 16.6% to 9%.

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 2018 a service evaluation of civil servants assigned to serve at the Office was conducted. Based on these evaluations, 29 civil servants were evaluated as excellent and 26 as good. No civil servant was evaluated as inadequate.

Ten staff members were brought in to serve, while 6 ended their service. Four new staff members were employed, with three employees terminating their employment.

A total of 25 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 21 completed it successfully and 4 were evaluated as unsuccessful. The increase in the number of tested applicants compared to previous years was the result of establishing the position of data protection officer at various resorts of the state administration and the necessity of re-testing them in accordance with the Civil Service Act.

As of 1 January 2018, the records showed 97 employees at the Office; as of 31 December 2018 this number was 101.

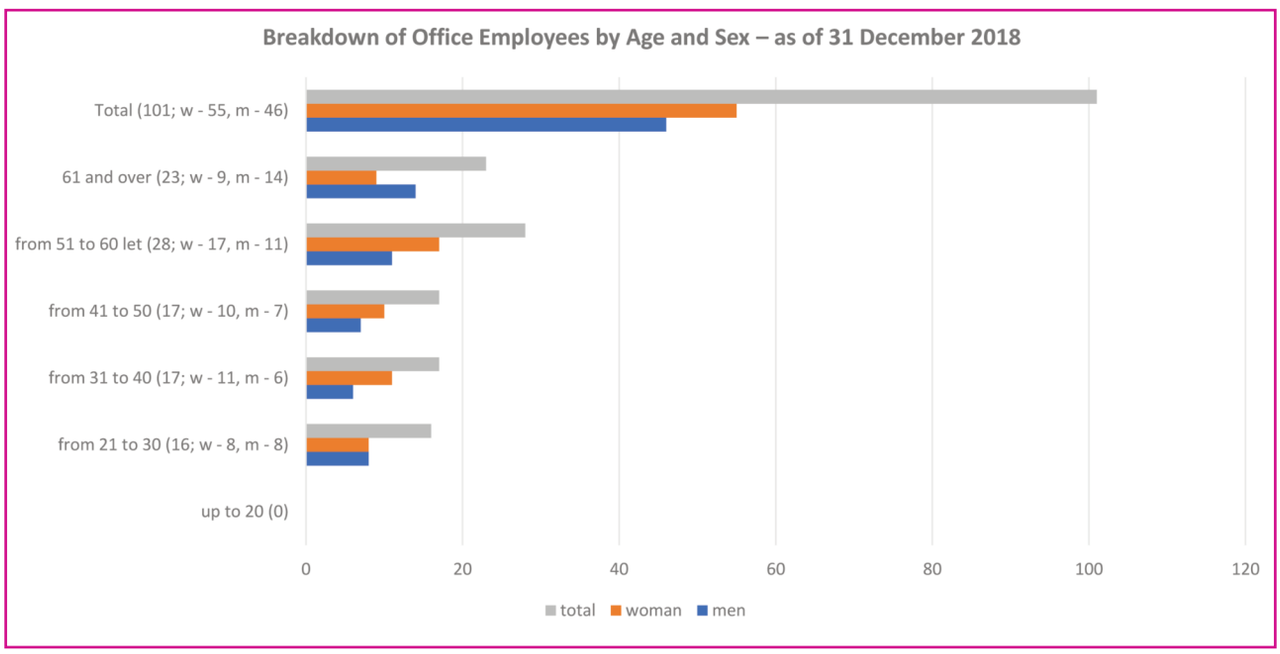
The average registered number of employees for 2018 was 99.10.

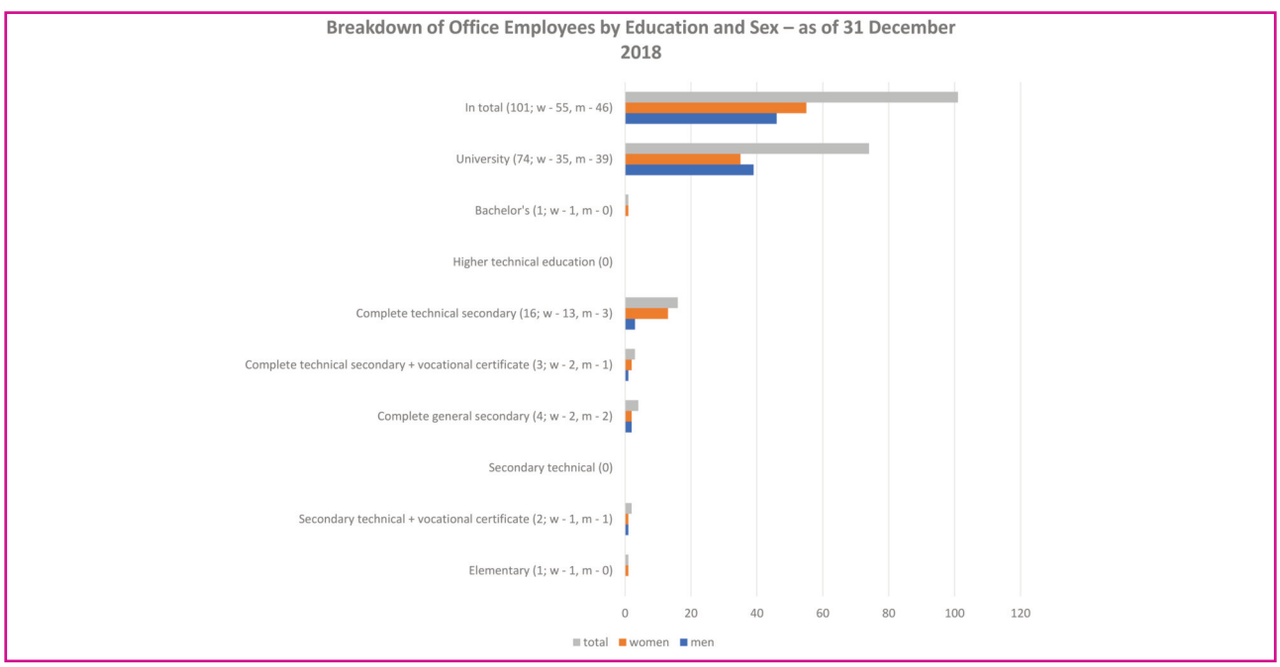
A further 37 persons performed activities at the Office on the basis of concluded agreements on work performed outside employment.

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 practice and much experience. Many of them have been employed at the Office for a long time and 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 attend courses in English, German and French. Employees can then apply those language skills in carrying out their work or service, with the language abilities of employees become ever more important with the new European concept of data and privacy protection. 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.





Economic Management

The Office budget was approved by Act No. 474/2017 Coll., on the State Budget of the Czech Republic for 2018.

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

	in CZK thousands
Summary indicators	
Total income	3 056.89
Total expenditures	158 534.20
Specific indicators – income	
Total non-tax, capital income and accepted transfers	3 056.89
of which: total income from EU budget not including CAP	0.00
other non-tax and capital income and accepted transfers total	3 056.89
Specific indicators – expenditures	
Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	158 534.20
Cross-sectional expenditure indicators	
Employee salaries and other payments for work performed	65 650.92
Mandatory insurance premiums paid by the employer *)	22 101.10
Contribution to the Cultural and Social Needs Fund	1 271.71
Salaries of employees in an employment relationship except those in service positions	12 553.16
Salaries of employees in service positions under the Act on Civil Service	40 084.79
Salaries of employees derived from the salaries of constitutional officials	11 007.49
Total expenditures co-financed from the EU budget	0.00
not including CAP 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	9 940.09

*) 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 2018.
The income budget for Heading 343 – Office for Personal Data Protection was fulfilled with an amount of CZK 3 056 890.
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 2017 (payment of remainder of deposit account for paying salaries and contributions to the Cultural and Social Needs Fund for December 2017)

2. Expenditures

Expenditure drawing of CZK 158 534 200 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 in the basic registers system
- 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 Office.

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

Drawing of the budget for employee salaries, other expenses for work performed and associated expenses, including the Cultural and Social Needs Fund, and compensation for sick leave, in the amount of CZK **89 169 690** corresponds to the qualification structure and meeting of the employee plan.
As of 31 December 2018 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 043V10 "Development and Renewal of Material and Technical Base for Office for Personal Data Protection from 2017" a total of CZK **9 940 090** was drawn.

Overview of budget drawing in 2018

Budget structure type	Name of indicator	Approved 2018 budget in CZK thousands	Final 2018 budget in CZK thousand	Reality as per accounting statemens as of 31 December 2018 in CZK thousands	Actual final budget in%
2211, 2212, 2324, 3113, 4132	Other non-tax income	0.00	0.00	3 056.89	
	Total income	**0.00**	**0.00**	**3 056.89**	
501	Salaries	62 944.81	64 764.73	63 645.44	98.27
5011	Salaries of employees in employment relation-ship with exception of employees in servise	12 041.28	12 711.53	12 553.16	98.75
5013	Salaries of employees in servise positions under the Act on Civil Service	39 834.73	40 284.79	40 084.79	99.50
5014	Salaries of empl. derived from salaries of const. officials	11 068.80	11 768.41	11 007.49	93.53
502	Other payments for work performed	1 890.91	2 005.48	2 005.48	100.00
5021	Other personnel expenses	1 890.91	2 005.48	2 005.48	100.00
5024	Severance	0,00	0,00	0,00	0,00
503	Mand. insurance paid by employer	22 044.15	23 559.00	22 101.10	93.81
5031	Mand. social security premiums	16 208.93	17 343.74	16 206.63	93.44
5032	Mand. public health insurance	5 835.22	6 215.26	5 894.47	94.84
512	Expenditures for certain alterations totangible items and procurement of certain rights to tangible items	0.00	80.00	3.29	4.11
513	Purchase of material	1 522.00	4 324.12	4 150.76	95.99

514	Interest and other fin. expenses	50.00	30.00	28.35	94.51
515	Water, fuel and energy	2 025.00	1 646.12	1 482.61	90.07
516	Purchase of services	12 068.63	54 272.75	47 918.16	88.29
517	Other purchase	38 885.86	5 250.84	2 816.82	53.65
518	Provided deposits, principal, quarantees and government loans	485.00	485.00	0.00	0.00
519	Exp. assoc. w/non-invest, purchases, contributions allowances and in-kind donations	3 164.70	3 408.65	3 015.32	88.46
534	Transfers to own funds and in relation to bodies without full legal personality	1 266.80	1 271.71	1 271.71	100.00
5342	Transfers to Cultural and Soc. Needs Fund and soc. funds of municipalities and region	1 266.80	1 271.71	1 271.71	100.00
536	Other non-inv. transf. oth. budg. tax payments and other mandatory payments	22.00	22.00	9.10	41.36
542	Compensation paid. to pop.	200.00	200.00	145.97	72.99
5424	Compensation during illness	200.00	200.00	145.97	72.99
	Total current expenditures	**146 569.86**	**161 320.40**	**148 594.10**	**92.11**
611	Acquisition of fixed intangible assets	7 600.00	7 931.77	3 600.28	45.39
612	Acquisition of fixed tangible assets	11 300.00	19 420.18	6 339.81	32.65
	Total capital expenditures	**18 900.00**	**27 351.95**	**9 940.09**	**36.34**
	TOTAL EXPENDITURES	165 469.86	188 672.36	158 534.20	84.03

Numerical data used from reports drawn up as of 31 December 2018.

INTERNAL AUDIT

The basic legal and regulatory standards governing the internal audit activities in 2018 were:

- Act No. 320/2001 Coll., on Financial Control in Public Administration and the Amendment to Certain Acts (Financial Control Act)
- Decree No. 416/2004 Coll., implementing Act No. 320/2001 Coll.
- *International Professional Practices Framework for Internal Auditing*
- the internal directives of the Office, which are regularly updated

The Internal Audit Department is organisationally separated from the management and executive structures, functionally independent and reports directly to the Office President.

The internal audit plan for 2018 was approved by the Office President 1 March 2018. The main basis for its drafting was a comprehensive risk analysis of the Office, including risks identified in performing internal audits. The annual plan also drew on the medium-term internal audit plan for the period 2019 to 2021, from the results of previous internal audits, from the requests of the Office management, from the obligations arising under the Act on Financial Control (the internal audit should check at least once a year e.g. the effectiveness of the internal control system on the basis of the provisions of Section 30 (7) of Act No. 320/2001 Coll.) and the capacity of the Internal Audit Department.

On the basis of the approved annual plan for 2018 the Internal Audit Department conducted a total of four audits. In compiling the programmes of the individual audits and selecting the investigated sample of operations for testing, it focused primarily on the setting of management and control mechanisms and the state of implementation of measures adopted for shortcomings found in the internal audits carried out and the possible risks in the audited areas and their potential impact.

The internal audits were focused on checking the following:

- watchkeeping
- the functionality and effectiveness of the internal control system
- fleet operations
- purchase of information system services and information technology

The results of the audits completed in 2018 were discussed with the managers of the audited departments, entities and the Office President. Their findings brought added value to the effective functioning of financial management and complying with the generally binding legal and internal regulations. They also showed the settings and functionality of selected audited systems.

In terms of the internal audits conducted, there is no indication that the Office financial statement did not provide a true and fair portrayal of the accounts.

For all the shortcomings identified in carrying out the audits, targeted, specific and deadlined measures were adopted. Implementation of the adopted measures is regularly monitored and evaluated by the Internal Audit Department.

During the internal audits, no serious findings within the meaning of Section 22 (6) of the Act on Financial Control were identified. Not possibilities for the emergence of corruption or fraud were recorded.

In 2018 the Internal Audit Department also:

1. provided consultation activities primarily in the following areas:
- risk management
- internal regulations
- property records
- implementing measures

2. organised:
- internal auditor training

Based on the results of the audit investigations, assurance can be provided that in the audited period in the selected sub-sections of internal operational and financial management, the established management and control mechanisms are adequate and effective with the exception of shortcomings of medium and low importance. These identified shortcomings were not however of such a nature as to impact in a fundamental manner the execution of financial management and functioning of the internal control system. They are however a support for increasing the quality of the oversight environment, updating and upholding internal regulations, employee training and protection of the legitimate rights and interest of the Office.

FINANCIAL STATEMENT

Approval of the final financial statement for 2018 and information on its transfer will take place by the standard deadline of 31 July 2019 in accordance with Annex 4 to Decree No. 383/2009 Coll., on account records in technical form of selected accounting units and their transfer to the central system of state accounting information and on the demands for technical and mixed forms of accounting records (Technical Decree on Accounting Records). In accordance with the communication of the Ministry of Finance on the application of several provisions of Act No. 221/2015 Coll. amending Act No. 563/1991 Coll., on Accounting, and in connection with Act No. 101/2000 Coll., the Office is not obliged to have its financial statement approved by an auditor.

Provision of information pursuant to the Act on Free Access to Information

In 2018 a total of 56 requests for information were addressed to the Office concerning its jurisdiction, which was 26 more than in the previous year. The reason for this was the overall media attention on personal data protection in connection with the General Regulation.

Full information was provided in 45 cases. In two cases the Office refused to provide information and in seven cases the information requests were partially rejected. The reason for this was primarily protection of personal data of persons who were contained in the requested documents, or the fact that the request targeted information to which Section 11 of Act No. 106/1999 Coll., on Free Access to Information, limits access. In two cases the petitioners did not pay the required fee for exceptionally extensive retrieval of information.

In their requests for information the petitioners focused primarily on the decision-making and control activities of the Office, i.e. on the results of administrative proceedings (administrative decisions) and the results of inspections (inspection reports). Also a subject of interest with regard for the force of the General Regulation was information concerning the number of submissions and complaints received in certain periods, the number of administration sanctions imposed, or information on data protection officers.

The provided information was published in a manner allowing remote access.

Annual Report of the Office for Personal Data Protection for the year 2018
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 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 2019.

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, 2019
ISBN 978-80-210-9224-2