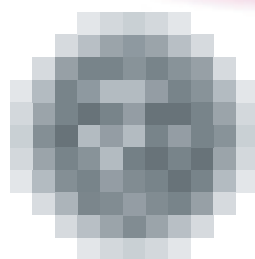


Annual Report 2019



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

Foreword by the President



Ladies and gentlemen,

The Annual Report you have opened contains topics that the Office for Personal Data Protection has addressed in performing its duties. They are defined by legislation, but they also reflect – albeit indirectly – all the issues that are currently in the limelight.

The year 2019 was thus the second year in which the issue of personal data protection received increased attention of the public as a result of the General Regulation coming into effect, as well as in relation to incorrect use of personal data of others in the context of misinformation, attempts at manipulation and also cyber attacks.

Owing to the positive tradition of personal data protection in the Czech Republic and the fact that the rights embodied in the Constitution can be enforced relatively effectively, the Office was able to handle the complaints of individuals who felt that their right to personal data protection was prejudiced. Consequently, our Office – unlike equivalent authorities in some other EU Member States – faced only an increase in the volume of its work, rather than having to accommodate new services and processes.

Supervisory activities in personal data protection in the narrower sense lie in the heart of the Office's work. They were significantly affected by waiting for the transposition laws and the related need to cope with the consequences of the lengthy adoption of national laws that were substantially amended during the legislative process. The figures and conclusions from the individual cases of review of administrative punishments must be interpreted in the light of these circumstances.

They were indeed affected by the several months of uncertainty and reduced pressure on public bodies as regards observance of rules in the handling of personal data. Similarly, there was a number of applicable regulations that had not been adequately updated. As a result, supervisory activities were performed also in areas which still lack accurate rules for personal data processing, in spite of the fact that they must be in place under the General Regulation. For example, the Office advised the Ministry of Labour and Social Affairs of the increasing trend of processing employee biometric data. The use of biometric technology by private controllers and municipal police is also problematic.

In consultancy and advice, we have a clear preference for wider-reaching professional events and individual consultations for data subjects and controllers.

Our engagement in the preparation of new legal regulations also has a far-reaching impact. Under the General Regulation, the duty to assess the effects of new processing on the rights and freedoms of natural persons before the processing commences may be assessed precisely at the time when the regulation that imposes the duty to process personal data is being prepared. The Office strongly urges that the assessment be properly performed in the inter-departmental commentary procedure. This is the only way of ensuring that the risks involved in processing need not be assessed by anyone who processes personal data under the law, or that the assessment may be limited to risks following from the integration of such processing into a more comprehensive information system. Inconspicuous as it may seem, this arrangement is a great help.

The Office performed its tasks under the Act on Basic Registries in the same manner and with the same high degree of reliability as ever before. The operation of the critical information system that provides basic identifiers and agenda identifiers of natural persons represents a second pillar of our work. This activity is rather hidden from view and the public feels the effects of the system's smooth operation indirectly, through government administration.

Preparation for the Office's new competence (initiated by the Chamber of Deputies of Parliament) was an absolute novelty in our work; it began to be exercised before the end of 2019 as the third pillar. In the area of right to information, since January 2020 the Office has been reviewing the decisions of the appellate body. It is also the superior authority for some obliged entities and also deals with cases of inactivity under the Act on Free Access to Information.

I would like to note that this report is the last report I submit within my (current) mandate. I am convinced that from this perspective, it confirms the trends I have followed throughout my term, i.e. active approach and non-ostentatious professionalism. I hope these trends are visible from the outside, for example, as we engage in cooperation within the European Data Protection Board, where the Office contributes to the Board's work, amongst other things, by shared reporting in several expert groups communicating exclusively in English; each of the ten experts performing these tasks simultaneously carries out his/her basic agenda in the Office.

However, they are particularly apparent from the decision-making practice of the Office. Out of my 120 second-instance decisions, 23 were challenged by an action. My decision was upheld in all the 11 cases in which court rulings have been rendered to date.

JUDr. Ivana Janů

President of the Office for Personal Data Protection

Table of Contents

THE OFFICE IN NUMBERS 2019	8
SUPERVISORY ACTIVITIES	11
COMPLAINTS AND SUBMISSIONS	11
DATA BREACH NOTIFICATIONS	16
INSPECTION ACTIVITIES	17
INSPECTION PLAN	19
FINDINGS FROM INSPECTION ACTIVITIES	20
Personal data processing within the provision of information from medical records (Bohnice Psychiatric Hospital)	20
Personal data processing in the context of newborn laboratory screening	22
Personal data processing in relation to the provision of electronic services by public authorities in the provision of services through ePortál operated by the Czech Social Security Administration	24
Personal data processing by TOPlist s.r.o. in the use of cookies to measure website traffic	27
Opening of a personal current account by a bank without the client's knowledge and request (UniCredit Bank, a.s.)	29
Personal data processing (performed directly by the inspected entity or on its behalf) targeting membership base, persons on the waiting list for membership, persons interested in membership, supporters and other persons (potential voters) approached by SPD – Tomio Okamura	30
Inspection of personal data processing carried out by a political party with emphasis on the membership base and on persons outside the party (i.e. members, persons on the waiting list for membership, persons interested in membership, supporters and other persons approached – potential voters)	32
Inspection of compliance with the duties stipulated by the General Regulation in processing of genetic data as special categories of personal data	33
Processing of personal data of holders of industrial property rights – natural persons listed in registers of industrial property rights (IPTR, s.r.o.)	35
Personal data processing through the hlidacvyboru.cz web portal (Open Data Company s.r.o.)	36
Processing of personal data attesting to health condition within the provision of accommodation services (MERKURIA UNION, s.r.o.)	37
Processing of personal data of persons transported in means of transport (Dopravní podnik hl. m. Prahy, akciová společnost)	39
Inspection of the processing of cookies by Velká Pecka s.r.o.	41
Inspection of an electricity supplier (ČEZ Prodej, a.s.)	42

SUPERVISION IN THE AREA OF COMMERCIAL COMMUNICATIONS	44
ADMINISTRATIVE PUNISHMENT	49
HANDLING OF COMPLAINTS PURSUANT TO SECTION 175 OF THE CODE OF ADMINISTRATIVE PROCEDURE	53
FINDINGS FROM JUDICIAL REVIEWS	54
ADVISORY AND CONSULTANCY ACTIVITIES	59
LEGISLATION	62
ANALYTICAL ACTIVITIES	66
INTERNATIONAL COOPERATION	72
CODES OF CONDUCT	72
PERSONAL DATA PROTECTION CERTIFICATION	72
DATA PROTECTION IMPACT ASSESSMENT (DPIA)	73
TRANSFER OF PERSONAL DATA ABROAD	74
SCHENGEN COOPERATION	76
INTERNATIONAL ACTIVITIES	78
FREE ACCESS TO INFORMATION	80
PREPARATION FOR PERFORMANCE OF NEW COMPETENCE OF THE OFFICE PURSUANT TO ACT NO. 106/1999 COLL., ON FREE ACCESS TO INFORMATION	80
PROVISION OF INFORMATION PURSUANT TO THE ACT ON FREE ACCES TO INFORMATION	82
ORG INFORMATION SYSTEM IN THE SYSTEM OF BASIC REGISTERS	84
MEDIA AND COMMUNICATION TOOLS	87
OPERATION OF THE OFFICE	90
PERSONNEL	90
ECONOMIC MANAGEMENT	92

The Office in numbers 2019

Inquiries and consultations	total inquiries	1836
	GDPR telephone consultancy line	2667
	prior consultation within the meaning of Article 36 of the GDPR	0
Submissions and complaints	submissions received	2482
	resolved by notifying the controller of possible	560
	passed on for inspection or other proceedings	145
	notification of a personal data breach pursuant to Article 33 of the GDPR	416
	provision of collaboration to prosecuting bodies	31
	resolved in some other manner	1677
Inspection activities (other than inspections relating to commercial communications)	initiated	63
	closed	75
	of which outstanding from previous years	32
	remedial actions imposed	19
	contested by objections	12
	objections upheld	1
	rejected	10
	partially upheld	1
	finances for failure to cooperate with inspection	4
Commercial communications (competence)	total submissions	2007
	inspections initiated	5
	inspections closed	17

pursuant to Act No. 480/2004 Coll.)	<ul style="list-style-type: none"> of which outstanding from previous years contested by objections objections upheld rejected partially upheld proceedings on penalty finances for failure to cooperate with inspection handled without initiating inspection by notifying the entity concerned of possible breach of duties 	<ul style="list-style-type: none"> 13 4 0 4 0 28 11 390
Administrative punishment other than proceedings concerning unsolicited commercial communications)	<ul style="list-style-type: none"> penalty proceedings held with legal entities and natural persons operating a business penalty proceedings with natural persons waiver of fine pursuant to Section 40a of Act No. 101/2000 Coll., or Section 65 of Act No. 110/2019 Coll. reprimand administrative punishment waived owing to the impossibility of punishing public authorities and public bodies 	<ul style="list-style-type: none"> 24 8 25 4 7
Decisions of the President of the Office	<ul style="list-style-type: none"> decisions contested by an appeal rejected appeals overturned and returned for further proceedings decision overturned and proceedings change of decision 	<ul style="list-style-type: none"> 15 14 6 1 4
Judicial review (Note: * total since 2001)	<ul style="list-style-type: none"> court actions lodged actions rejected by court actions overturned by court court proceedings closed/pending since 2001 	<ul style="list-style-type: none"> 10 6 1 141/24
Authorisations for transfer of personal data abroad	<ul style="list-style-type: none"> requests for transfer of personal data abroad received decisions authorising transfers decisions dismissing transfers proceedings discontinued on procedural grounds 	<ul style="list-style-type: none"> 1 1 0 0
Complaints under Section 175 of the Code of Administrative Procedure	<ul style="list-style-type: none"> complaints received resolved as justified handled as partially justified resolved as groundless pending 	<ul style="list-style-type: none"> 30 4 0 19 7

Requests under the Act on Free Access to Information	requests received	90
	fully accepted	63
	partially rejected	24
	fully rejected	3
	requests for reimbursement of costs of exceptional	6
	of which costs already reimbursed	3
Comments on drafts	draft laws	3
	laws	80
	implementing regulations	43
	draft Government regulations	16
	draft decrees	27
	non-legislative documents	41

Supervisory activities

• COMPLAINTS AND SUBMISSIONS

By analysing the 2,482 complaints and submissions received in 2019 that contested the procedure of personal data controllers, it can be concluded in terms of the private/public sector ratio that submissions and complaints against personal data processing in private-law relationships predominated. This can be attributed to the higher number of controllers in this sector, as well as the mandatory appointment of data protection officers in all public authorities and public bodies where data protection officers have cultivated the process of personal data processing during the less than two years since their introduction.

In the public sector, the Office addressed, for example, complaints against publication of applicants' address details when disclosing information provided pursuant to Act No. 106/1999 Coll., on free access to information, where especially municipalities failed to anonymise the applicant's details in the disclosed document, or anonymised them inadequately.

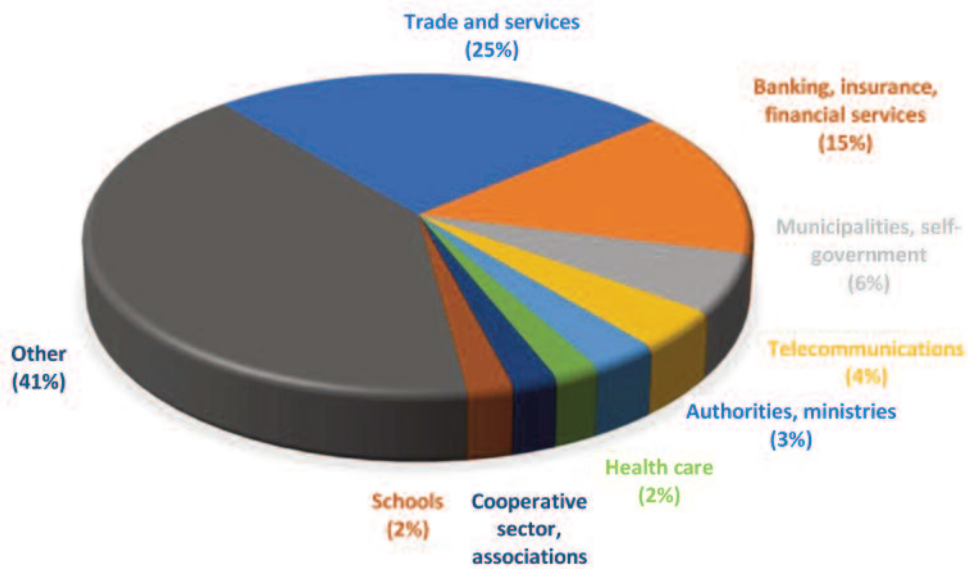
In numerous cases the complaints concerned publication of recordings (or minutes) of municipal assembly or city council meetings on the internet. This occurred at variance with the duty to anonymise personal data of citizens or third parties contained in the recording based on their acting on a private basis (i.e. those who did not act in connection with a matter of public interest).

In the public-law sphere, the Office also dealt with complaints against inspection of basic registries by officials without a legal ground.

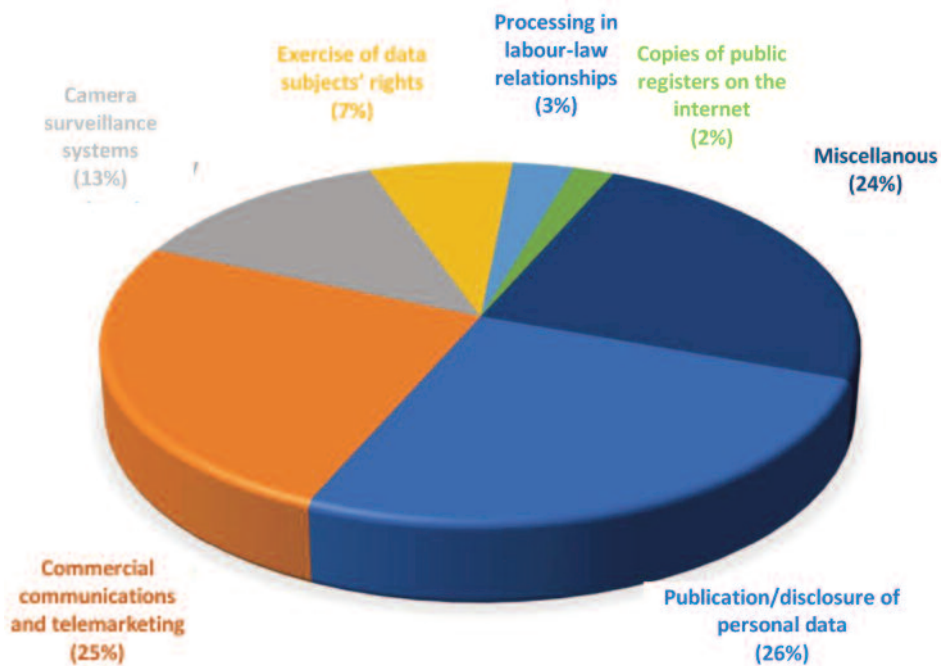
In the private sector, complaints concerning personal data processing for marketing purposes comprised a major portion of the agenda. These include complaints concerning sending of commercial communications in printed form by post¹ without the person affected by the processing (data subject) being aware

¹ For the supervisory activities of the Office in relation to dissemination of commercial communications by electronic

SUBMISSIONS/COMPLAINTS BY THE CONTROLLER'S FIELD OF ACTIVITY (SECTOR)



MOST FREQUENT COMPLAINTS



of the source from which the controller obtained his/her personal data. This also includes complaints concerning the manner in which consent to personal data processing for marketing purposes was obtained, where in some cases it was virtually impossible to obtain the service in question without giving such consent.

Petitioners often approached the Office even after exercising a right granted to them by the General Regulation vis-à-vis the companies concerned (e.g. they withdrew their consent, exercised their right to erasure, objected to processing or inquired about the origin of their personal data in the controller's database); nevertheless, the controller continued processing their data for marketing purposes and continued approaching them with commercial communications, either using electronic means or by post.

A substantial part of complaints concerning data processing for marketing purposes was related to telemarketing calls, which the affected persons perceived as the most harassing. It was obvious from the contents of these complaints that the petitioners were often unaware of the identity of the entity (controller) on whose behalf they had been called, as well as the source from which the controller obtained their contact details and, where applicable, also other personal data. Subsequently, in February 2019, the Office for Personal Data Protection published guidance on its website on how to defend oneself against unsolicited marketing calls that are made without any previous contact between the called party and the calling party. This material, titled How to defend against unsolicited telemarketing, provides information, *inter alia*, on how persons targeted by unsolicited telemarketing calls can exercise their rights.

Also, during the period of time that has elapsed since the rights of data subjects were strengthened by the General Regulation, many controllers have failed to respect data subjects' rights. As a rule, the controller failed to provide the data subject, at the latter's request, with adequate information on the data processing, or failed to respond to the data subject's request, without informing the data subject about the reasons why the controller did not grant his/her request.

Some controllers continued to hinder data subjects' access to their data by placing excessive requirements for verification of the data subject's identity despite the fact that the latter had been sufficiently established in the course of previous communication. In these situations, the controller's doubts regarding the applicant's identity were unfounded. The Office further addressed significant cases of failure to respect data subjects' rights within the exercise of the supervisory powers delegated to the Office.

As in previous years, in 2019 the Office dealt with cases where the controller, after being requested by the data subject to provide a copy of the personal data processed, refused to provide a copy of the recording of the call (or its transcript) that had allegedly given rise to a contract with the data subject, amended an existing contract or documented performance of an existing contract, as appropriate. The Office concluded that the complaints against failure to provide a copy of the recording (or transcript) of the call were substantiated as the recording/transcript is a key to determining whether a contract to which the data subject is a party was indeed established or amended, as well as to establishing whether and, if so, on what grounds the controller was entitled to carry out the relevant processing.

The complaints processed in 2019 included complaints about the practice of making the provision of a service conditional on making a copy of an identity document (personal identity card, passport). These were situations in which the controller had no duty to require this under a

legal regulation. In the assessment of these complaints, the Office evaluated whether the a copy of the identity document in the given case and, where the legal ground was based on consent, whether the consent had been given freely, and last but not least, whether the controller had complied with the principle of data minimisation. Indeed, as a rule, the identification of a person consists in recording the necessary identification details from the presented proof of identity rather than making and keeping a copy thereof.

The Office took a similar approach, i.e. based especially on the existence of a legal ground for processing and the data minimisation principle, in relation to complaints against the processing of the birth identification number by public-law and private-law entities such as associations.

Petitioners also often approached the Office with submissions concerning non-performance or inadequate performance of the controller's duty to provide information on personal data processing (e.g. by including this information in the controller's terms and conditions) or pointed out that the controller confuses the duty to provide information with obtaining consent, as a result of which they considered such processing non-transparent.

The Office also encountered complaints indicating that personal data were processed with a fraudulent intention. This included, for example, enforcement of payments after registration on a web portal (e.g. auctions) or e-shop, where the registering person was unaware that the controller regarded the "registration" as an act establishing a contract (e.g. arrangement of an advertising service). Subsequently, the data subject was charged for the unsolicited service or penalised for non-observance of the "terms and conditions". The Office referred these submissions and complaints to the Czech Police as there were grounds to suspect that such entities were guilty of the criminal offence of fraud or extortion.

Processing with a fraudulent intention was also suspected in cases where the controller collected and published personal identification data of natural persons operating a business from a public register without the entrepreneur being aware that s/he was advertised (in an advertising catalogue). The data subject was then contacted by the controller by telephone and unknowingly manipulated (e.g. by request to "update the data") into concluding a distance contract (by telephone). S/he was subsequently requested to pay a price for the service and then a contractual penalty if the service was not paid.

In 2019, the Office also often addressed complaints concerning fraudulent conduct of persons acting on behalf of energy dealers. These persons either already had the personal data of the persons they contacted using telemarketing calls and did not inform them about the actual source of the data, or even obtained the data subjects' personal data in a manner that was obviously fraudulent. Most of them (in case of door-to-door sales) presented themselves as employees of the subjects' current energy supplier and asked for documents and contracts.

The Office even noted cases where persons acting on behalf of energy dealers committed identity theft by falsifying the signature on the contract or even by falsifying the subsequent verification telephone call.

Last year, the Office was again approached by natural persons affected by processing of their personal data through their publication on the internet, either for journalistic purposes or within posts and discussions on social networks and websites.

When assessing these complaints, the Office first evaluated whether the General Regulation was applicable to the publication in question. As part of this evaluation, the Office assessed whether the data were published exclusively within personal activities (e.g. in a personal

profile on a social network, during a discussion, social network blog or on a hobby website) and whether processing occurred, i.e. whether the publication was systematic by nature (whether it was an output from records or data entered in records).

In cases of *ad hoc* publication of information on a natural person, which is not covered by the substantive scope of the General Regulation, and in cases of processing of data that did not constitute processing in the sense of the General Regulation, the Office informed the petitioner about the possibility to have recourse, in civil proceedings, to the provisions of Act No. 89/2012 Coll., the Civil Code, that provide for the protection of personal rights. In such a case, the petitioner was also advised that in addition to civil liability of the person who disseminates information about him/her on the internet, there may also be liability on the part of internet service providers (e.g. search engines) pursuant to Act No. 480/2004 Coll., on certain services of the information society, also with reference to the recommendations published on the Office's website on the steps to be taken in these cases.

In cases where personal data were published for journalistic purposes, the Office assessed the case after the Act on Personal Data Processing came into effect, taking into account also those of its provisions that regulate an exemption from the right to erasure in relation to data processing for journalistic purposes. Further procedure of the Office in handling these complaints was based on assessment of the relationship between the right to information and the right to privacy, especially whether the relevant purpose of processing continued, but also taking account of the controller's status. In this context, the controller's subject of activity was examined in terms of whether the controller was the holder of a journalistic licence or was the publisher of periodic press.

In 2019, the Office also received and dealt with complaints against the procedure of private entities operating copies of public registers on the internet which, after the affected person exercised his/her right, did not satisfy his/her objection against processing or request for erasure of personal data. As a rule, such cases were subsequently forwarded by the Complaints and Consultations Unit for further supervisory measures.

In 2019, the Office did not notice any decrease in the number of complaints concerning the use of surveillance cameras, whether within neighbourly (civil) disputes or by private-law and public-law entities to protect property. This is true despite the Office's long-lasting awareness-raising efforts on its website.

In case of complaints against personal data processing by employers, the Office received, along with complaints concerning monitoring of employees (which are to be assessed by the State Labour Inspectorate), also complaints from (former) employees against failure to provide access to the personal data being processed.

Same as in previous years, where the controller's violation was minor or the controller's violation could be easily and promptly remedied, the Office continued its good practice of advising controllers about the possible breach of the personal data protection rules without the need to resort to other administrative procedures. This approach of the Office is based on application of the principle of subsidiarity of repressive administrative action, which prevents punishment, as well as on continued education of controllers in relation to the General Regulation.

When assessing trivial shortcomings, which occur especially on the part of small controllers, the Office did not initiate proceedings *ex officio*; instead it opted for a procedure where the

controller concerned was reminded of its duties and called to remedy the erroneous processing. In most cases, this procedure proved to be a good practice as it led the controller concerned to change the unsatisfactory personal data processing practice.

In the past year, the Office applied this approach in more than five hundred cases, thus ensuring a prompt and efficient remedy. However, some controllers did not respond to the informative letter, or did not respond adequately. In such cases, it was necessary to address the matter by initiating an inspection or using some other administrative procedure.

• DATA BREACH NOTIFICATIONS

In 2019, the Office received a total of 416 data breach notifications. The notifications differed in terms of the nature of the notified risk of a security incident affecting data subjects as well as in compliance with the formal requirements laid down by the General Regulation in its Art. 33 (3) concerning notifications to the supervisory authority.

It was specifically in order to make it as easy as possible for controllers to notify data security incidents that a form for notifying personal data breaches was published on the Office's website in 2019. Although non-mandatory, the form was soon picked up by controllers from a wide range of personal data processing activities.

The personal data breaches reported to the Office occurred both in the private and public sectors. Same as in the previous year, both sectors saw a number of notifications concerning cybernetic incidents affecting personal data processed. This most often involved an attack by malicious software (ransomware), which encrypted data in information systems; it then demanded a ransom to unblock the data. The Office received dozens of notifications concerning such security incidents during the year.

With a view to mitigating the risk of loss of data availability, the Office often emphasised in its response to the controllers that it is necessary to regularly back up data in order to reduce the impact of such illegal conduct.

Given that phishing attacks² were responsible for infected systems in an overwhelming majority of cases, consistent education of employees has also become a necessity.

The notifications received were also concerned with occasional negligence of employees consisting e.g. in erroneous sending of personal data to other than the intended addressees, sending e-mail communications to addressees in "non-blind carbon copies", and loss of devices containing personal data.

In the area of personal data processing in printed form, loss (of documents, consignments, etc.) was the most frequently notified incident, as well as their theft by a former or even existing employee, usually in an attempt to harm the employer.

In handling these notifications, the Office took into account, amongst other things, the objective of the notification duty laid down in the General Regulation, which is primarily not

² Phishing is a form of computer crime aimed at obtaining unauthorised access credentials to an information system, e.g. from employees.

to impose pecuniary penalties or to initiate inspection. Depending on the gravity of the notifications received, the Office set aside some notifications without further measures, communicated with controllers and provided them with recommendations and, in some cases, also explanation why the notification in question did not pose a risk to the data subjects.

Some cases were further handled within the Office's supervisory activities. The latter was applied, for example, in the case of a request from Czech Television and Czech Radio for a list of electricity consumers. The controller – an energy company – had failed to ensure that the data base that was subsequently transmitted to the above two entities do not contain personal data of approx. 40 thousand customers purchasing only gas and not electricity. For natural persons, the personal data concerned included name, surname, date of birth, permanent address and address of the delivery point; for natural persons operating a business, name, surname, business name where applicable, company identification number, address of the registered office and address of the delivery point. Some of these persons were subsequently requested to pay the television and radio licence fee. The Office found violation of Art. 32 (1) of the General Regulation, i.e. the controller's duty to implement appropriate technical and organisational measures, and imposed a fine of CZK 40,000 on the controller.

The Office presented general findings from notifications of personal data breaches on its website and also on suitable occasions, such as seminars for data protection officers.

• INSPECTION ACTIVITIES

Inspections initiated by the Office in 2019 were already carried out pursuant to the General Data Protection Regulation, based on findings from the complaints received and following the inspection plan for 2019.

In connection with the adoption of Act No. 110/2019 Coll., on personal data processing, and its coming into effect on 24 April 2019, which introduced an amended regulation of the Office and its organisation, the Supervision Department was reorganised with effect from 1 July 2019. Its structure now meets the requirements laid down in the Act on Personal Data Processing and makes it possible to perform inspections in the most efficient manner possible. In this arrangement, inspection teams are formed at specialised units to complement existing inspectors. Pursuant to the transitory Section 66 (3) of the Act on Personal Data Processing, existing inspectors will thus be able to complete their term of office.

As of 1 July 2019, the four existing inspectorates were replaced by two units, each of them focusing exclusively on inspection and related supervisory activities in the private³/public⁴ sector. Another unit provides cooperation to inspectors in the inspections conducted by them and carries out its own independent inspection activities. This will allow for a better diversification and planning of inspection activities, also as regards the necessary professional knowledge in each sector.

³ Private Sector Inspection Unit.

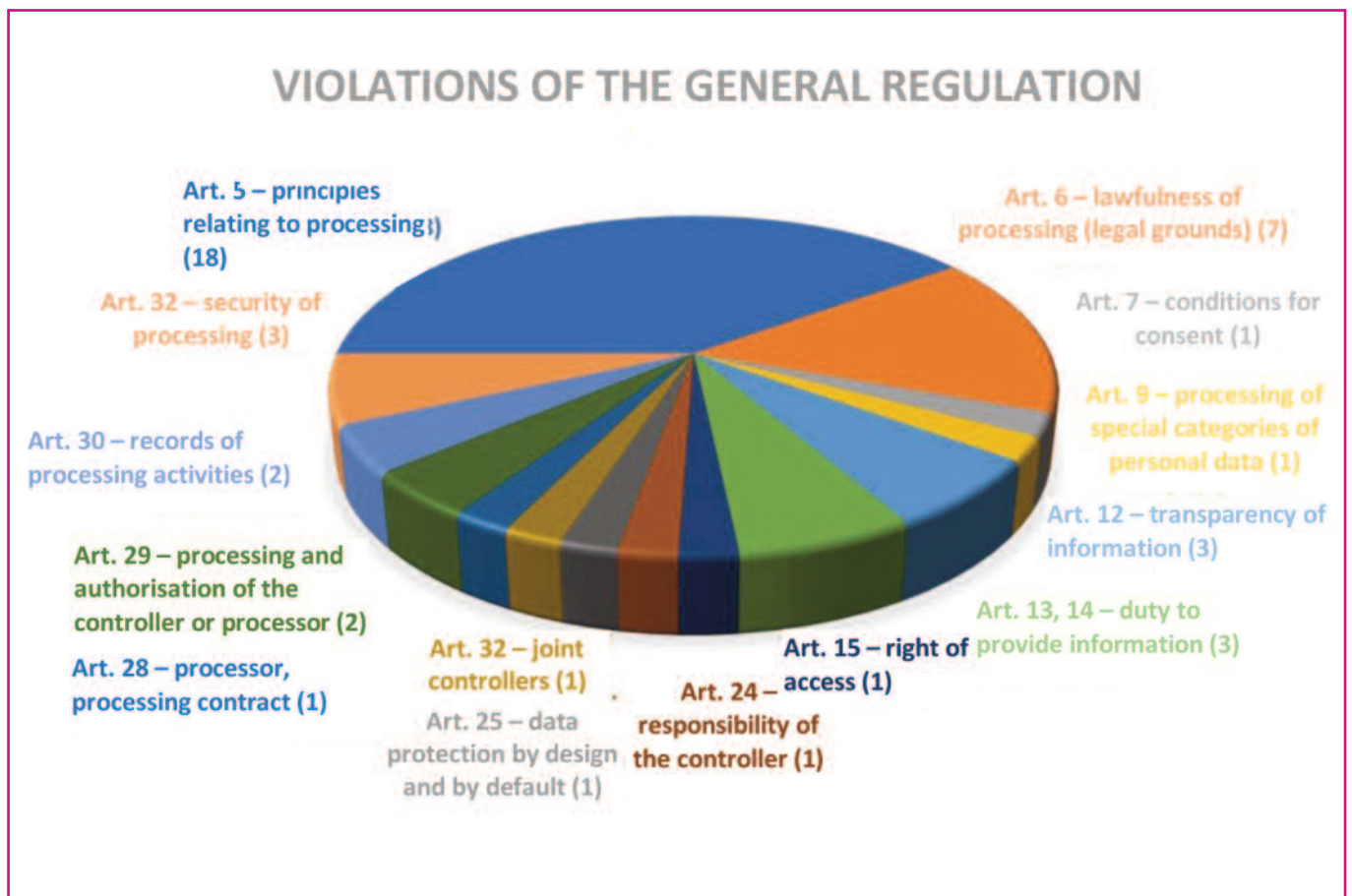
⁴ Public Sector Inspection Unit.

Inspection activities in 2019 were concerned with a wide range of duties following from the General Regulation and Act No. 110/2019 Coll., on personal data processing. A closure look at violations of the General Regulation found during the inspections is provided on the following page.

Most often, the inspectors found non-observance of the basic principles of processing and absence of legal grounds for personal data processing. Further violations ascertained by the inspectors concerned the data subjects' rights. This often involved a breach of transparency of information within the meaning of Article 12 or provision of information under Article 13 GDPR. In certain cases, breaches concerning personal data security were also found.

The coming into effect of the General Regulation also had its implications in 2019 in the mutual European cooperation of supervisory authorities in the area of personal data protection.

In four inspection cases, the Office acted as the lead supervisory authority in 2019. This entailed necessity of the procedure pursuant to the applicable provisions of the General Regulation concerning cooperation between supervisory authorities; to this end, the Office used the European Commission's system for exchange of information on the internal market (IMI). In one inspection case, the inspection was carried out on the basis of a submission forwarded to the Office by the British supervisory authority – the Information Commissioner's Office. The inspection was concerned with the exercise of data subjects' rights. Based on the inspection, the Office found that the inspected entity had breached the duty set out in Art. 15 (1)(c) of the GDPR.

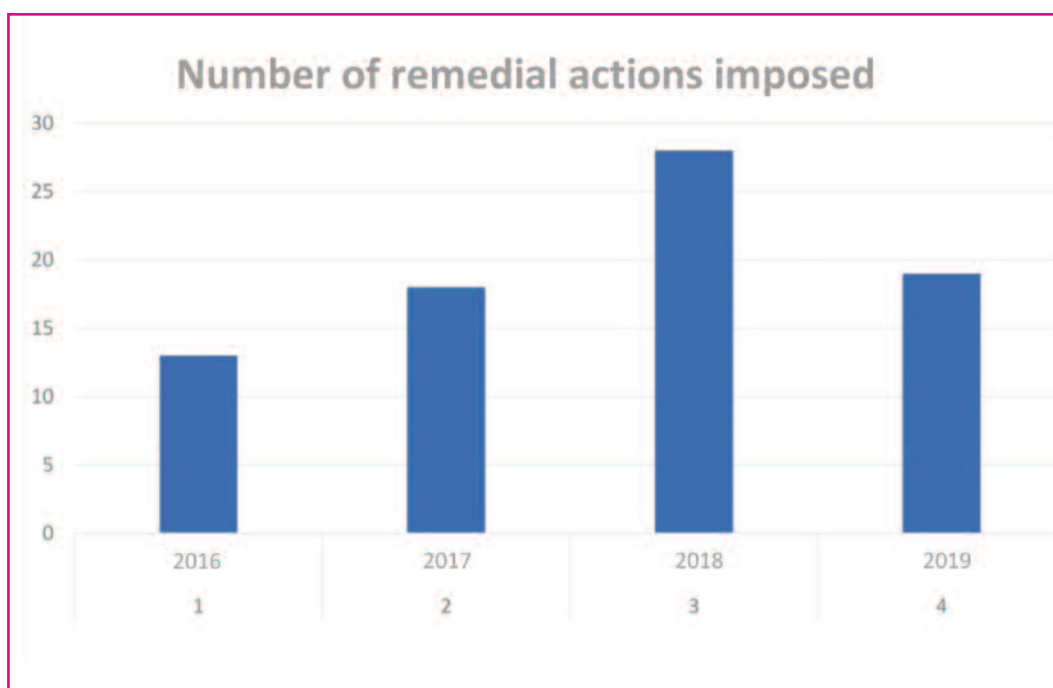


Also, the Office, in the role of the lead supervisory authority, inspected a company providing antivirus software, focusing on the processing of personal data of the software's users. The complaint pointed out the impossibility to deactivate the default privacy protection settings in a free version of the antivirus software.

Detailed information on these two inspections was published on the Office's website in 2019.

Another inspection in which the Office acted as the lead supervisory authority concerned the processing of personal data taken from public registers or published in some other manner. Due to its comprehensiveness, the inspection will be completed in 2020.

The Office again encountered non-cooperating entities in its inspection activities in 2019; in 11 cases, the Office had to impose a fine for failure to provide cooperation pursuant to Act No. 255/2012 Coll., on inspection (the Inspection Rules).



● INSPECTION PLAN

The Office's inspection plan for 2019 was set up on the basis of findings made in the handling of complaints and on the basis of the Office's aspiration to inspect selected comprehensive areas of activities involving the use of certain modern technologies and means used by all people to a greater or lesser extent.

For this reason, inspections targeting the use of cookies in the private sector were included in the inspection plan, in three different companies. The objective was to determine how these files were used in practice in relation to users and to evaluate their use in view of the applicable legislation.

Within the inspection plan, the Office also focused on inspecting a phenomenon that emerged in the recent years – processing of biometric data, i.e. data carrying the physiological characteristics of a natural person or characteristics of the person's behaviour enabling its

unique identification. Therefore, the Office included in the inspection plan two casinos that use fingerprints to identify players in the operation of games of chance.

Based on the inspection plan, the Office also carried out inspections in a bank entity and in a non-bank entity, focusing on the processing of personal data with respect to applicants for concluding a credit agreement online, with emphasis on the exercise of data subjects' rights.

Another comprehensive area dealt with by the Office in 2019 based on the inspection plan was health care. In this sector, the Office focused on inspection of newborn laboratory screening, i.e. active screening for diseases of children born in the territory of the Czech Republic. Its purpose is to ensure nationwide diagnostics and treatment of diseases before they can develop and cause irreversible damage to children' health.

Within the health care sector, the Office also included in the 2019 inspection plan inspections in two companies engaged in testing of genetic data (DNA). The inspection was included in the inspection plan on the basis of findings from a meeting of the European Data Protection Board with a view to evaluating the findings made also on a Europe-wide scale.

The Office also included in the inspection plan the current issue of elections to the European Parliament. For this reason, it scheduled inspections of two political parties with a view to inspecting personal data processing covering the parties' members and, if appropriate, processing reaching beyond the parties' membership base.

The inspection of personal data processing in the public sector was further represented in the inspection plan by an inspection of the Czech Social Security Administration concerned with comprehensive inspection of personal data processing through ePortál. Within the inspection plan, the Office also focused on the General Financial Directorate, carrying out a comprehensive inspection of the Tax Portal. Selected inspections are described in more detail in the chapter Findings from Inspection Activities.

Same as in previous years, some of the inspections included in the inspection plan were not completed in 2019, although all were opened as scheduled. The Office will provide information about the results of these inspections in the usual manner via its website.

● FINDINGS FROM INSPECTION ACTIVITIES

Inspector Jana Rybínová

Personal data processing within the provision of information from medical records (Bohnice Psychiatric Hospital)

The inspection of the Bohnice Psychiatric Hospital (hereinafter also the "inspected entity") was initiated on the basis of a submission forwarded to the Office by the Czech Police concerning suspected unauthorised disclosure of personal data of the aggrieved party, Z. F., to J. K., a convicted criminal. The data had been disclosed through the submission of a copy of a document titled Letter for prisons and for medical facility (hereinafter also the "letter"), sent to the inspected entity by the District Court.

In terms of personal data protection, the inspected entity was suspected of breaching security of personal data of the aggrieved party, Z. F. In the pre-trial procedure preceding the judgement of the District Court in conjunction with the resolution of the Municipal Court

in Prague by which the convicted person, J.J., was found guilty of stalking pursuant to Section 354 (1) (b) of the Criminal Code and was ordered, *inter alia*, to undergo protective in-patient psychiatric treatment, the aggrieved party had requested, pursuant to Section 158 (6) of Act No. 141/1961 Coll., on criminal court proceedings (the Code of Criminal Procedure), that her personal details consisting in her birth date, birth identification number, residence and postal address be maintained confidential within the meaning of Section 55 (1)(c) of the Code of Criminal Procedure and that she be advised of the release of the convict, J. K., from prison.

The inspected entity was advised of the aggrieved party's request through the Letter for prisons and for medical facility. However, a copy of the aforementioned letter including personal data of the aggrieved party was made available to the convict, J. K., by an employee of the inspected entity.

The inspection was concerned with fulfilment of the duties stipulated by the General Regulation in relation to personal data processing within the provision of information from medical records, namely their administrative part. In this respect, internal regulations concerning technical and organisational security of personal data and procedures of health care workers were also inspected, especially their compliance with the duties of a personal data controller within the meaning of Articles 30 and 32 of the General Regulation.

The case, within the scope of submission of the aggrieved party's request and provision of the associated favourable court resolution to the inspected entity, is subject to Act No. 40/2009 Coll., the Criminal Code, and Act No. 45/2013 Coll., on victims of crime, i.e. regulations applying Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose 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 2008/97/JHA.

It was ascertained that the inspected entity was processing data that constituted personal data of the data subject, Z. F., within the meaning of Art. 4 (1) of the General Regulation. Fulfilling the statutory duty laid down by Act No. 141/1961 Coll. and Act No. 45/2013 Coll., the inspected entity determined the purpose and means of personal data processing. As such it is a personal data controller pursuant to Art. 4 (7) of the General Regulation and is responsible for the processing concerned. Within the meaning of Art. 4 (3) of the GDPR, the inspected entity collected the personal data of the aggrieved party, Z. F., kept them in the form of medical records, processed them as part of the medical records within the meaning of Art. 4 (2) of the General Regulation and, last but not least, made them available to the patient, J. K., within the meaning of Art. 4 (9) of the General Regulation.

The Office further found that by failing to implement adequate technical and organisational measures within the meaning of Art. 24 (1) of the General Regulation and by making available, through its employee, the personal data of Z. F. to the convict as part of consulting medical records, the inspected entity violated the principle of personal data processing stipulated in Art. 5 (1)(f) of the GDPR.

Through its employee, the inspected entity illegitimately made available to the convicted person, J. K., the letter containing personal data of the aggrieved person, Z. F. The inspectors found that the inspected entity had failed to sufficiently assess the risks related to the filing of the letter containing personal data of Z. F. in the medical records of J. K. to which the latter has

access within the meaning of Section 65 of Act No. 372/2011 Coll., on health care services and the conditions for their provision (the Act on Health Care Services). In view of the information contained in the letter, the letter should not have been included in the medical records. The aforementioned violation cannot be remedied by the arguments presented by the inspected entity that it was proceeding in accordance with Section 2(e) or Section 1 (1)(g) of Decree No. 98/2012 Coll., on medical records, because the data from Z. F. are not related to the course and result of the health care services provided.

By failing to adopt adequate technical and organisational measures to ensure protection of Z. F.'s personal data within the meaning of Art. 24 (1) of the General Regulation, which resulted in a systematic violation of the principle of personal data processing within the meaning of Art. 32 (1) and (4) of the General Regulation, the inspected entity failed to ensure a sufficient level of personal data security appropriate to the given risk. At the same time, it failed to provide for sufficient regulations and instructions for the procedure of its employees in processing personal data of aggrieved persons who requested information under Section 55 (1)(c) and Section 103a of Act No. 141/1961 Coll., concerning the date when the patient's protective treatment was to end. Thus, the inspected entity violated the principle of personal data processing as expressed in Art. 5 (1)(f) of the General Regulation.

The inspected entity raised objections against the findings contained in the inspection record, which the President of the Office rejected by her decision. Subsequently, an Order was issued in the case and delivered to the inspected entity, whereby the inspected entity was ordered to adopt appropriate technical and organisational measures. The inspected entity complied with this obligation.

The inspected entity paid the imposed fine in the amount of CZK 10,000.

Personal data processing in the context of newborn laboratory screening

The inspection was carried out on the basis of the Office's inspection plan in four hospitals – Mělník Hospital, Brno University Hospital, Královské Vinohrady University Hospital and Havlíčkův Brod Hospital (hereinafter also the "inspected persons"), following inspections carried out by the Office in 2015. At that time, it was found that the inspected entities were storing "dry blood spot" specimens from newborns, i.e. blood samples taken for newborn laboratory screening, for a disproportionately long time that is not appropriate to the purpose of the processing.

Newborn laboratory screening (hereinafter also the "NLS") falls under preventive care within the meaning of Section 5 (2)(a) of Act No. 372/2011 Coll., i.e. it is *"carried out with a view to early identification of factors that are causally linked to the occurrence of a disease or deterioration of health, and implementation of measures aimed at eliminating or minimising the effect of these factors and preventing their occurrence"*; the objective is to ensure rapid diagnostics and early treatment of newborns with rare diseases in accordance with Resolutions of the Government of the Czech Republic No. 466/2010 (National Strategy for Rare Diseases) and No. 76/2015 (National Action Plan for Rare Diseases). The screening focuses on endocrine-related disorders (2), hereditary metabolic disorders (15) and cystic fibrosis. Newborn laboratory screening is based on analysing blood collected from newborns.

The inspection of all the inspected entities focused on compliance with the duties laid down by the General Regulation in relation to the processing of personal data in the context of newborn laboratory screening (including blood samples), the period of storage of samples taken and

their disposal and the fulfilment of other duties laid down by the General Regulation concerning the rights of data subjects, in particular Articles 5, 6, 9 and 12 to 23 of the General Regulation.

V The inspections covered all procedures in processing (handling) of the samples taken, i.e. taking of the blood drop, its keeping and securing by the inspected entities that collect the sample, as well as transition, security and disposal in laboratories of the inspected persons that analyse the blood sample. At present, NLS is performed on the basis of Guidance for Newborn Laboratory Screening and its annex (Bulletin of the Ministry of Health – year 2016, issue 6, released on 31 May 2016).

V Personal data of newborns, their mothers and paediatricians, which constitute personal data within the meaning of Art. 4 (1) of the General Regulation, are collected within the newborn laboratory screening. The processing of personal data carried out within newborn laboratory screening (the personal data included in the screening cards – request slips) is thus lawful as it is carried out in accordance with Art. 6 (1)(a) of the General Regulation. The data subject (the legal representative of the newborn) has given his/her consent to the processing of his/her personal data for a specific purpose (including consent to storing of the dry blood spot), where within the meaning of Art. 4 (11) of the GDPR, the consent given by the data subject (legal representative) is a freely given, specific, informed and unambiguous indication of wishes of the data subject (the newborn's legal representative).

V The screening involves processing of specific data attributed to a natural person for the purpose of laboratory examination for medical purposes. This means that data concerning health within the meaning of Art. 4 (15) of the General Regulation are processed that constitute special categories of personal data within the meaning of Article 9 of the General Regulation. The processing of special categories of personal data is lawful and is based on a legal ground that follows from Art. 9 (2)(a) of the General Regulation because the data subject (the legal representative of the newborn) has given his/her explicit consent to the processing of the personal data concerned for one purpose, i.e. newborn laboratory screening, where the consent given by the data subject (the newborn's legal representative) is a freely given, specific, informed and unambiguous indication of wishes of the data subject (the newborn's legal representative) within the meaning of Art. 4 (11) of the General Regulation.

The inspection did not establish any breach of the duties on the part of the inspected entities imposed on them as personal data controllers under Art. 30 (1) of the General Regulation as they have in place precisely defined procedures for processing of personal data or special categories of personal data. Also, they maintain records of processing activities containing information pursuant to paragraphs 1 to 5 of Article 30 of the General Regulation.

Taking into account the specific nature, scope, context, procedures and purposes of the processing, including consideration of the risk in processing, the inspectors concluded that the technical and organisational measures adopted ensure an appropriate level of security within the meaning of Article 32 of the General Regulation and the processing is in accordance with the principle laid down in Art. 5 (1)(f) of the General Regulation.

Within the meaning of Art. 4 (7) of the GDPR, inspected entities that perform blood collection are controllers of personal data (special categories of personal data) of data subjects processed within the newborn laboratory screening from the time of blood collection to the time when screening cards are made available for transportation to the relevant laboratory, i.e.

they process personal data in accordance with the principle set out in Art. 5 (1)(e) of the General Regulation. Each screening card bears the name, surname, date of birth and other information enabling identification of the data subjects for a strictly defined period of time.

Within the meaning of Art. 4 (7) of the GDPR, inspected entities performing laboratory examinations are controllers of personal data (special categories of personal data) processed within the framework of newborn laboratory screening, starting from the time when they take over screening cards from the respective hospitals for the purpose of laboratory examination. They store the cards after the laboratory examination for a period of 5 years in accordance with paragraph 15 (b) of Annex 3, Retention Periods of Medical Records or Parts Thereof, to Decree No. 98/2012 Coll., on medical records. Inspected entities process personal data within the meaning of Art. 4 (2) of the General Regulation and the relevant processing is performed in conformity with Art. 5 (1)(e) of the General Regulation.

Inspector Božena Čajková

Personal data processing in relation to the provision of electronic services by public authorities in the provision of services through ePortál operated by the Czech Social Security Administration

The inspection was performed on the basis of the Office's inspection plan for 2019. It concentrated on fulfilment of the duties stipulated by the General Regulation in relation to personal data processing in the provision of services to citizens by public authorities via ePortál operated by the Czech Social Security Administration (hereinafter also the "inspected entity" or the "CSSA").

The Office focused on compliance with the principles applicable to the processing of personal data (of clients and employees) and fulfilment of duties by the inspected entity as a controller pursuant to Art. 4 (7) of the General Regulation. This included, in particular, observance of the principle of legitimacy and lawfulness of processing, data minimisation, accuracy and storage limitation. As for duties, these include the duty to provide information, duty to provide cooperation in the exercise of the data subject's right under Articles 15 to 23 of the GDPR (right of access to personal data), duty to enter into a data processing contract under Article 28 of the General Regulation, duty to maintain records of activities under Article 30 of the General Regulation, duty to adopt technical and organisational measures to ensure personal data security under Article 32 of the General Regulation, and implementation of measures in communicating and notifying security breaches pursuant to Articles 34 and 35 of the GDPR.

The inspected entity is a social security body whose competence is regulated by special legal regulations. In specified cases, within its authority, it provides online electronic services in the form of the ePortál application of the CSSA, enabling the client to obtain specific information and services by remote online access through the internet. Also, it provides secured consulting of selected data kept by the CSSA and enables and offers the use of interactive forms and useful online services enabling CSSA clients to communicate online with the CSSA as well as with the district social security administrations. ePortál has been introduced as internet self-care, an application facilitating clients' communication with the CSSA, exchange of information between the CSSA client and the CSSA, including personal data of ePortál clients.

In addition to the tasks imposed by Section 5 of Act No. 582/1991 Coll., on organisation and implementation of social security, the CSSA inspects the fulfilment of duties by social security bodies, assesses the medical condition and working capacity of citizens for the purposes of

social security, maintains records of employees unfit to work and, in specified cases, administers sickness insurance. According to EU coordination regulations, the inspected entity is a liaison body vis-à-vis foreign institutions for sickness and maternity pay, pensions and pecuniary benefits in case of occupational injuries and occupational diseases. Other legal regulations also entrust the inspected entity with authority and lay down requirements for State administration to be exercised by the inspected entity in the area of social security and sickness insurance (Act No. 155/1995 Coll., on pension insurance, Act No. 187/2006 Coll., on sickness insurance, Act No. 589/1992 Coll., on social security and contributions towards the State employment policy).

The inspected entity also performs the tasks of a service body pursuant to Act No. 234/2014 Coll., on civil service, an employer pursuant to Act No. 262/2006 Coll., the Labour Code, and an administrator of critical infrastructure of the State pursuant to Act No. 181/2014 Coll., on cyber security and amending related laws, and Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, requisites of pleadings in the area of cyber security and destruction of data.

The inspected entity, as the controller, processes the necessary personal data of CSSA clients and employees pursuant to the above special legal regulations. It also has several legitimate statutory authorisations for personal data processing. As an employer, it performs legal obligations for the performance of a contract in accordance with Art. 6 (1)(b) of the General Regulation. Specifically, the following purposes are concerned:

- handling of social security matters (i.e. premiums for social security and contribution towards the State employment policy, sickness insurance, pension insurance and matters concerning people with disabilities);
- handling of matters of medical assessment services (hereinafter the “assessment service”) for the insurance and non-insurance social security system and employment;
- data base management (management of the register of insured persons, insurance relationships, mandatory underlying documents for pension insurance and benefit files in pension insurance);
- provision of information and other services to authorised persons in social security and assessment services (including mutual communication and cooperation);
- provision of information outside social security and assessment services to authorised persons (including mutual communication and cooperation);
- human resources management;
- inspection activities;
- handling of security-related matters;
- handling of legal matters and projects;
- internal administration;
- bookkeeping (covering areas other than benefits as well as benefit payments);
- handling of matters relating to information and communication technologies;
- provision of information to authorised persons outside social security and assessment services to authorised persons (including mutual communication and cooperation).

The inspected entity processes personal data of ePortál clients for activities necessary to comply with the statutory duty stipulated by the above laws.

In view of the subject of the inspection, the inspectors also focused on fulfilment of the duty to provide information pursuant to Article 12, within the scope of Articles 13 and 14 of the General Regulation, on the web portal of the CSSA. The website of the CSSA contains several links for clients concerning personal data processing (GDPR

— information on personal data processing, leaflet titled Information on Personal Data Processing, Rules of Operation of the CSSA administration's ePortál for the portal's clients). The article titled "GDPR

— information on personal data processing" provides complete information on processing of clients' personal data. The inspected entity has adopted appropriate measures to provide clients with all information pursuant to Articles 13 and 14 of the General Regulation.

The inspectors also evaluated fulfilment of the duty laid down in Articles 15 to 23 of the General Regulation. According to the aforementioned provisions, the data subject has the right to access personal data, i.e. the right to request and obtain relevant information on the processing of his/her personal data, as well as the right to object. The data protection officer has substantive competence for handling requests to exercise the data subjects' rights.

The right to erasure of personal data is not applicable to the inspected entity if the processing is necessary for the performance of duties required by Czech laws or for the fulfilment of a task in the public interest or in the exercise of official authority. This is entrusted to the CSSA. A total of 13 data subjects turned to the inspected entity with a request for the exercise of rights under Articles 15 to 23 of the General Regulation in the period from January to August 2019.

The inspectors further checked compliance with the duty following for the inspected entity from Art. 30 (1) of the General Regulation. This is the duty to maintain a record of processing activities. The inspected entity presented a guideline with annexes titled List of Processing activities and Records of Controller's Processing Activities and Specification of Purposes of Processing. Records are also kept in electronic form. The procedures in maintaining records of activities are contained in the above guideline. The inspected entity prepares mapping questionnaires that activities.

In view of the subject of the inspection, the Office also evaluated whether and to what extent the inspected entity was fulfilling duties concerning personal data security in relation to the provision of ePortál online electronic services, which is a duty of the inspected entity under Articles 25 and 32 of the GDPR.

It was ascertained that the ePortál application is part of the Critical Information Infrastructure Information System, which is protected by personal data protection by design. It serves to introduce and implement appropriate technical and organisational measures with a view to protecting the rights of data subjects. Personal data protection by default is provided for on the basis of legal regulations governing cyber security.

Thus, personal data security is provided at the level of critical information infrastructure. Furthermore, the inspected entity has introduced and implements regimen measures and measures of physical security for ePortál.

All online communication of a user of the CSSA ePortál is secured by encryption; protective information and communication security measures are in place for the CSSA ePortál. Identity verification is the system's cornerstone; data integrity is ensured to protect data against misuse, loss, etc.

The inspection did not find any breach of duties.

Personal data processing by TOPlist s.r.o. in the use of cookies to measure website traffic

The inspection was initiated on the basis of the Office's inspection plan for 2019. It was included in the plan based on the Office's findings to date and also based on the "Recommendations on processing of cookies and similar means of monitoring as of 25 May 2018", a material published by the Office on 22 May 2018. The entity inspected was TOPlist s.r.o. (hereinafter also the "inspected entity").

The inspected entity provides the TOPlist service, which includes, as its integral part, processing of personal data of visitors to websites for individual users (website operators) based on their registration.

The purpose of the personal data processing is to measure website traffic. This purpose is determined by the individual users, where the TOPlist service represents a means chosen by them to achieve this goal. Therefore, in this case, the users are in the position of personal data controllers under Art. 4 (7) of the General Regulation.

The inspected entity carries out the aforementioned processing on the basis of a contract with the user and according to the user's instructions, i.e. based on data indicated in the registration form. In the registration form, the user defines the website where the measurement is to be performed and, at the same time, whether information on traffic should be included in the statistics at www.toplist.cz and, if this is the case, in what category. Furthermore, the user decides whether or not the traffic details will be available to the public.

The inspectors concluded that the inspected entity was in the position of personal data processor pursuant to Art. 4 (8) of the General Regulation as it processed personal data for the controller.

The service of measuring website traffic (hereinafter the "TOPlist service") enables the user of this service to monitor website traffic statistics and also to compare them with traffic on other websites registered at www.toplist.cz (e.g. website traffic of competitors in the given sector). This is a service provided free of charge on the basis of registration at www.toplist.cz. Furthermore, the user may also use an extended paid version of the service, TOPlist Profi.

The basic factor measured by the TOPlist service is the number of visits to a web page. Visit means that the web page is displayed in a browser (identified using the IP address and cookies). If the same website from the same device is visited within the span of 30 minutes, it is considered to be merely "displayed". On the other hand, if a visitor returns from the same device to a website after 30 minutes, a new visit is recorded.

Anonymous "ui" cookies are used by the TOPlist service to distinguish "visiting" from "displaying". The cookie contains a random number in the range from 1 to 65,000. It is stored in the browser of the visitor to the website being measured for the period of 30 days and on the server for 30 minutes from the last request. When a visitor goes to a measured page, the IP address of the device and a random cookie are stored for thirty minutes in the storage data base of the inspected entity. At this time it is evaluated whether the page is "visited" or "displayed". IP addresses are stored for a certain period of time and users of the TOPlist service have access to them.

In order to determine whether the inspected entity processes personal data of visitors to the websites of the TOPlist service users (website operators), it was necessary to assess whether the information collected could be assigned to an identified or identifiable natural person.

An identified person is an individual whose identity can be directly determined based on the collected information (i.e. a unique identifier such as birth identification number, or a unique combination of identifiers, such as name, surname, address, is available). An identifiable person is an individual who cannot be directly identified from the collected information itself, but whose identity can be determined on the basis of that information (using other available information and means). Unambiguous identification of a natural person is not restricted to the civil identity of the natural person concerned. In certain cases, especially in the internet environment, unambiguous individualisation of the user based on a certain element may suffice. In accordance with Recital 26 of the General Regulation, a natural person is identifiable when means such as singling out can be used. Thus, individualisation may be achieved by pairing data with individual identifiers, such as the IP address, MAC address or other device identifier of a device usually used by individuals.

It was also necessary to emphasise in this respect that it is explicitly stated in Art. 4 (1) of the GDPR that a natural person is identifiable, for example, by reference to an online identifier. While the IP address, as a network identifier, primarily constitutes the technical data of the device in question, it must usually be regarded as personal data. This applies especially where it is likely that the given device is the property of a specific natural person.

Based on Recital 26 of the General Regulation, account must be taken of all the means reasonably likely to be used by the controller or by another person, if a certain IP address in itself does not enable permanent identification of a device connected to the internet. IP address constitutes personal data for anyone who has a feasible and legal possibility to attribute it to specific individuals regardless of who attributes it, or who can reasonably assume that such a possibility can exist.

It is thus not decisive whether the individual is directly identifiable, i.e. whether the controller connects the data itself on the basis of the information that is available to it or that it can acquire, or indirectly identifiable, i.e. whether interaction of several entities is necessary for the identification of the individual. After all, the same conclusions were already reached by the Court of Justice of the European Union (hereinafter the "CJ EU") in connection to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Specifically, in judgment of 24 November 2011 in case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL*, and in judgment of 19 October 2016 in case C-582/14, *Breyer v Bundesrepublik Deutschland*.

On the basis of the above, the inspectors concluded that the inspected entity processed personal data within the meaning of Art. 4 (1) and Art. 4 (2) of the General Regulation.

During the inspection, the inspected entity modified the TOPlist service in such a way that all IP addresses obtained were automatically anonymised. Anonymisation is carried out prior to any further statistical processing of data in such a way as to avoid any reverse identification of the data subject (taking into account the available technology).

The inspection revealed that the technical and organisational measures adopted with a view to ensuring security of the processed personal data of website visitors were documented by the inspected entity in its Internal Rules for Personal Data Handling. The same measures were described in the records of processing activities maintained by the company as personal data processor pursuant to Art. 30 (2) of the General Regulation. The technical and organisational

measures adopted were evaluated as appropriate. The Office did not find any breach of the GDPR in connection with the personal data processing in question.

Inspector Daniel Rován

Opening of a personal current account by a bank without the client's knowledge and request (UniCredit Bank, a.s.)

The inspection was carried out on the basis of a complaint in which the complainant stated and documented that UniCredit Bank, a.s. (hereinafter the "inspected entity") had opened a personal current account for him without his request. The inspected entity had the complainant's personal data needed to open the account because he acted as the authorised person for his employer's company account kept by the inspected entity.

In response to the complaint, the inspected entity stated that the complainant's banker had opened for the client a current account, "U konto" with U5 insurance by the AXA Pojišťovna insurance company, which the inspected entity documented by a record in the history of contacts. The account was allegedly subject to a debt collection procedure and, therefore, no fees were charged.

During the entire existence of the account, the inspected entity repeatedly contacted the client/complainant with business offers, proposals for a change in the Terms and Conditions and the Product Terms and Conditions, advised him of the closure of the branch where the personal account was kept and downtimes of the systems needed to access Online Banking. The communication was partially related to the company's account because the bank uses the Online Banking as a communication channel, regardless of the product in question.

According to the complainant's statement, the U5 insurance set up for him was cancelled from the outset on the grounds of failure to pay premiums, where AXA Pojišťovna informed the client of this fact in writing. Fees were charged starting from March 2018; otherwise, there were no movements in the account. Between 21 June 2017 and 9 October 2017, the date when a change to the banking system was implemented, the bank did not record any transactions in the account and, therefore, no statement of account was generated. The inspected entity provided evidence of this fact in the form of a copy of the transactions log for the period from 6 October 2017 to 30 November 2018, i.e. until the account was closed.

On 9 October 2018, the complainant was approached by the inspected entity with a claim for repayment of unauthorised debit in the amount of CZK 1,456. Following the reminder notice received, the complainant filed a complaint. The inspected entity was unable to find contractual documents in electronic and physical archives and, as a result, was unable to prove that the agreement on keeping the account had been concluded with the client; therefore, the bank acknowledged the complaint as justified. The account was closed with effect from 20 November 2018, the debit was settled and all related records in the relevant registers were deleted. Measures were taken to ensure deletion of records in the Client Information Bank Register and the Individuals Register kept in SOLUS. At the time when the complaint was being investigated, the banker responsible for the error was already in her notice period.

The case was evaluated by the inspected entity as unauthorised and purpose-driven opening of an account. The inspected entity advised the complainant of the result of the investigation on 19 November 2018, notifying him as follows by e-mail: ... *we have established that the Bank erred in opening the Account. Based on your advice, we have arranged for refund of all*

fees including debit interest and the Account will be closed. We further confirm that we have provided for removal of the negative records from the bank register. Please accept our sincere apology for the error.

The inspected entity stated that the investigation of the complaint had not discovered participation of any other person in this error.

The documentation for opening the current account had been signed by a single employee, which was in accord with the Bank's competence rules. The account had been opened by an authorised banker whose employment with the bank had terminated by notice on the grounds of breach of duties following from the legal regulations pertaining to the work performed by her in an especially gross manner. The notice of termination had been given for other erroneous conduct by the banker and was unrelated to the complaint being investigated.

Thus, it followed from the statement of the inspected entity that it was unable to find contractual documents in electronic and physical archives and, as a result, was unable to prove that the agreement on keeping the account had been concluded with the client. The bank itself acknowledged the complaint as justified. The account was closed, the debit was settled and all related records in the relevant registers were deleted.

The inspection found violation of the following:

- Art. 5 (1)(a) of the General Regulation as the inspected entity in no way proved lawful and correct processing of the complainant's personal data for the given purpose;
- Art. 5 (1)(b) of the General Regulation as the inspected entity collected and processed the complainant's personal data also for a purpose that was not explicit and legitimate;
- Art. 5 (1)(f) of the General Regulation as the inspected entity failed to prove compliance with the internal regulations described in the inspection findings, thus failing to ensure compliance with the technical and organisational measures in place;
- Art. 6 (1) of the General Regulation as it was not demonstrated that in the complainant's case, the inspected entity fulfilled any of the necessary preconditions for lawfulness of personal data processing as set out in the General Regulation.

Since the inspected entity had remedied the defective state of affairs before the inspection was initiated, the Office set the case aside without initiating proceedings because, in view of the foregoing, there was a lack of grounds for initiating administrative proceedings pursuant to Section 40 of Act No. 101/2000 Coll.

Personal data processing (performed directly by the inspected entity or on its behalf) targeting membership base, persons on the waiting list for membership, persons interested in membership, supporters and other persons (potential voters) approached by SPD – Tomio Okamura

The inspection was carried out on the basis of the Office's inspection plan for 2019 in which it was included in view of the current EU-wide topic of fair elections.

The investigation was concerned with fulfilment of the duties by which the inspected entity is bound under the General Regulation in personal data processing carried out either directly by the inspected entity or on its behalf, with a focus on the membership base, persons on the waiting list for membership, persons interested in membership, supporters and other persons (potential voters) approached by the inspected entity.

Within its activities, the inspected entity processes four different data bases for which records of processing have been drawn up. The documents specify the scope of the personal data processed, *specifically name, surname, permanent address, postal address, date of birth, e-mail address, telephone number, education, signature, profession and occupation, political opinions and criminal offences*. Legal ground for personal data processing consists in fulfilment of legal obligations and consent given by the data subject. The personal data concerned are stored both in electronic form and hard copy.

Cloud storage is indicated in the document as the place of storage (for personal data in electronic form). Personal data in printed form are stored by the political group formed by the party's deputies in a filing cabinet the premises of the Chamber of Deputies of Parliament.

The deadline for erasure of the personal data is set at five years after termination of membership, or non-acceptance of a candidate for membership in the party. The deadline for erasure of donors' personal data is set at two years of expiry of the deadline for keeping of tax records laid down by the tax regulations.

Only authorised persons have access to personal data. Personal data are processed manually.

The documents also contain information about 34 personal data processors, including their list in one of the documents. The personal data are not transferred outside the European Union and the documents specify protective and security measures.

The inspected entity has adopted an *Internal Guideline on Personal Data Protection* that lays down employees' duties in personal data protection. Failure to comply with the guideline is subject to contractual penalty and reimbursement of any damage incurred. The guideline lists, *inter alia*, the responsible persons' obligations; for example, to carry out, once annually, an internal audit of compliance with the processing procedures, security and storage of personal data, acquainting all employees with the Directive, and the associated training.

The inspected entity submitted to the Office *contracts for personal data processing* concluded with natural persons operating a business. The contracts are concerned with *payroll, human resources and operational agenda of the controller in accordance with a contract of mandate and the generally binding legal regulations*. Article 2.3 of the contract contains the following provisions: *The Personal Data processing on the basis of the Contract is concerned with sensitive data in the sense of the Regulation*. In this respect, the inspected entity stated that *this point was related to a special category of personal data (sensitive data), specifically political opinions and criminal offences, because a clean criminal record was required for membership in the political movement, as well as non-adherence to political opinions and groups that could be in conflict with the law or the movement's political opinions*.

The contract also stipulates that the personal data will be processed free of charge. It stipulates the obligation to introduce *appropriate technical, organisational, personnel and other suitable measures* to prevent unauthorised or accidental access to personal data and data carriers. It also contains, *inter alia*, a non-disclosure arrangement.

In addition, the inspected entity has in place a *Service Contract* (involving processing activities) for evaluation of interventions on social networks and strategy setting; under the contract, *the provider agrees to connect to its software a project for the client to influence public opinion on social networks and in discussion forums on the internet and, at the same time, to manage the project*.

The inspection verified the fulfilment of duties of a personal data controller stipulated especially in Article 5 (principles relating to processing of personal data), Article 6 (lawfulness of processing), Article 9 (special categories of personal data) and Article 32 (security) of the General Regulation.

The inspection findings revealed violation of Art. 5 (1)(c), (d), (e) because, at variance with Art. 5 (1)(c) of the GDPR, the inspected entity processes personal data of the “donors” group beyond the scope necessary for unambiguous identification of the party to the contract.

It was also ascertained that the inspected entity did not process accurate personal data under the requirement of Art. 5 (1)(d) of the General Regulation, which was verified in the case of a specific member, and the inspected entity also set the deadline for erasure of personal data of non-accepted persons interested in membership and non-accepted persons on the waiting list at variance with Art. 5 (1)(e) of the General Regulation. The same applies to the “donors” group where the time limit stipulated by the legal regulations was excessively extended by two years by the inspected entity.

Furthermore, the inspection revealed violation of Article 6 of the General Regulation, because the inspected entity incorrectly determined the legal title on the basis of which it processed personal data. Personal data of members were not processed under Art. 6 (1)(c), but rather under Art. 6 (1)(f) of the GDPR.

As regards the subject of the inspection, i.e. verifying whether incorrect practices affecting fair elections were used in the processing procedures, no findings were made during the inspection.

Inspector Jiřina Rippelová

Inspection of personal data processing carried out by a political party with emphasis on the membership base and on persons outside the party (i.e. members, persons on the waiting list for membership, persons interested in membership, supporters and other persons approached – potential voters)

In 2019, the Office inspected the political party TOP 09 (hereinafter also the “inspected entity”). The inspection was initiated and performed on the basis of the Office’s inspection plan for 2019. It was included in the inspection plan in view of the current EU-wide topic of fair elections. It was defined as inspection of personal data processing by a political party or movement focused on targeted approaching of individuals for political purposes in connection with the legislation transposing the General Regulation.

The inspectors focused on targeted approaching of individuals (members and candidates for membership, supporters and, if appropriate, other persons approached, i.e. potential voters) for political purposes, regardless of whether they are approached directly by the inspected entity or some other party on its behalf.

The Office found that the inspected entity was collecting information on persons wishing to receive the distributed newsletter, supporters and members of the political party, as well as candidates for membership.

Persons showing interest in receiving newsletters register their e-mail address, supporters register via the website or the my.top09.cz portal, and members of the party/persons interested in membership complete an application form. TOP 09 also uses social networks (Facebook, Instagram, Twitter), where it has an account with a fan site. Thus, it processes personal data of persons interested in receiving newsletters, supporters, candidates for membership and

members, and it also participates in the processing of personal data of users of social networks who have visited its fan site.

In view of the above, the inspected entity is in the position of a personal data controller, or in relation to persons approached via campaigns placed on social networks, in the position of a joint controller. In the sense of the judgement of the Grand Chamber of the Court of Justice of the European Union of 5 June 2018 in Case C-210/16 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH), both Facebook Ireland Ltd. and Facebook Inc., as well as individual owners of fan pages (profiles) on Facebook, must be regarded as (joint) personal data controllers.

Hence, although in this particular case the inspected entity in fact does not have information about the identity of the persons approached (i.e. personal data), as the owner of a fan site it must be regarded as a joint controller together with the above companies that operate the social network in question.

In relation to the relevant processing, the inspection revealed that the inspected entity was using the services of processors and was cooperating with another joint controller. The Office also found that the inspected entity had concluded contracts meeting the requirements of Art. 26 (1) and Art. 28 (3) of the General Regulation. According to the inspection findings, the processing in question is based on consent to personal data processing, or the controller's legitimate interest, as well as on performance of a contract.

Furthermore, the inspected entity provides information to the data subjects from which it collects personal data, within a scope and in a manner corresponding to the requirements set out in Art. 12 (1) and (13).

Also, no breach was found in the area of personal data security, i.e. duties following from Article 32 of the GDPR

However, the inspectors found violation of the duty pursuant to Article 30 of the General Regulation because the submitted records of processing activities did not contain all the required requisites. One category of data subjects (persons interested in receiving newsletters) was not contained in the records at all.

Since the inspected entity immediately remedied the defective state of affairs, the Office did not impose measures to remedy the ascertained shortcomings and refrained from imposing a fine.

Inspection of compliance with the duties stipulated by the General Regulation in processing of genetic data as special categories of personal data

Based on its inspection plan, the Office performed an inspection of Forezní DNA servis, s.r.o. (hereinafter also the "inspected entity"), concerned with personal data processing by a company testing genetic data (DNA), i.e. a special category of personal data.

The Office found out that the inspected entity was providing its clients with a service consisting in paternity establishment and genetic genealogy. Establishing paternity (maternity, blood relationship) is an activity that accounts for approximately twenty per cent of the inspected entity's activities. The main focus of activities is research and development, e.g. in the area of skeletal remains and particularly endangered animal species. In practice, the above percentage amounts to an average of ten persons interested in the paternity test and ten persons interested in the blood relationship test each month. Each test, i.e. DNA analysis, is performed on the basis of a request (order) from the data subject (customer). An order may be placed in person,

by telephone, e-mail, fax, or by completing an electronic order form on the inspected entity's website, or on the website of the online shop at 4N6shop.cz. Subsequently, the required form, information for data subjects on handling of the DNA samples, relevant sampling kits and instructions for use of the sampling kit are handed over/sent to the customers.

For the purposes of establishment of paternity and genetic genealogy that the inspected entity provides as a service to its clients (customers), the inspected entity collects and further processes the following identification and contact details: name and surname, e-mail address, telephone number, contact address for sending printed results of the analyses, and signature. The forms used by the inspected entity for collecting customers' personal data have a corresponding scope.

Genetic data, i.e. specimens consisting in swabs from the oral cavity, are also processed. As regards the actual DNA analysis, the inspected entity only tests the non-coding part of DNA, i.e. it does not process e.g. information on medical condition. The result of the test for blood relationship (e.g. paternity) always gives only a certain degree of likelihood that the specimens under comparison match (the "paternity index").

The inspection concluded that in the case at hand, legal grounds for the personal data processing in question were stipulated by Art. 6 (1)(b) of the General Regulation (performance of a contract) in relation to processing of personal data that are necessary for the performance of a contract to which the data subject (client) is a party, and also by Art. 6 (1)(a) and Art. 9 (1)(a) of the GDPR (consent or explicit consent). Specifically, this concerns processing of special categories of data (information from a DNA sample).

The inspectors also assessed fulfilment of the duty to provide information. They found that information on the testing procedure is available on the inspected entity's website, or the website of the online shop through which the inspected entity was offering its services. Thus, prior to ordering a specific type of test, the client can study a detailed description of the procedure from submitting the request to the performance of the tests to sending or handing over the results and subsequent deletion and destruction of the data and samples.

Clients also have access to a form intended for exercise of their rights. The inspected entity thus provides all relevant information on the manner of personal data processing and on the rights of the data subjects.

During the inspection, the inspected entity submitted to the inspectors a set of internal regulations describing all aspects of processing of personal data and defining their scope necessary for the performance of the inspected entity's activities. It specifies the legal grounds for the processing and contact details of the inspected entity as the controller of the relevant personal data. The inspected entity has thus fulfilled, *inter alia*, its duty under Article 30 of the General Regulation, specifically to maintain records of its processing activities.

Within assessment of fulfilment of the duty to adopt measures to ensure security of the personal data being processed, the inspectors evaluated both physical security of the relevant premises and the technical and organisational measures in place. They concluded that the inspected entity was not in breach of the duties laid down by the General Regulation.

Inspector František Bartoš

Processing of personal data of holders of industrial property rights – natural persons listed in registers of industrial property rights (IPTR, s.r.o.)

The inspection was performed on the basis of the Office's inspection plan for 2019 and a submission sent by the Industrial Property Office.

The inspection was concerned with fulfilment of the duties of a personal data controller stipulated by the General Regulation in processing of personal data of holders of industrial rights – natural persons – listed by the inspected entity in the registers of industrial rights.

The Industrial Property Office stated that the inspected entity was sending to holders of industrial property rights commercial offers for publication (registration) of their industrial property rights on the inspected entity's website. However, as the inspected entity itself admits in the written communication offering registration, it obtains information from the registers of international patents published pursuant to the Patent Cooperation Treaty and trademarks applied for at the World Intellectual Property Organisation with its seat in Geneva, Switzerland, pursuant to the Madrid Agreement concerning the International Registration of Marks and the Protocol to that Agreement.

The personal data contained in individual registers of industrial property rights serve for third parties' reference and for creating a reliable source of information and legal certainty that is necessary for protection of the interests of holders of industrial property rights, fairness of transactions and proper functioning of industrial property rights on the market. It follows from the nature of industrial rights, which are intangible assets, that information on them maintained in individual registers is the only source of information for getting the full picture of the right concerned and enables any third party to become acquainted with this information. It is obvious from the complaints filed by the persons concerned, i.e. copyright holders, that the offers they receive from the inspected entity also contain a request for payment of an amount for publication in the inspected entity's own register, specifically AUD 2,795, EUR 1,954, SEK 18,785 or USD 2,356.

During the inspection, the inspected entity repeatedly failed to provide cooperation, for which fines in the total amount of CZK 100,000 were imposed on it based on a final decision in accordance with the Inspection Rules, where the enforcement of the fines was forwarded to the Customs Administration.

It was possible to infer from the complaints that the Office received from individual complainants via the Industrial Property Office that the individual data subjects had requested that the inspected entity carry out erasure of personal data within the meaning of Article 17, exercised the right to restriction of processing under Article 18 or exercised the right to object under Article 21 of the GDPR.

However, with the exception of a case involving e-mail correspondence with two complainants (they were invited to supplement their submissions) who had accepted the proposed contract by their signatures, no request under Articles 17, 18 and 21 of the General Regulation was ascertained during the inspection.

In view of:

- the manner of collecting and using the personal data of the addressees of the offer letters, including information provided by the inspected entity to the addressees in the offer letters regarding the source of their personal data;

- the determined purpose, including the legal grounds (contractual offer);
- the fact that the inspection could not ascertain whether the inspected entity further processed the address details used, i.e. the suspicion that the controller's duties under Article 14 of the General Regulation had been breached;

if the personal data were not obtained from the data subjects, the inspectors were not able to ascertain violation of the General Regulation.

Personal data processing through the [hlidacvyboru.cz](http://www.hlidacvyboru.cz) web portal (Open Data Company s.r.o.)

The inspection was concerned with fulfilment of the duties of a personal data controller stipulated by the General Regulation in relation to personal data processing through the web portal www.hlidacvyboru.cz, operated by Open Data Company s.r.o. (hereinafter also the "inspected entity").

In his submission, the complainant stated that on the above-specified website, the operator was publishing information on members of committees of unit owners' associations, including information on the complainant as a member of the Committee of the Association of Unit Owners in Prague's eight district (hereinafter also the "Association"). The information in question consisted of name, surname, academic degree, position in the Association and information on data sources. The complainant stated that this constituted a disproportionate interference with his private life, where the company operating the website had nothing in common with the Association.

The complainant further furnished evidence that he had objected against the processing of his personal data and had requested that the company erase his personal data. Pending resolution of the objection, the complainant had exercised the right to restriction of processing under Article 18 of the General Regulation.

V The inspection revealed that the inspected entity had responded to the complainant's request for erasure of personal data. According to the inspected entity, the complainant's personal data fell in the group of "unlimited public information", i.e. information published by the public administration without any limitation, and any person may access all such information without any further conditions. In the following part of the reply, the inspected entity informed the complainant that the prerequisites for processing of his personal data in a public register on the basis of a legitimate interest were met without there being a need to obtain the consent of data subjects under the General Regulation.

The inspected entity further stated that it had assessed its legitimate interest in publishing the complainant's personal data and, after documenting this fact, it was prepared to submit this conclusion to the Office for inspection in accordance with the accountability principle.

V The Office also ascertained during the inspection that the inspected entity was obtaining information from public registers, namely the Commercial Register – register of associations of unit owners, from the Insolvency Register and other registers, and was offering this activity within its business activities.

The complainant had repeatedly raised an objection at the controller under Article 21 of the General Regulation and requested restriction of processing under Article 18 of the General Regulation until a decision on the objection was made and, subsequently, erasure from the [hlidacvybor.cz](http://www.hlidacvybor.cz) website.

In its statement, the inspected entity stated that it did not accept the complainant's request because it was processing personal data on the basis of its legitimate interest while relying *inter alia* on the balance test. The test had shown that the inspected entity was meeting the prerequisites for processing of personal data obtained from public registers on the basis of a legitimate interest without the need to obtain the consent of the persons concerned.

The inspection concluded that the inspected entity had breached its duty pursuant to Art. 6 (1)(a) of the General Regulation, i.e. it processed personal data without the complainant's consent and in the absence of any other legal grounds.

After the complainant objected to the processing of his personal data within the meaning of Art. 21 (1) of the GDPR, the inspected entity was not entitled to continue processing his personal data on the *hlidacvyboru.cz* website because the substantiation it provided concerning its legitimate interests in publication of the complainant's personal data as a member of the Association's committee was not in conformity with the General Regulation. The inspected entity also failed to sufficiently prove the existence of other material grounds for processing of the complainant's personal data on the *hlidacvyboru.cz* website that would be in accordance with the General Regulation.

By failing to comply with the complainant's request for erasure of his personal data, the inspected entity violated Art. 17 (1)(c) of the General Regulation.

The inspected entity raised objections against the findings contained in the inspection record, which the President of the Office rejected and the inspection record was confirmed. In the subsequent administrative proceedings, the inspected entity was ordered to end the processing of the complainant's personal data, destroy them and subsequently inform the complainant accordingly. The inspected entity complied with this obligation.

Inspector Petr Krejčí

Processing of personal data attesting to health condition within the provision of accommodation services (MERKURIA UNION, s.r.o.)

Based on a submission forwarded by the Social Affairs Department of the Regional Authority of the Pardubice Region, the Office performed an inspection at MERKURIA UNION, s.r.o., with its registered office in Nová Ves u Litomyšle. The inspection revealed that the aforementioned company was providing social services based on several trade licences in its "Pohodlí" retirement home. Specifically, this included inn-keeping activities, purchase of goods for the purpose of their resale and sale, real estate management and maintenance, and activities in real estate. The accommodation facility provides services to 55 persons in various degrees of dependence on assistance who receive allowances for care granted by the Czech Labour Office.

It was found that the accommodation provider, MERKURIA UNION, s.r.o., was also collecting sensitive data concerning the medical condition of the residents. In the "Agreement on Accommodation and Meals", it requires residents to submit upon admission to the accommodation facility a medical report and information on a contact person or relatives. It was established that the files of the accommodated persons contained documents titled "Social inquiry" with brief records concerning the areas in which the resident needed assistance from another person, as well as information about the person's medical condition and contact details of a close person. Twelve social care assistants provide assistance to the residents of the accommodation facility and they come into contact with the residents' personal data.

Given that MERKURIA UNION, s.r.o. is not authorised to provide health care and social care, there was a suspicion that the accommodation provider was collecting sensitive personal data without authorisation. Therefore, the Office was asked to investigate the above submissions.

The Office's inspection was concerned with fulfilment of the duties stipulated by the General Regulation and Act No. 110/2019 Coll., on personal data processing, which replaced Act No. 101/2000 Coll. with effect from 24 April 2019, in the processing of personal data of the clients receiving accommodation and meals from the "Pohodlí" Retirement Home. The home also provides them with health care and social services without statutory authorisation within the meaning of Section 78 of Act No. 108/2006 Coll., on social services, including the processing of special categories of personal data, which should be based on a legal ground pursuant to Art. 9 (2)(g) of the General Regulation, within the scope of the controller's business activities.

If the inspected entity provides in its facility, in addition to meals, also health care and social services to the accommodated clients without authorisation to provide such services pursuant to Section 11 of Act No. 372/2011 Coll., on health care services and the conditions for their provision (the Act on Health Care Services) and Section 78 of Act No. 108/2006 Coll., on social services (in the case of the "Pohodlí" Retirement Home, the services were provided using the retirement home's employees until June 2018 and later their status was changed to social care assistants operating a business under a special law, and allowances for care granted by the Czech Labour Office were paid for this care depending on the degree of dependence on the assistance of another person, whether into the account of the inspected entity or, at the time being, into the account of one of the social care assistants, and hence the inspected entity has access, in particular, to the special categories of personal data indicated in the documents filed in the "patient medical records" or in the "client file", thus failing to satisfy any of the conditions set out in Art. 6 (1)(a) GDPR and any of the exemptions from the prohibition to process special categories of personal data set out in Art. 9 (2)(a) to (j) of the General Regulation), the inspected entity's processing did not meet the requirement for lawfulness of processing of data subjects' personal data, or violated the prohibition to process special categories of data subjects' personal data.

In the case at hand, the inspected entity was not authorised to process even the clients' birth identification numbers. Within its business activities, the inspected entity only possessed trade licences for accommodation and catering services and it thus also failed to comply with the conditions of Act No. 133/2000 Coll., on population records and birth identification numbers and on amendment to certain laws (the Act on Population Records).

If the inspected entity uses its registered office in which the "Pohodlí" Retirement Home is located for provision of social care and is actively engaged in such care, including presentation of its activities, it is obliged to comply with the requirement for lawfulness of personal data processing. This involves fulfilment of the duties of a personal data controller pursuant to the General Regulation and Act No. 110/2019 Coll. in conjunction with Act No. 108/2006 Coll., on social services. The inspected entity is obliged to ensure that this activity is performed only by a person authorised to do so, especially pursuant to Act No. 108/2006 Coll. (Section 78) and Act No. 372/2011 Coll. (Section 11), and that unauthorised persons do not have access to the patients' medical records maintained and to the clients' personal files, while ensuring that the persons concerned have been demonstrably acquainted with the procedures in handling documents as a guarantee of protection of the patients'/clients' personal data contained in the relevant documents.

In particular, patients' medical records may be accessed only by a person authorised under the law, i.e. also within the meaning of Section 3 (3) of Act No. 98/2012 Coll., on medical records. This must be a health care worker or some other professional who has provided the patient with a health care service, made a corresponding entry in the medical records and confirmed correctness of the entry by his/her signature.

The inspection carried out by the Office confirmed the suspicion of unlawful conduct of the inspected entity to the full extent.

The inspector discovered serious and long-lasting violations of the above laws, for which a fine of CZK 50,000 was imposed on the inspected entity in administrative proceedings.

Processing of personal data of persons transported in means of transport (Dopravní podnik hl. m. Prahy, akciová společnost)

The inspection in the public transport company Dopravní podnik hl. m. Prahy, akciová společnost (hereinafter also the "inspected entity") was initiated on the basis of the Office's control plan for 2019.

The inspection focused on the inspected entity's conduct in the area of personal data protection since the last inspection conducted in 2012.

The inspection was concerned with fulfilment of the duties stipulated by the General Regulation in conjunction with Act No. 110/2019 Coll., on personal data processing, in processing of personal data of data subjects in the context of the checking of tickets and the subsequent processing of personal data, as well as in connection with the purchase of season tickets.

At the site where the physical inspection was performed, certain data are recorded in electronic forms when personal data of customers/passengers who purchase (season) tickets in printed form from an employee at the counter are entered directly in electronic systems. These data comprise name, surname, date of birth, date of issue and expiry date and, for student discounts, school (Id. No.), school year, and grade. Pre-printed boxes for data on sex, birth identification number, postal code and country are not to be completed.

The inspected entity did not process the data from these pre-printed boxes, and the boxes themselves were deleted from the form as redundant during the inspection.

Similar systemic measures related to personal data protection are also in place at other points of sale in relation to the issue of cards, collection of applications for the travel pass, complaints, and issue of duplicates of cards with records of deactivated cards that are stored in a safe place (locked in cash boxes or safes).

Under Art. 12 (3) of operating regulation D 6, "Regulation for Ticket Checks" effective from 1 July 2012, a ticket inspector may check personal data of passengers in order to enforce the payment of surcharge on the fare. This occurs on the basis of a document issued by the competent administrative authority within the following scope: name, surname, date and place of birth, postal address, type and number of the document from which the personal data were ascertained.

The inspected person processes personal data, as is obvious from the standardised record of the ticket check drawn up by ticket inspectors in connection with the recording of identification details of passengers who fail to present a valid ticket and fail to pay the fare and surcharge on the fare for the purpose of enforcing the claim in court proceedings. The personal

data concerned comprise number of the record serving as a variable symbol for the payment, date, time, transport line, authorised person/identification tag number, place of the check, surcharge, basic fare, surname and name of the passenger/debtor, date and place of birth, information ascertained from the document, country, postal address – street, building number, municipality, telephone number/e-mail, marked box in a checklist for description of the event, ticket number, information on whether or not the ticket was removed from the passenger, passenger's confirmation of correctness of the recorded data, information on whether or not the passenger accepted a copy of the record, signed or refused to sign the record, internal record, date of signature of the passenger/debtor, signature of a person authorised by the transport company, his/her stamp, and information for the passengers on the reverse side concerning payment options and the travel company's further procedure.

The "Declaration of debt assumption" form, which the transport inspector completes to the same level of detail as when recording the passenger's details, is used in the event that the passenger is unable to pay the applicable surcharge in cash on the spot and has no personal identity document and another person volunteers to pay the surcharge for the passenger (not applicable when the payment is made on the spot). However, such a person must be over 18 years of age or a person of legal age accompanying a minor who assumes the minor's debt from the ticket check.

It is obvious from the standardised record of passenger personal identity check that is completed by the Czech Police in case a passenger fails to prove his/her identity and pay the fare and the surcharge on the fare to the ticket inspector when travelling without a valid ticket, that the inspected entity collects the following personal data of the passenger: date, time, place of the check, surname, name, date of birth and birth identification number divided by a slash, information on from what document the data were obtained, permanent address – street, building number, postal code, district, note, officer's identification number and signature, where the number after the slash following the date of birth serves the Police only to verify the passenger's (true) identity; the inspected entity does not process this particular piece of information any further and subsequently renders it illegible in the printed form by blacking it out.

It is worth considering whether it is reasonable, from the perspective of the principle of minimisation, and whether it is justifiable for the inspected entity to even have this redundant information included in the form given that the inspected entity does not process it any further. Using the document on payment of the surcharge on the fare by a passenger who failed to submit a valid ticket, the inspected entity processes the following: document number, date, transport line and time, where the receipt for the passenger contains the following: document number, transport line, time, vehicle number, inspector identification tag number, date.

In accordance with the principles of personal data processing set out in Article 5, the inspected entity was able to demonstrate compliance in the sense of the principle of responsibility for compliance with all the rules stipulated by the General Regulation pursuant to paragraph 2 of the aforementioned Article, i.e. a requirement which always applies, and it hence did not violate the principles of personal data processing set out in Art. 5 (1) of the GDPR. With reference to Art. 5 (2), the inspected entity was able to demonstrate compliance with all principles directly related to proving lawfulness of personal data processing in connection with the conclusion of a contract with a data subject on (repeated) provision of the service consisting

in public city transport and metropolitan area integrated transport system by the inspected entity, i.e. the transport company.

In connection with the activities of the inspected entity and given that certain measures were implemented already during the inspection, the inspectors did not ascertain any breach of the duty to provide information to data subjects as referred to in Art. 12 (1) of the General Regulation. Similarly, no breach of the duty to provide information following a request of a data subject pursuant to Art. 12 (3) of the General Regulation was found.

The inspected entity did not violate its duties within the scope of the subject of the inspection as set out in Articles 24 and 25 of the GDPR as it guaranteed that the processing was carried out in accordance with the aforementioned provisions and the inspectors did not ascertain any breach in terms of personal data protection.

The inspected entity guaranteed to maintain records of all processing activities within the meaning of Article 30 of the General Regulation and within the scope of the inspection, i.e. records concerning the processing of personal data of passengers to whom recorded cards were issued, as well as concerning the processing of personal data of passengers who failed to present a valid ticket, failed to pay the fare and surcharge on the fare and were recorded as debtors, and also in connection with the sale of tickets, claims, etc. under its responsibility.

At present, the inspected entity has rules and regulations in place that guarantee compliance with Act No. 110/2019 Coll. and the General Regulation in the performance of its activities.

Private Sector Inspection Unit

Inspection of the processing of cookies by Velká Pecka s.r.o.

Based on the Office's inspection plan for 2019, the Private Sector Inspection Unit conducted an inspection concerning the processing of cookies⁵ and their use in remarketing at Velká Pecka s.r.o. (hereinafter also the "inspected entity").

Within the inspection, the Office first focused on the legal framework under which cookies are maintained. The provisions applicable in Czech legislation are contained in Section 89 (3) of Act No. 127/2005 Coll., on electronic communications – transposition of Art. 5 (3) of Directive 2002/58/EC. On the basis of the Directive, the opt-out principle was introduced for cookies in Czech laws, i.e. users of end devices had to be notified that cookies would be stored on their device and they had the option to refuse such storage. The Directive was amended in 2009 and redesigned to the opt-in principle, i.e. users must first obtain all information about the processing of cookies and subsequently accept such processing before the cookies can be stored on their devices.

The Czech legislator reflected this amendment in the relevant law, i.e. Act No. 127/2005 Coll., but did so incorrectly. As a result, national legislation (Act No. 127/2005 Coll.) is at variance with the legal framework of the European Union (Directive 2002/58/EC), because the opt-in principle was introduced on the basis of the amendment to Directive 2002/58/EC, but the national laws in fact continue to operate with the opt-out principle.

⁵ Cookies are small text files that are stored on the user's device (computer, telephone, etc.) when visiting a website and carry information about the websites visited by the user and the information searched on them. Therefore, companies often use cookies to target advertising to defined users. The practical implications for the data subject are such that the websites browsed by him/her (e.g. news websites and other portals with advertising space) subsequently show a targeted offer of websites visited earlier.

Inspectors thus had to deal primarily with the legal question concerning the relationship between national and EU laws. In general, the case-law of the European Court of Justice lays down the principle of precedence of EU law over national legislation, based on the ruling in case 6/64 *Costa v E.N.E.L.* Another legal principle lies in “Euro-conforming interpretation” following from the ruling in case 14/83 *von Colson*, which sets the duty to interpret national laws in the light of EU regulations. However, the inspectors found that the variance between national and EU laws was so serious that it could not be overcome by interpretation conforming to EU law.

The inspection also examined the effect of Directives. However, it had to assess the case-law of the European Court of Justice (e.g. *Marshall*, C-152/84, *Tullio Ratti*, C-148/79 and *Van Duyn*, C-41/74).

Based on these rulings, the inspectors concluded that, in principle, a Directive cannot have a direct effect on an individual. Therefore, the Office concluded that the inspection had to take place in the light of national legal regulations.

On the basis of the above, the inspectors focused on whether or not the inspected entity proceeded in accordance with the General Regulation as well as Act No. 127/2005 Coll. in handling personal data (cookies) for remarketing purposes.

First, they concluded that cookies can be subsumed under the notion of personal data within the meaning of Art. 4 (1) of the General Regulation, in conjunction with Recital 30 of the General Regulation, which states that natural persons may be associated with cookie identifiers. However, these identifiers leave traces that, in combination with other information obtained by servers, can lead to unambiguous identification of a specific natural person and may be used for profiling.

Another question under scrutiny was whether the inspected entity was in the position of personal data controller within the meaning of Art. 4 (7) of the General Regulation. The inspectors concluded that the inspected entity was in the position of personal data controller because it had determined the purpose and means of personal data processing. In the case at hand, purpose consists in personalisation of displayed advertisements and preferential offering of goods, while means of personal data processing consist in the individual services that the inspected entity uses (e.g. *DoubleClick*, *Custom Audiences* and *Lookalike Audiences*).

In the conclusion of their investigation, the inspectors stated that the inspected entity was obtaining personal data in accordance with the parameters set out in Section 89 (3) of Act No. 127/2005 Coll. as it was providing the data subjects with information in accordance with the requirements of the cited provision. At the same time, the inspected entity properly fulfils the duty to provide information within the meaning of Articles 12 to 14 of the General Regulation and informs the data subjects especially about the scope and purpose of personal data processing while simultaneously allowing them to decline such processing.

The inspected entity did not raise any objections against the inspection findings.

Support Unit

Inspection of an electricity supplier (ČEZ Prodej, a.s.)

On the basis of a reported personal data breach, the Office performed and closed an inspection of an electricity supplier.

The inspection was concerned with fulfilment of duties by which the inspected entity, ČEZ Prodej, a.s., was bound under the General Regulation in connection with the transmission of

personal data of gas consumers (who are not electricity consumers at the same time) that were provided on the basis of Section 8 (10) of Act No. 348/2005 Coll., on radio and television broadcasting. Under the above law, an entity supplying electricity to consumers has the duty to provide the statutory broadcasting operator with information about consumers with whom the supplier has concluded contracts for electricity supply.

Within 30 days of the date of delivery of a request to this effect, the supplier of electricity to consumers shall provide the address of the delivery point and certain other personal data. These comprise, for a consumer who is a natural person, name(s) and surname, date of birth and permanent address (for foreigners, the place of long-term residence), or, for a consumer who is a natural person operating a business, name, surname, or business name if applicable, place of business and identification number, or, for a consumer who is a legal entity, business name or name, legal form, registered office and identification number, or, for a consumer who is an organisational component of the State or a territorial self-governing unit, name, registered office and identification number of the consumer.

Under the law, a supplier of electricity to consumers may claim from the broadcasting operator reimbursement of purposefully expended costs incurred by the supplier in direct connection with satisfying the supplier's request.

The inspected entity learned about the incident in question only following a complaint filed by a customer who had been contacted by Czech Radio in connection with payment of the licence fee. An analysis was performed which revealed that an employee of the inspected entity incorrectly handled data bases of customers purchasing both electricity and gas.

Transmission of a database which contained personal data of gas consumers to Czech Radio and Czech Television constituted unlawful personal data processing because the inspected entity has no legal ground for transmitting personal data of gas consumers.

The inspected entity did not have in place a separate management document for the procedure in administering the above duty that would regulate individual data exports; the handling of data is governed by general procedures set out in the management documentation for personal data protection and for information security and cyber security.

The adopted (general) measures and instructions for employees that were in place before the breach was detected resulted in breach on the part of the relevant employee in creating the data base and hence also breach of the General Regulation.

Without delay after the incorrectly generated database was detected, the responsible manager issued an instruction for the employees' procedure in creating the relevant data bases. The inspected entity also provided its employees with relevant training. Furthermore, representatives of Czech Television and Czech Radio were informed about the situation without delay by telephone and in writing and were asked for cooperation, erasure/anonymisation of personal data, discontinuation of the process of sending reminder notices and enforcement of licence fees in relation to the personal data transmitted without authorisation.

The Office found that by the aforesaid conduct, the inspected entity had breached the duties stipulated by Art. 6 (1) of the General Regulation (lawfulness of processing) and Article 29 of the General Regulation (processing only under the authority of the controller).

• SUPERVISION IN THE AREA OF COMMERCIAL COMMUNICATIONS

In 2019, the Office received a total of 2,007 complaints concerning the sending of unsolicited commercial communications; the complaints were filed using the form that is available for this purpose on the Office's website or via the electronic filing system.

It should be noted at this point that it is very important for filing a complaint that the petitioner (complainant) completes the source code of the e-mail message (the form for filing complaints against the sending of unsolicited commercial communications contains detailed instructions on where the source code of the e-mail message can be found and how it can be inserted in the form); the complainant should also attach the text of the received e-mail or a screenshot of the received unsolicited text message. These data then serve as evidence.

If the complaint is filed via the Office's electronic filing department (posta@uouu.cz), the complainant should send the entire e-mail (the entire communication received by him/her) in the .msg or .eml format (the entire message is then stored in one of these formats, including the text and the source code of the e-mail message). It is useful to provide also other information in the submission itself, most often e.g. information that the complainant has expressed disagreement with receiving any further commercial communications, including proof to this effect, information on the complainant's relationship to the sender, etc.

If a complaint is filed using the web form, the complainant can at any time check the progress of processing of his/her complaint. Progress is updated every time the handling of the complaint moves to a next stage (e.g. analysis, notification of the subject of possible breach, inspection, resolution of the inspection).

Complaints in relation to which it was found that the sender was a foreign entity within the EU were forwarded to the competent foreign supervisory authorities based on cross-border cooperation. For this purpose, Regulation (EC) No 2006/2004 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation)⁶ established the CPC system (Consumer Protection Cooperation). In some cases, the Commercial Communications Unit made use of the option to make an inquiry or to request cooperation via the IMI (Internal Market Information) system.

In 2019, within cross-border cooperation, the Commercial Communications Unit directed requests to the competent supervisory authorities (twice in Poland, twice in the United Kingdom, twice in Germany, once in Ireland, once in Lithuania, and once in Hungary). This cooperation is yet to be properly evaluated in terms of implementation of necessary enforcement measures to prevent or stop dissemination of unsolicited commercial communications by companies established in the respective countries. These cases were not closed by the end of 2019 or it was ascertained that the entities distributing the commercial communications were merely registered in the given country and either did not operate there or could not be reached.

⁶ On 17 January 2020, Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 enters into effect.

Numerous complaints were also directed against foreign entities established outside the EU. In some cases, the sender or the party for whose benefit the commercial communications were sent could not be traced. These were mostly suspicious online shops that do not provide any contact details on their website and were also in focus of the Czech Trade Inspection Authority or operated outside the European Union.

Inspection activities and imposition of penalties accounted for the greater part of the Commercial Communications Unit's activities in 2019. Where only a small number of complaints were raised, the entities concerned were merely advised of the possible violation of the law in dissemination of commercial communications. They were also thoroughly instructed on how to proceed in order to send commercial communications in accordance with the law. On the other hand, in cases where there are numerous complaints, the entity in question is subject to an inspection procedure.

In 2019, the Unit initiated 18 inspection procedures and opened administrative proceedings with 28 entities, resulting in the imposition of a penalty. The Unit imposed penalties in the amount of CZK 2,099,000 for the dissemination of unsolicited commercial communications. In addition, administrative proceedings on imposition of a procedural fine for failure to provide cooperation during the inspection were conducted in 11 cases, where the total amount of the penalties imposed was CZK 475,000. A total of 390 entities were advised of possible violation of the law in 2019.

The Commercial Communications Unit also provided information to the public. This information was intended for potential recipients of commercial communications as well as for companies that were uncertain about how to send commercial communications correctly. To this end, the Office reviewed in 2019 the section titled Frequently Asked Questions on Act No. 480/2004 Coll. and several reports were released based on the supervisory practice in the area of dissemination of commercial communications.

Inspection of GlobalAdvertisement s.r.o.

The inspection was initiated on the basis of complaints concerning the distribution of unsolicited commercial communications. It assessed fulfilment of the duties following from Act No. 480/2004 Coll. concerning the distribution of commercial communications by electronic means.

Complaints against the sending of unsolicited commercial communications by the aforementioned company continued to be filed also in the course of the inspection procedure. In all, the number of complaints filed was 675.

GlobalAdvertisement s.r.o. initially cooperated in the inspection procedure and provided at least general statements on the complaints. It admitted having sent the commercial communications, to its clients' e-mails. The company stated that it was building the client data base e.g. through the Fortune Wheel entertainment game and the clients had given their consent to receiving the commercial communications. Nevertheless, the inspected entity failed to document this consent in any way, nor did it present the conditions or details of the Fortune Wheel game in spite of several requests that the inspectors made to this effect during the inspection. Subsequently, the inspected entity furnished only details concerning affiliate programmes in relation to two companies for whose benefit it had been sending commercial communications.

Affiliate programmes are a commission marketing scheme used in online advertising. They link the website of a seller of goods or services with the websites of parties recommending the goods or services (promoters). Promoters are paid by the seller on a commission basis.

The affiliate programme mechanism can be simply described in four steps:

- the customer visits the seller's website via the promoter's website or orders the seller's goods or services through the promoter;
- the seller subsequently contacts the customer and verifies the order;
- the customer pays to the seller;
- the seller pays the commission to the promoter (the amount of the commission is agreed internally; it may be a fixed amount, a percentage, etc.).

As follows from the above, affiliate programmes are marketing tools. The advantage of this type of marketing is that the effectiveness of the advertising can be easily measured by the number of clicks on the promoter's website. Another advantage of these programmes is that the advertising is directed at a target customer group, which brings savings in the costs of advertising.

However, as the number of complaints was increasing and the inspected entity was being requested to provide additional statements, the company stopped communicating with the Office.

The Office subsequently imposed a penalty in the amount of CZK 300,000 for failure to provide the necessary cooperation. The amount of the penalty reflects, in particular, the large number of complaints delivered and the long period of time (several months) during which the inspected entity failed to provide cooperation despite the fact that all the requests were demonstrably delivered to it (the authorised person logged in to the data box). The inspected entity had been sending commercial communications concerning offers of goods and services from various online shops, which made the inspectors' investigation more challenging. The Office thus requested cooperation from the online shops for whose benefit the commercial communications had been disseminated.

The Office also contacted the hosting services providers with a view to determining to whom hosting services had been provided in relation to the domains of the e-mail addresses from which the commercial communications had been disseminated, as well as to the domains of the websites of the online shops for the benefit of which the commercial communications had been sent. Last but not least, the Office also referred to the texts that had been disseminated and, more importantly, the source codes from the commercial communications.

During the inspection, the Office detected links among several companies and discovered that they were involved in some of the affiliate programmes. In the cases investigated, the inspected entity was the distributor of the commercial communications. Other companies (for whose benefit the commercial communications were sent by the inspected entity) were the disseminators of the relevant commercial communications in the position of mandator – party ordering the commercial communications, because by engaging in the affiliate programme, they disseminated the commercial communications and caused them to be distributed.

As stated above, the inspected entity did not provide any evidence of consent (i.e. legal grounds) to the sending of commercial communications to the relevant e-mail addresses. The inspected entity's assertion that the e-mail addresses originated e.g. from the "fortune wheel"

cannot be regarded as demonstrable consent to the sending of commercial communications. Therefore, the inspected entity breached the obligations laid down in Section 7 (2) of Act No. 480/2004 Coll., i.e. the duty to use electronic contact information for the purpose of dissemination of commercial communications only in relation to users who have given their prior consent to this effect.

Furthermore, the Office came to the conclusion that Section 7 (4)(b) of Act No. 480/2004 Coll. had also been violated because the commercial communications did not contain an unambiguous identification of the person on whose behalf the communication was made. The Office also noted in this respect that the companies for whose benefit the commercial communications were disseminated had too breached Section 7 (2) of Act No. 480/2004 because they were disseminators of commercial communications in the position of mandator – party ordering the commercial communications.

No objections were raised by the inspected entity against the inspection record.

Since GlobalAdvertisement s.r.o. had ceased to exist on 11 July 2019, the relevant administrative proceedings could no longer be pursued against the company. Thus, administrative proceedings were initiated only with the companies for whose benefit the relevant commercial communications had been disseminated.

As for the applicable provisions of Act No. 480/2004 Coll. pertaining to the sending of commercial communications, it should be noted that public-law liability for an infraction pursuant to Section 11 (1) of Act No. 480/2004 Coll. is formulated as no-fault liability (liability for a legal situation where it is not necessary to examine culpability for the unlawful state of affairs in relation to a legal entity). It is specifically for this reason, and also with a view to meeting the legislator's intention (to protect privacy as extensively as possible), that persons for whose benefit commercial communications are disseminated are also considered disseminators of commercial communications.

Therefore, along with the actual sender (GlobalAdvertisement s.r.o.), the companies for whose benefit the commercial communications were sent are also responsible for the distribution of the commercial communications.

Disseminators of commercial communications, whether the ordering entity (i.e. the party for whose benefit the commercial communications are distributed) or those who actually send them, should always sufficiently verify whether the addressees of the commercial communications have granted their consent to such sending, and in general, whether the distribution is carried out under the law.

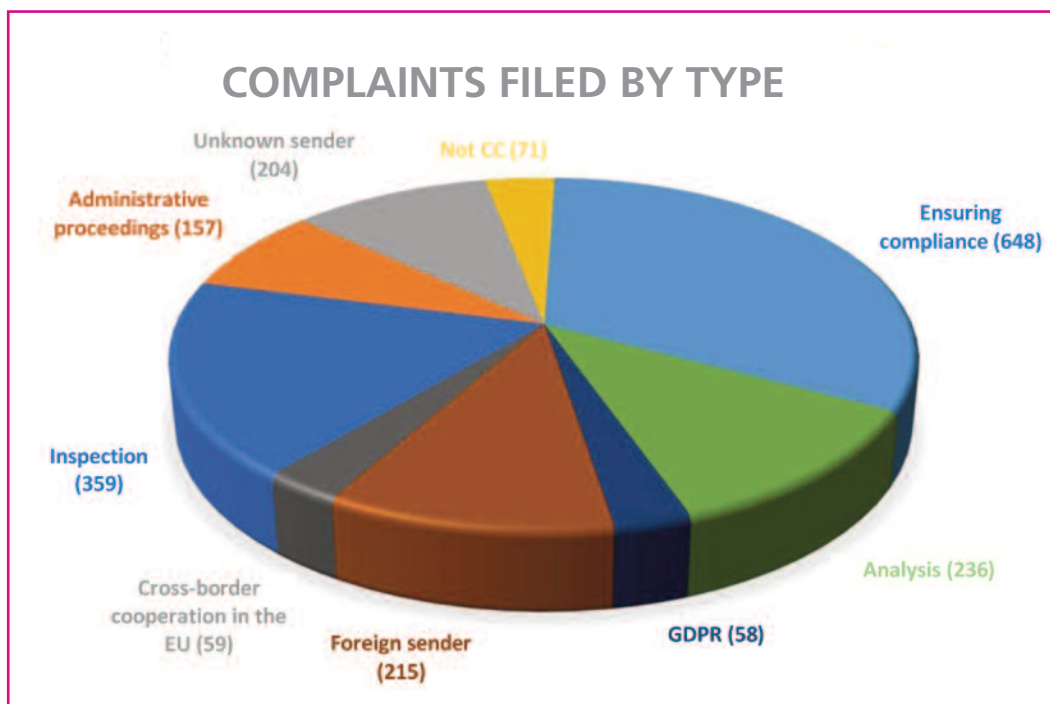
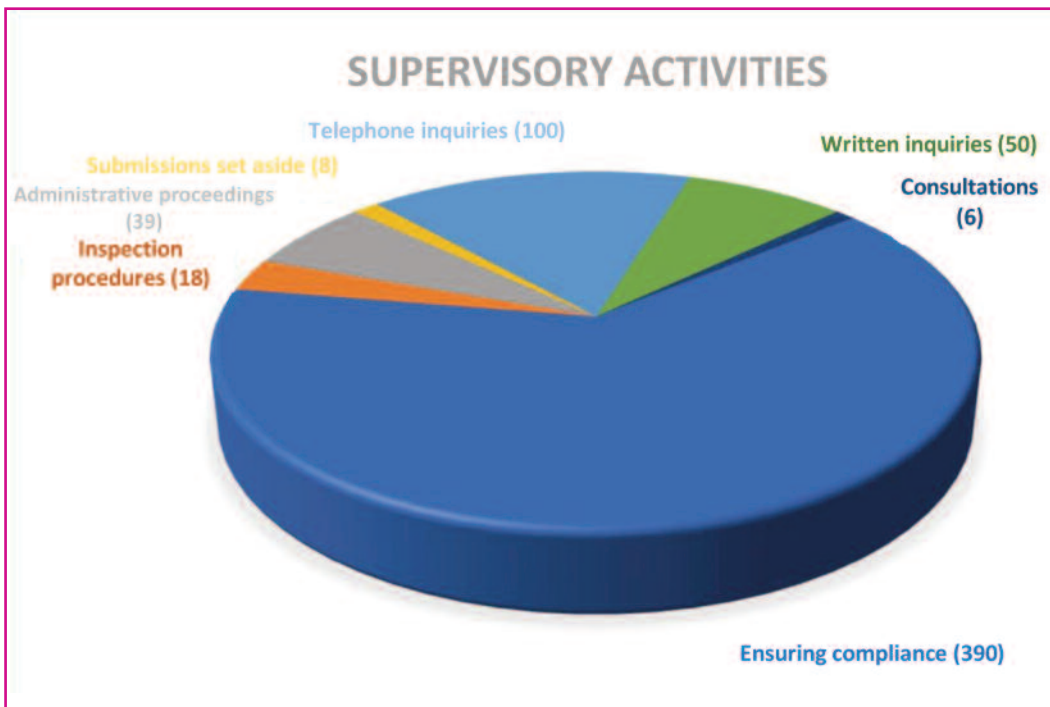
By delegating the sending of the commercial communications to GlobalAdvertisement s.r.o., the companies for whose benefit the commercial communications were sent are not relieved from liability. To the contrary, they must be able to furnish consents from the addressees of the commercial communications or obtain these consents from the distributing company. It is not sufficient to rely on assurances of the distributing company that it has the relevant consent.

By nature, consent to the sending of commercial communications requires that the person granting it must know what s/he consents to (the purpose of the commercial communications and how they will be sent) and by whom, or for the benefit of whom, they will be sent. Such consent must also be demonstrable.

For the above-specified breach, a penalty was imposed on the companies for whose benefit the relevant commercial communication had been disseminated, in the amount of CZK

350,000, CZK 9,000 and CZK 15,000, respectively. The penalties imposed reflected, in particular, the number of complaints received (i.e. commercial communications sent). As an important mitigating circumstance, it was taken into consideration that the companies in question had not been the actual senders of the relevant commercial communications and their reputation and goodwill could also be harmed by the improper conduct of the sender.

The following page depicts graphically the supervisory activities in 2019 and the progress of resolution of individual complaints in 2019.



● ADMINISTRATIVE PUNISHMENT

In 2019, Act No. 110/2019 Coll., on personal data processing, took effect. It supplements and complements in certain ways the directly effective General Regulation and its adoption significantly affected the area of administrative punishment.

In view of the fact that the Office continued to resolve cases opened before the effective date of the Act on Personal Data Processing (i.e. at a time when Act No. 101/2000 Coll., on personal data protection, was in effect), it was necessary to deal in administrative proceedings with the question as to which law should be applied in case of a conflict between the two.

In administrative proceedings initiated and not concluded by a final decision before the effective date of the Act on Personal Data Processing, it was necessary to apply Section 66 (5) of Act No. 110/2019 Coll., and complete the proceedings pursuant to Act No. 101/2000 Coll. If the relevant conduct occurred during the term of effect of Act No. 101/2000 Coll., but the Office resolved it only after the new Act on Personal Data Processing came into effect, it was also necessary to take into account Art. 40 (6) of the Charter of Fundamental Rights and Freedoms, according to which punishability of an act is assessed, and the punishment imposed, according to the law effective at the time when the punishable conduct occurred.

The newer law is applied only if it is more favourable for the offender. Typically, this was the case with respect to breaches of the duty stipulated in Section 15 (1) of Act No. 101/2000 Coll., i.e. the duty of the controller's employees to maintain confidentiality of personal data, where such conduct is no longer punishable as an infraction under the Act on Personal Data Processing.

A case concerning an employee of the Czech Police can serve as a specific example. She unjustifiably perused a criminal file through the information system and provided the information contained in the file to a third party. In view of the above, the Office had to set the case aside by its resolution pursuant to Section 76 (1)(a) of Act No. 250/2016 Coll., on liability for infractions and proceedings concerning infractions, since the proceedings were now conducted during the term of effect of the Act on Personal Data Processing whose provisions were more favourable for the offender.

Taking of effect of the Act on Personal Data Processing also significantly affected administrative punishments by public authorities and bodies due to its Section 62 (5), which stipulates that the Office shall waive administrative punishment also with respect to authorities and bodies set out in Art. 83 (7) of the General Regulation. By virtue of this provision, the Czech Republic applied its discretion to implement certain variations from the GDPR in its national legislation and provided for the possibility of waiving administrative punishment with respect to public authorities and bodies established in the country. In 2019, the Office applied this provision to seven authorities and bodies (in case of two of them, such a decision was only adopted by the Office's appellate body) in respect of which it found specific violation of the rules for personal data processing stipulated by the General Regulation. These included e.g. the Ministry of the Interior, a school, the City of Brno and the Czech Schools Inspectorate.

For example, the Office found that the Ministry of Transport had committed an infraction pursuant to Section 62 (1)(a) of the Act on Personal Data Processing. In the case concerned, the Ministry had failed to ensure that the tender dossier provided to several tenderers for the supply of the electronic toll system would not contain personal data of the employees of a company

participating in the preparation of the dossier. This included the name, surname, telephone number, working e-mail address, job title or position and information on completion of training, authorship or coauthorship of the document or participation in meetings.

The Ministry is a public authority (public body), and the Office thus had to waive administrative punishment pursuant to Section 62 (5) of the Act on Personal Data Processing.

In 2019, the Office also applied in its decision-making Section 65 of the Act on Personal Data Processing, which allows the Office to set aside certain types of unlawful conduct by a resolution without initiating infraction proceedings. Such a procedure may be applied only in case of, for example, a low severity of breach or endangerment of the protected interest affected by the conduct in question or if the controller has ensured remedy immediately after the breach of the rules for personal data processing has been found. A similar provision had already been contained in Section 40a of Act No. 101/2000 Coll.

The Office applied the above provision in 25 cases (six of which were subject to the previous legal regulation contained in Act No. 101/2000 Coll.).

It was usually applied in cases of publication of documents pursuant to Act No. 106/1999 Coll., on free access to information, without sufficient anonymisation. In such cases, if the breach was not particularly serious, the Office invited the responsible authority or body [to explain or remedy the state of affairs] pursuant to Section 54 (1)(b) of the Act on Personal Data Processing. In case of immediate remedy, the Office set the case aside by virtue of its resolution pursuant to Article 65 of the Act on Personal Data Processing. Otherwise, infraction proceedings were initiated against the responsible authority or body.

As a specific example of the application of the aforesaid provision of Section 65 of the Act on Personal Data Processing, we can describe the case of a complaint against publication of applications under Act No. 106/1999 Coll. that contained the applicant's personal data on the electronic official notice board of Újezd pod Troskami. Possible violation of the principle of purpose limitation set out in Art. 5 (1)(b) of the General Regulation was inferred from this submission as the municipality of Újezd pod Troskami had processed the applicant's personal data for a purpose other than for which it originally collected them. The Office sent to the municipality a request for remedy of the unlawful state of affairs, which was complied with by the municipality. Therefore, without initiating infraction proceedings, the Office set the case aside, because it was clear from the conduct of the suspect after the act was committed that the required goal consisting in immediate remedy of the discovered unlawful state of affairs had been attained.

In 2019, the Office most often dealt with violation of Art. 6 (1) of the General Regulation, including the corresponding Section 5 (2) of the previous legal rule, i.e. Act No. 101/2000 Coll. These provisions stipulate the duty to have a legal ground to process personal data.

Another most frequently violated provision was Art. 5 (1)(f) of the General Regulation, or, in proceedings that were still assessed under the previous legal rule, the corresponding provision of Section 13 of Act No. 101/2000 Coll., i.e. violation of the principle of "integrity and confidentiality". The principle consists in the obligation to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

It is also necessary to mention the frequent failure to facilitate the exercise of the data subjects' rights, as provided for in Articles 12 to 23 of the General Regulation.

Examples of the Decision - Making of the Office:

On the basis of files provided by the Police of the Czech Republic, the Office initiated a procedure to issue an administrative order against a natural person operating a business and decided on imposing a fine in the amount of CZK 54,000 due to violation of Art. 6 (1) of the General Regulation.

The party to the procedure committed the unlawful act by using, as a representative of a financial services provider and intermediary in executing contracts for another financial services provider, the following personal data of 18 persons with a view to filling in offers for execution of an insurance contract: name, surname, birth identification number, place of birth, permanent address, citizenship, occupation and payment details. The data subjects affected were unaware of this manner of use of their personal data. The party to the procedure obtained the said personal data for the purpose of arranging a part-time job and drafting the employment contract. However, the job was never actually arranged. Some of the insurance contracts were cancelled before the commencement of their performance, but a request for payment of the regular premium was delivered to several data subjects.

In view of the fact that these persons were not aware of negotiating the execution of an insurance contract, it was clear that the party to the proceedings did not have any legal grounds for processing their personal data.

Based on the file provided by the Czech Police, the Office initiated administrative proceedings against a limited liability company in which a fine of CZK 30,000 was imposed.

The Office found in the proceedings that when arranging loans, the company had not ensured safe keeping of personal data of approximately 300 clients including their name, surname, birth identification number, identity card number, address of residence, telephone number and information on the loan contained in the consumer loan agreements which were freely stored in a paper box in a shared garage of a residential building and subsequently found in a garbage can.

Personal data processing must always comply with the basic principles stipulated by Article 5 of the General Regulation. These principles represent the basic rules on which all processing procedures are based, as well as the most important principles applicable to the handling of personal data by controllers.

To comply with this principle, the controller must thoroughly consider all the risks associated with the personal data processing and take appropriate measures to exclude the risks to the maximum possible degree.

In the given case, the company failed to sufficiently consider the risks for the rights and freedoms of its clients and thus did not adopt appropriate security measures to protect them from unauthorised or unlawful processing and accidental loss, destruction or damage, as it left the box containing documents originating from its activities and containing the clients' personal data freely accessible in a residential building. It must have been clear that any of the residents of the building could have accessed and freely dispose of the data.

Based on an inspection carried out in 2019, the Office initiated a procedure to issue an administrative order and imposed a fine in the amount of CZK 15,000 on an online shop that violated Art. 15 (1) of GDPR, i.e. the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. Where that is the case, the data subject has the right to access to the personal data and the

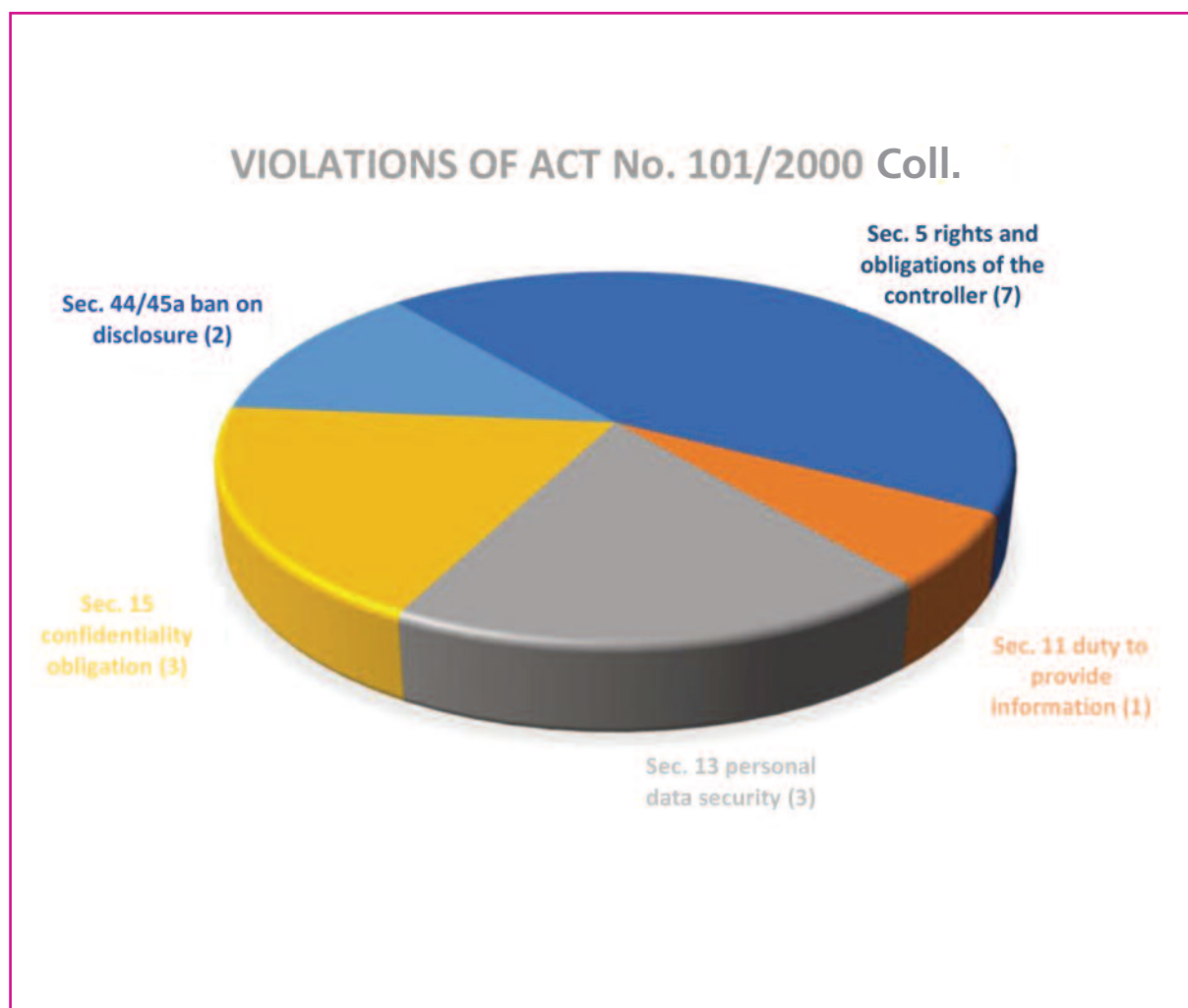
information set out in Art. 15 (1)(a) to (g) of the Regulation due to the controller's failure to provide to the client at request information on the client's personal data being processed.

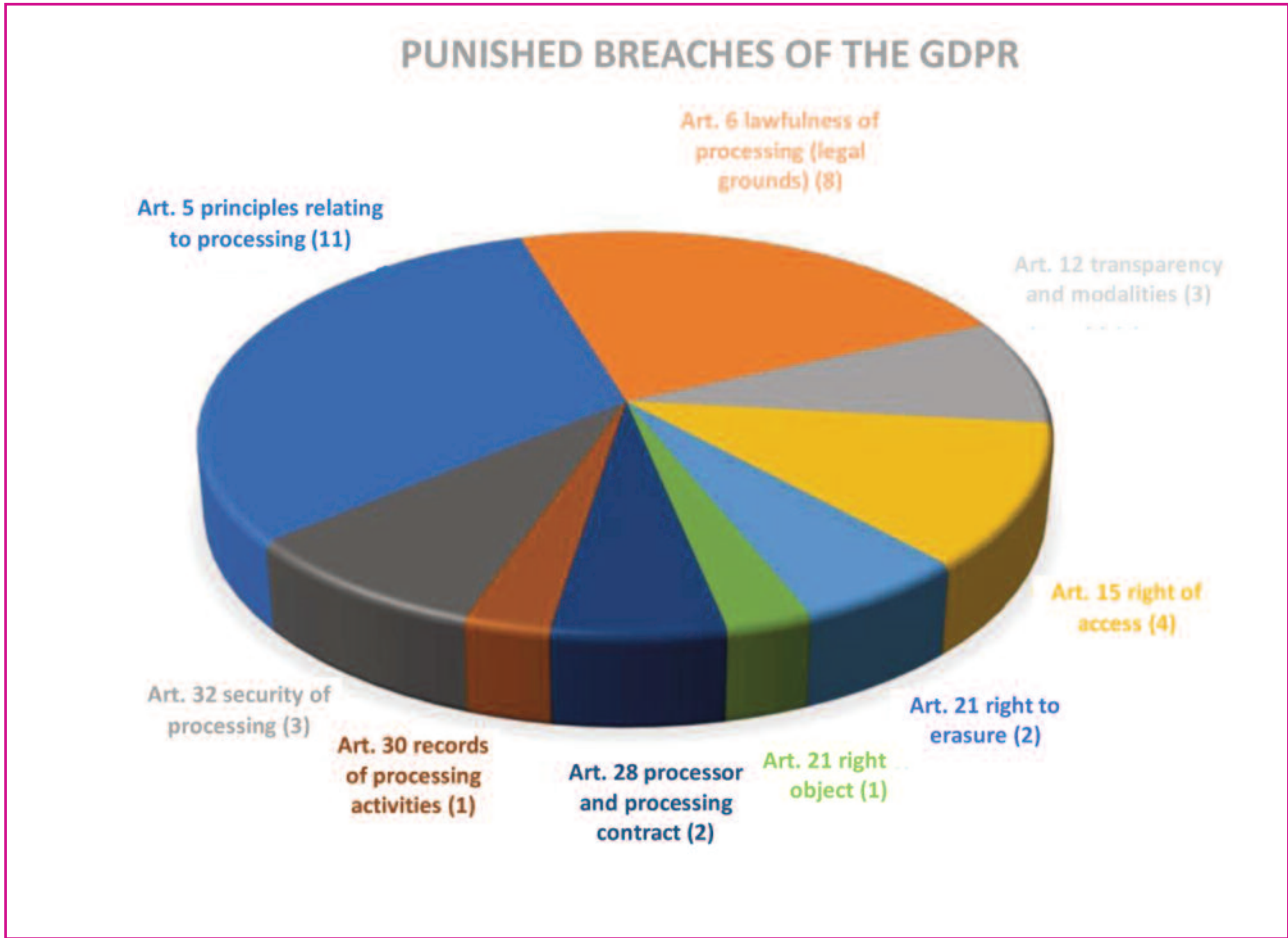
In 2019, the Office imposed fines amounting to nearly one million Czech crowns on a total of 32 entities for violation of Act No. 101/2000 Coll. and the General Regulation and/or the Act on Personal Data Processing.

In the year under scrutiny, the Office used the possibility of imposing an administrative penalty other than a fine in four cases that were not particularly serious; the penalty had the form of a reprimand.

Same as the previous legal rule, the Act on Personal Data Processing authorises the Office to punish breaches of the ban on disclosure, as distinct merits independent of violation of the General Regulation.

In 2019, the Office dealt with several dozens of such submissions. Proceedings were initiated in three cases, of which two cases were pursued under the previous legislation (Sections 44a and 45 of Act No. 101/2000 Coll.). Fines for breach of the ban on disclosure of personal data under some other legal regulation were imposed in two cases, one in the amount of CZK 140,000 on a legal person, and one in the amount of CZK 2,000 on a natural person.





• HANDLING OF COMPLAINTS PURSUANT TO SECTION 175 OF THE CODE OF ADMINISTRATIVE PROCEDURE

The Code of Administrative Procedure allows those who are not satisfied with the handling of their cases by administrative authorities, including the Office for Personal Data Protection, to lodge a complaint pursuant to Section 175 of the Code of Administrative Procedure.⁷ Specifically, the affected persons may lodge complaints with administrative authorities against inappropriate conduct of officials or against the procedure applied by an administrative authority. Complainants may also avail themselves of this option if the Code of Administrative Procedure does not provide them with other means of protection, i.e. especially appeals or other ordinary or extraordinary remedies.

In 2019, the Office dealt with a total of 30 complaints filed on the basis of Section 175 of Act No. 500/2004 Coll. In most cases, the complainants were dissatisfied with the manner in

⁷ Act No. 500/2004 Coll. of 24 June 2004, the Code of Administrative Procedure

which their previous submission concerning a possible violation of legal regulations in the area of personal data protection had been handled, especially when it was found unjustified and set aside without adopting any measures. In four cases, the complainants approached the Office with a complaint against inspection procedures.

Four of the 30 complaints were assessed as justified. In these cases, supervisory procedures were initiated to re-assess the complaint and, if appropriate, inspection or administrative proceedings conducted. Seven complaints received by the Office in 2019 will be brought forward to 2020.

In four cases, the complainants disagreed with an already completed assessment of their complaint and, therefore, turned to the President of the Office. In all these cases, the previous procedure of the Office was found justified and the complaints were dismissed as baseless.

Same as in previous years, none of the submissions received by the Office in 2019 addressed inappropriate conduct of public officials.

● FINDINGS FROM JUDICIAL REVIEWS

1. Prevention of bullying in schools is not grounds for unlawful interference in the privacy of minors

In its judgment Ref. No. 14 A 89/2017-47 of 11 March 2019, in proceedings on an action against the decision of the President of the Office of 5 October 2017, Ref. No. UOOU-04002/17-23, lodged by the town of Moravský Beroun, the Municipal Court in Prague dealt with the violation of privacy of fourth grade pupils, i.e. minors who enjoy increased protection of privacy.

In the case, the Municipal Assembly of Moravský Beroun processed the data of pupils who had been involved in bullying (as victim and bullies) including names and surnames, information on the attended school, including grade, and all information concerning the bullying contained in the output of psychological intervention (hereinafter the “psychological assessment”).

In the decision contested by the action, the Office for Personal Data Protection stated that the resolution of a complaint concerning bullying falls within the reserved competence of the Municipal Council. Therefore, the Assembly should have been provided with only general information about the fact that bullying of a pupil of the relevant school was being addressed and certain procedures triggered. Information on the manner of bullying and names and surnames of the pupils involved are data whose dissemination constitutes an especially serious interference with the private life of these pupils and which the Assembly does not need to know in order to be informed of the measures adopted.

In view of the principle of proportionality, the Office believes that protection of personal data of primary school pupils and prevention of unauthorised interference with their privacy in such a sensitive matter should have priority over the right to information.

In the reasoning of its judgement by virtue of which the action lodged by Moravský Beroun was dismissed, the Municipal Court in Prague stated, in particular, that protection of privacy and dignity is particularly necessary when providing information on minor children or similarly vulnerable persons. It follows from the above that courts and other public authorities (including the Office for Personal Data Protection) are obliged to pay increased attention to such

information and provide it with greater protection (see also the judgement of the Constitutional Court of 20 December 2016, File No. Pl. ÚS 3/14).

The Municipal Court in Prague added that minors (due to their yet incomplete intellectual and moral development) can be particularly harmed by breach of their privacy, i.e. that it could be more difficult for them to deal with a situation where their identification details are disclosed to an excessive degree. *"This applies especially if the information disclosed concerns particularly sensitive issues, which bullying undoubtedly is. First of all, it is a very delicate and negative issue from the viewpoint of the victim, but due to their age, even the bullies may comprehend the causes and consequences of their actions inadequately and, therefore, it is necessary to exert appropriate professional influence on them, rather than ostracising them (especially if they still attend lower grades of primary school)."*

The Municipal Court in Prague also heard a case concerning the powers of a municipal assembly as one of the municipal bodies, which are exhaustively listed in Section 84 of the Act on Municipalities, and the powers of a city council (which are exhaustively listed in Section 102 of the Act on Municipalities). It follows from these provisions that, except for the statutory exemptions, the council may not delegate its powers to any other body, nor may the assembly assume the statutory powers of the council. The court thus agreed with the Office when it stated that *"[...] it was not strictly necessary to inform the members of the assembly in detail on the occurrence of any problems, including the provision of the unanonymised psychological assessment, since it was not up to the members of the assembly to render a final decision in the case, and thus there was no fundamental reason why they would need to be acquainted with the problems that had occurred in the fourth grade of the primary school in such detail (including the names of the bullies and the victim)"*.

Consequently, there was no need to inform the members of the municipal assembly of bullying at the school operated by the town of Moravský Beroun in such detail on account of their office, as they were not competent to render any decisions in the matters at hand.

2. The level of security of data concerning health must correspond to their nature

In its judgment Ref. No. 8 A 55/2014-68, the Municipal Court in Prague dismissed the action filed by the hospital Lužická nemocnice a poliklinika, a.s., with its seat in Rumburk (hereinafter the "hospital") against the decision of the President of the Office of 24 January 2014, Ref. No. UOOU-06285/13-32.

By virtue of this decision, the President of the Office dismissed the appeal lodged by the hospital against the first-instance decision of the Office of 27 November 2013, Ref. No. UOOU-06285/13-27, whereby it imposed on the hospital a fine in the amount of CZK 120,000 for an administrative offence committed pursuant to Section 45 (1)(h) of Act No. 101/2000 Coll. The alleged offence consisted in failure by the hospital to take measures to ensure security of personal data processing in relation to maintaining medical records of its patients.

The administrative proceedings were based on an inspection by the Office, which took place in the hospital in connection with investigation of a complaint filed by a patient concerning loss of a part of her medical records containing sensitive data.

Within the inspection, personal data security pursuant to the requirements of Section 13 of Act No. 101/2000 Coll. was verified, and a breach of this provision was found in relation to maintaining medical records in both hard copy and electronic form.

Hard copies of medical records (over a thousand documents) from the obstetrics and gynaecology and surgical departments were stored in unsecured (non-lockable) cabinets. Errors in keeping medical records in electronic form consisted in failure to make electronic records that would allow for determining and verifying when, by whom and for what reason the personal data contained in the electronic medical records were perused, which is at variance with the duty stipulated in Section 13 (4)(c) of Act No. 101/2000 Coll.

In this respect, the Municipal Court in Prague concluded that the arguments related to ambiguity of the legislation alleged by the hospital were unfounded, and referred to the judgment of the Supreme Administrative Court of 10 May 2006, Ref. No. 3 As 21/2005-105. In the judgment, the Supreme Administrative Court commented on the statutory duty to adopt specific measures pursuant to Section 13 of Act No. 101/2000 Coll., as follows: “[...] *measures that the controller is obliged to take include technical, Supervisory activities/57 organisational, legal and other measures. [...] [T]he language used sets too high a standard in a way, as it leaves the manner and means of securing personal data at the controllers’ and processors’ own discretion, while it imposes high penalties for nonperformance of the given duty. However, the complainant’s arguments cannot be accepted since had there been any actual basis to them, it would ultimately result in inapplicability of Section 13 of the Act as a whole.*”

The Municipal Court in Prague further stated that data concerning health are sensitive data pursuant to Section 4(b) of Act No. 101/2000 Coll., and must be secured accordingly. Appropriate level of security corresponding to the risks following from the nature of the data was also required under Art. 17 (1) of Directive 95/46/EC.

As to the duty to make electronic records of perusal of data in the system (“logging”), the Municipal Court in Prague stated that a mere contract for securing updates of the hospital information system and the provider’s declaration that the system meets all the statutory requirements cannot release the Plaintiff from liability for the administrative offence, while pointing out that the Supreme Administrative Court reached this conclusion in its judgement of 26 December 2016, Ref. No. 3 As 121/2014-35. The judgment states, inter alia, that the duty to protect personal data is a “*public-law duty from which the controller or processor of personal data cannot be released by acting under private-law provisions (execution of a contract with another person)*”.

It was undisputed between the parties to the court proceedings that the perusal of medical records kept in electronic form had not been monitored, and the Plaintiff had not even subscribed to such a service (logging). In this respect, the court explained that Section 13 (4)(c) of Act No. 101/2000 Coll. is concerned with the protection of personal data in electronic form and requires that it be possible to determine and verify who processed the data subject to protection in any respect. It added that pursuant to Article 17 of Directive 95/46/EC, “[...] *the controller is obliged to protect personal data against accidental or unauthorised access. Such protection is ensured only if it is possible to determine who specifically perused the medical records. Without logging every case of mere perusing of the medical records, the requirements of the Directive cannot be met.*”

3. Operative part of a decision concerning breach of duties in personal data processing is sufficiently precise even if the number of entities is not precisely specified

Administrative Court dismissed as ungrounded the cassation complaint of the Construction Housing Cooperative Prague (hereinafter the “cooperative”) against judgment of the Municipal Court in Prague of 12 October 2017, file No. 11 A 83/2017-32, whereby the Supreme Administrative Court dismissed the action lodged by the cooperative against the decision of the President of the Office of 16 February 2017, Ref. No. UOOU-10704/16-15.

By virtue of its action lodged with the Municipal Court in Prague, the cooperative pleaded that the above-specified decision be annulled. The President of the Office dismissed the appeal lodged against the first-instance decision of the Office of 29 November 2016, Ref. No. UOOU-10704/16-8, whereby it imposed on the cooperative a fine in the amount of CZK 250,000 for four administrative offences committed pursuant to Section 45 (1)(c), (d), (f) and (h) of Act No. 101/2000 Coll. The cooperative committed the administrative offences in relation to processing of personal data of the owners, tenants, subtenants and spouses and other members of the household of the tenants of residential and non-residential units owned or managed by the cooperative.

In particular, the Supreme Administrative Court concurred with the statement of the Office, where the Office pointed out that the number of data subjects is extremely high and changes dynamically. According to the court, *“[i]t is clear that it would be disproportionately burdensome to request from the defendant precise specification of the number of data subjects concerned for the purposes of defining the conduct under assessment. This would, of course, be appropriate in situations where the offence concerns a single or several individual data subject(s) or where it is possible to determine a more exact number without exerting unreasonable efforts (e.g. if personal data are processed by automated means and are therefore exactly quantified). However, it can be generally expected that precisely in the sphere of supervision over compliance with regulations in the area of protection of personal data, which are usually subject to mass processing, it is common that the personal data concerned, data subjects and other circumstances are defined only generally with specification of a reasonable estimate of their number (and of course also their category).”* The cooperative considered defective the operative part of the Office’s decision in that each individual data subject was not specified. It must be pointed out that there were thousands of data subjects affected whose exact number was constantly changing and such a specification would not be feasible.

In this respect, the Supreme Administrative Court accepted the reasoning of the contested judgement of the Municipal Court in Prague. The judgement stated, inter alia, that *“[...] in respect of the deliberation on the gravity of the Plaintiff’s unlawful conduct, the court does not consider it necessary that ‘every single’ data subject affected by the Plaintiff’s conduct be exactly specified; an approximate determination of the number of data subjects – given the number of units managed or owned by the Plaintiff, whose exact number is specified in the operative part of the decision – is absolutely sufficient for considering the seriousness and scope of the unlawful conduct”*.

By contrast, what is important is that in its decision, the Office *“[...] defined the act in terms of substance and time, provided its legal qualification and, to the maximum extent possible while upholding the principle of procedural economy, specified the category of the data subjects affected by the offence and an indicative number of these data subjects”*.

The Supreme Administrative Court also dealt with the issue of possible application of the new legislation comprised in the GDPR to the liability of the Cooperative, which claimed impunity.

In this respect, the Supreme Administrative Court agreed with the Office, referring to resolution of the extended chamber Ref. No. 5 As 104/2013-46, according to which a new, more favourable legislation could be applied only in administrative proceedings or in proceedings held before a Regional Court.



Advisory and consultancy activities

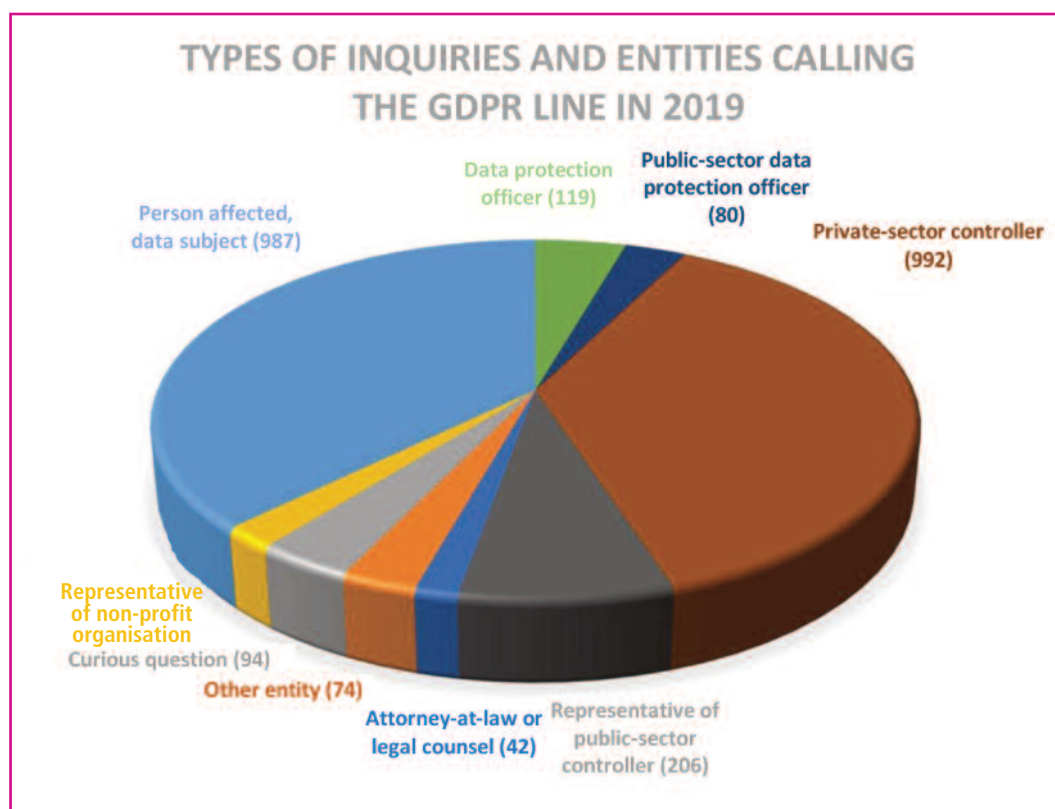
Also in the second year of effect of the General Regulation, the Office's consultation activities focused both on explaining new concepts introduced by the directly applicable Regulation, as well as the basic principles of personal data protection already valid for dozens of years, whose knowledge and awareness must be constantly deepened. This applies, in particular, to controllers who do not have lawyers at their disposal, let alone a data protection officer. Moreover, since 24 April 2019, the responses to inquiries and consultations were already provided with reference to the laws issued in connection with the GDPR and Directive 2016/680, which entered into effect in that year – Act No. 110/2019 Coll., on personal data processing, and Act No. 111/2019 Coll., amending certain laws in connection with the adoption of the Act on Personal Data Processing.

Answers to numerous inquiries, whose number was however not as large as in the year when the General Regulation entered into effect, were provided both in the form of written and telephone contact with the inquirer, or a personal interview during the visit of the inquirer in the Office's premises.

As regards the written form, a brief answer by e-mail was preferred for most of the inquiries, which is in accordance with the Office's mission to support public understanding of matters of personal data protection. More extensive legal analyses were provided in respect of requests concerning complex aspects of personal data processing.

In 2019, both the general and professional public commonly used the GDPR telephone line through which over 2,600 inquiries were answered. Many of the callers were data subjects to whom the staff provided information on how they could exercise the rights under the General Regulation. There was also a large number of persons responsible for processing at the controller, both in the private and public sectors. The employees of the information line also answered dozens of inquiries from data protection officers.

The telephone line was often used by data subjects who discussed potential breach of their rights in the area of personal data protection, as well as employees of controllers or processors inquiring about the manner of performance of any of the obligations under the GDPR.



Other types of inquiries were also encountered, such as questions from attorneys-at-law and trainee attorneys concerned with the merits of the matter concerning personal data processing they were dealing with.

The advantage of answering inquiries by telephone is not only expedience, but also the possibility to immediately respond to the inquirer’s additional questions, unlike in written communication, which is discontinuous. However, the inquirer must acknowledge that this type of fast consultancy can provide only general information on the problem at hand or the background for exercising the data subject’s rights in the given case.

Given the great interest of the public in the area of personal data processing through camera surveillance systems, a telephone line dedicated to answering questions in this area was also in operation.

Great many answers were available to the public in the section “*Frequently asked questions by areas of data processing*” at the Office’s website, which were regularly supplemented and updated in view of the developments in the field of personal data protection and, if appropriate, they replaced older opinions of the Office. This section, too, served for quick and effective provision of answers in case of some written questions.

Last year, the Office provided over twenty comprehensive personal consultations at request of controllers or processors from both the public and private sector. The central governmental authorities that availed themselves of this possibility included the Ministry of the Interior, the

Ministry of Finance, the Ministry of Justice, the Ministry of Industry and Trade, and also the Customs Administration and the Police of the Czech Republic.

In consultations provided to private-law entities, the issue of processing biometric data as special category of personal data pursuant to Article 9 of GDPR was repeatedly discussed; the wording of this provision introduced stricter conditions for processing of these data enabling or confirming unique identification of a natural person compared to the previous legal regulation in the already repealed Act No. 101/2000 Coll., on personal data protection. Questions regarding the use of dynamic biometric signature to confirm identification of a natural person entering into a contractual relationship were also common.

The Office also consulted the use of the facial recognition technology for identification of those who commit spectator violence in football stadiums with the view to preventing these persons from accessing the stadiums. Some countries (e.g. Denmark) embedded biometric identification of football spectators in their laws with a view to solving the long-term Europe-wide problem of spectator violence based on a law authorising the supervisory authority to permit such processing by a football club as a private-law entity on the grounds of substantial public interest, if the club provides for suitable and specific measures to safeguard personal data required by Art. 9 (2)(g) of the General Regulation. However, the Czech Act on Personal Data Processing does not grant to the Office any such authority and the required guarantees are not specified in the applicable Act No. 115/2001 Coll., on support for sports, either.

It was therefore recommended to wait for an amendment to the Act on Support for Sports being prepared by the Ministry of the Interior, which should also include data protection impact assessment under Art. 35 (2)(b) of the GDPR. Its objective must be to deal with important issues of protection of privacy, personal data and risks following from the use of facial recognition technology.

Another topic repeatedly encountered in the consultations was the relationship between the entities involved in personal data processing. Determination of whether such a relationship is:

- a relationship between two independent controllers, each of them determining the purpose and means of processing;
- a relationship between the controller and the processor carrying out personal data processing for the controller; or
- a relationship between joint controllers, who determine the purpose and means of processing jointly

often depends on the specific regulation of the specific relationships embedded e.g. in a contract concluded between these entities.

However, it can be stated in general that if the purpose of processing is determined for the controller by law, e.g. in case of medical facilities or banks, and such an entity processes personal data for another purpose following from the law for another entity, the former need not be in the position of a processor, but it can, even in such a situation, be in the position of a controller or joint controller. In such a case, the contract between these entities need not contain all the requisites of contract with the processor required by Article 28 of the GDPR.

The Office also consulted a wide range of inquiries concerning education, local governments, private-law relationships and other areas closely tied with personal data processing.

In 2019, the Office for Personal Data Protection received no request that would, in terms of contents or nature, form a request for prior consultation pursuant to Article 36 of the General

Regulation. Such a consultation should be requested by the personal data controller if it concludes that the data protection impact assessment under Article 35 of the General Regulation indicates that the processing would result in a high risk, despite having adopted measures to mitigate this risk. However, as follows from this provision, this is an extreme case of high-risk processing, which is expected to occur especially in processing usually carried out using new technologies that have not yet been proven to be safe.

In 2019, the Office held four seminars for data protection officers following up on the preceding year's seminars, where the June seminar was also devoted to the above-mentioned new national legislation on personal data protection and administrative punishment. The Office also obtained information on the activities of the data protection officers at the individual controllers by means of a questionnaire survey.

The capacity of the Office's meeting hall has always been fully utilised, and the December Small-scale Controllers Day attended by representatives and owners of small and medium-sized companies who are not obliged to appoint a data protection officer was no exception.

In cooperation with the regional data protection officers, two more seminars were held in Pardubice and Karlovy Vary for officers in the Pardubice and Karlovy Vary regions.

Employees of the Consultation Unit also participated in the preparation of contributions to the personal data protection manual for mayors issued by the Union of Towns and Municipalities. It contains short, practical and comprehensible recommendations as to how to proceed in handling personal data in various activities carried out by the municipality, e.g. in congratulating citizens celebrating an important jubilee and welcoming newborn citizens, entering data in municipal chronicles and processing personal data of applicants for assignment of a municipal flat.

• LEGISLATION

On 24 April 2019, Act No. 110/2019 Coll., on personal data processing, and accompanying Act No. 111/2019 Coll. entered into force. They implemented the EU legislation on personal data protection in the Czech laws. The EU legislation includes:

1. GDPR;
2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by 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;
3. Directive (EU) 2016/681 of the European Parliament and of the Council (EU) 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

None of the above-mentioned Czech laws introduced fundamental deviations from the General Regulation. What changed substantially was the breakdown of the existing unified regulation of personal data protection into the following segments:

1. general, governed by the GDPR, whether directly or on the basis of Section 4 (2) and exemptions in Sections 5 to 15 of the Act on Personal Data Processing
2. public policy (Sections 24 to 42 of the Act on Personal Data Processing)
3. national security (Sections 43 to 49 of the Act on Personal Data Processing)

Personal data processing in the area of public policy and national security is governed exclusively by the Act on Personal Data Processing, and based on a decision of the national legislator, the General Regulation applies to neither of the two segments, not even subsidiarily.

The second fundamental change consists in non-systematic exclusion of the entire public sector from the criminal-law competences of the Office. In practice, the Office found that data protection officers are lacking in the public sector, and, even when they are appointed, they are often bypassed when matters concerning personal data protection are dealt with. This leads to the fact that the conceptual aids of the supreme administrative authorities for regulated entities do not always provide instructions concerning practical issues or offer incorrect solutions. These aids are also rarely fully up-to-date, failing to reflect the rapid development of EU personal data protection legislation (cf. the new opinions of the Board).⁸

The third regulation differing from the existing ones consists in the new rules for personal data processing for the purpose of scientific or historical research, statistical purposes, journalistic purposes or for the purposes of academic, artistic or literary expression contained in Articles 16 to 23 of the Act on Personal Data Processing. The Office considers it necessary for the regulators to prepare conceptual aids on how to apply the new legislation in practice.

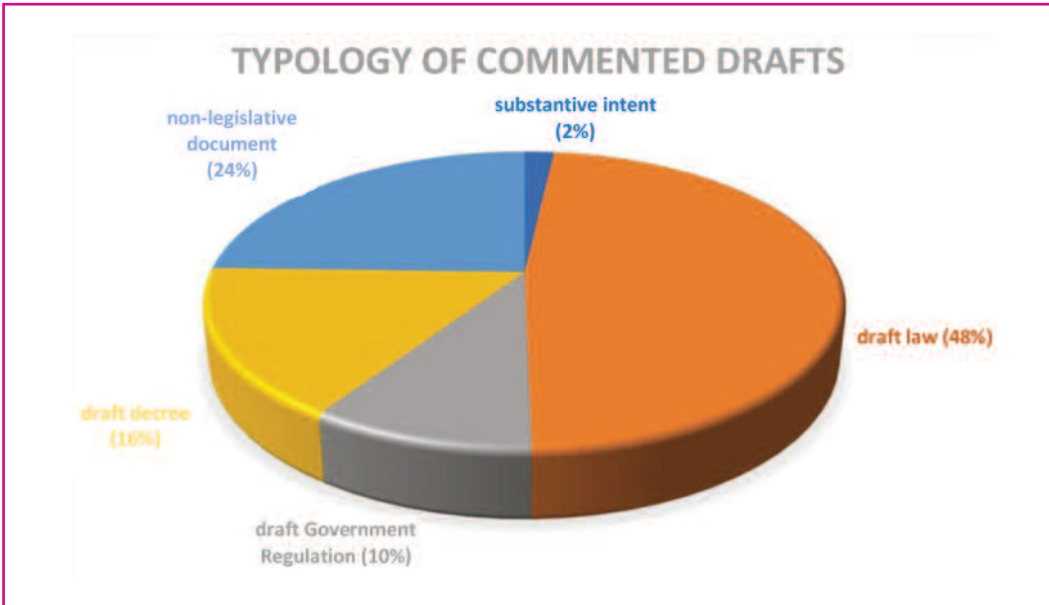
The Office insisted that Section 1 of the Act on Personal Data Processing maintain that personal data protection forms part of broader protection of privacy and that Section 7 sets the age limit for a child's capacity to grant consent to personal data processing at 15 years.

It failed to push forward the provision that the GDPR be applicable subsidiarily for all personal data processing and the previous regulation of punishment in the public sector remain effective. Neither did it manage to improve the relationship between the Office and the judiciary system to ensure that incorrect court decisions concerning personal data need not be remedied only by the Constitutional Court, as was the case of salaries of public officials in the case of *Law in public interest v. Zlín* of 17 October 2017, File No. IV ÚS 1378/16.

The Office accepted the long-term efforts of part of the professional public to entrust it with competences in the area of free access to information. However, due to the absence of transitory provisions in the substandard legislation approved by the Parliament (where the Parliament passed the draft law on personal data processing in the wording proposed by the Senate, while the accompanying law was passed in the wording proposed by the Chamber of Deputies), this legislation will cause extreme difficulties to the Office.

The Office attempted to remedy the situation by convincing the Chamber of Deputies to pass an amending motion; however, these efforts were jointly opposed by the Ministry of the Interior and the Senate. Consequently, there is a risk that the Office will be overburdened by new caseload, which could result in exceeding the statutory deadlines for rendering a decision.

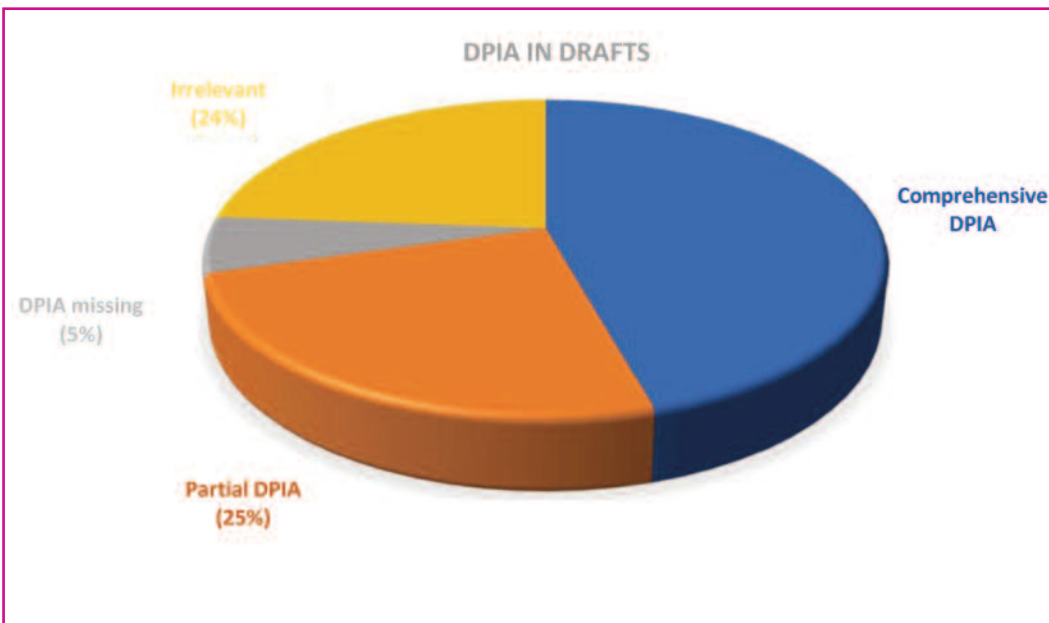
⁸ https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en



Evaluation of impacts of the proposed solution in terms of protection of privacy and personal data

The Office continued to strive to improve the quality of legislative assessment of the impacts of the proposed solution in relation to protection of privacy and personal data (DPIA) in order to meet the requirements of Article 35 of the General Regulation. These efforts have newly found a basis in Section 10 of the Act on Personal Data Processing, according to which the controller need not carry out assessment of the impact of data processing on personal data protection prior to commencement of personal data processing if it is required to carry out such processing under a legal regulation.

It is therefore necessary that the legislative DPIA also include evaluation of high-risk matters related to personal data processing together with evaluation of mechanisms used to reduce or completely eliminate them.



Cooperation with the Chamber of Deputies and the Senate

Pursuant to Section 54 (3) of the Act on Personal Data Processing, some of the political groups formed by the Deputies informally discussed the proposed amendments with the Office, which is very beneficial for the protection of privacy in the Czech Republic. For example, the Office stated that comparing the central debt enforcement records with the Insolvency Register was inappropriate due to different purpose of personal data processing. The Office considers the concept of the Insolvency Register freely providing information without structuring and classification of life roles and the necessary data to be unsatisfactory, of which it advised the Ministry of Justice already in 2012.

Private law

The Ministry of Justice has prepared a draft amendment to the new Civil Code concerning transposition of the Directive on certain aspects concerning contracts for the supply of digital content and digital services. The draft also includes the controversial *alinea* 2 in Article 3 (1) on monetisation of personal data.

The Office continues to discuss with the legislator how this provision of EU law should be best transposed into the Czech legislation so as to ensure highest possible protection of personal data as a human right under the Charter of Fundamental Rights of the EU.

The Ministry of Labour and Social Affairs submitted a draft amendment to the new Labour Code, which, however, neglected the regulation of biometrics. At the same time, employers often base the processing of certain biometric data of employees for the purposes of controlling entry, presence and access on the employees' consent. However, such use of consent in the relationship between the employer and the employee is unacceptable in view of the provisions of the General Regulation. The Ministry of Labour and Social Affairs did not accept the Office's comments due to narrow focus of the draft amendment. However, it agreed with the Office that it would work on regulating biometrics.

The Ministry of Health has prepared a draft law on electronic health care and secure sharing of data among health care services providers (the Act on Electronic Health Care, "eHealth"), which has been the biggest change in the area of health care in recent years. The Office will continue to discuss its formulation with the legislator.

Public Law

The 2021 census of population, buildings and apartments will have a fundamental impact on privacy. In discussing the draft articulated wording of the related law, the Office followed up on cooperation with the Czech Statistical Office in preparation of its draft substantive intent. It succeeded in interlocking the authorisation to collect data with the purpose of their processing. The Office believes that this census will create conditions for a fully "administrative" census in 2031, i.e. without filling in questionnaires.

The Ministry of Defence submitted to the Government a draft amendment to the Act on Military Intelligence. To strengthen the protection of privacy, the Office managed to push forward a proposal for establishing an inspector for cyber defence directly subordinated to the Minister, similar to a data protection officer. Another guarantee should be provided by the decision on the obligation to establish and secure an interface for connection of detection tools at a set point in the public communication network and the obligation to tolerate the placement and operation of these tools.

Moreover, the Office reached an agreement with the Ministry of Justice on an amendment to the draft legislation regulating the publication of beneficial owners of shares in companies so as to better protect their privacy.

Privacy in electronic communications

The draft regulation on respect for private life and personal data protection in electronic communications has not advanced to the stage of Council General Approach even after months of discussions during the Finnish presidency. The Office pointed out, in particular, the lack of link between the authorisation for the national regulation and the difficulties associated with breach of confidentiality of communication in order to combat child pornography and terrorism.

● ANALYTICAL ACTIVITIES

In 2019, the Analytics Unit continued to participate in the tasks and activities of the Office that required a detailed analysis and search for systemic solutions compliant with the purpose, principles and requirements of the General Regulation.

The European data protection landscape, where the Office currently performs its activities, is rapidly developing, and if necessary, the changes are unified by the European Data Protection Board (hereinafter the “Board”).⁹ *Vis-à-vis* the public, these developments take the form of guidelines, opinions and recommendations concerning the individual matters or issues.¹⁰

The Board’s materials reflect the complexity of the topic and significantly contribute to improving the know-how in the area of personal data protection. At the same time, its outputs are focused on practice and intended primarily for the obliged entities, especially controllers/processors. The Analytics Unit also participates in the preparation of materials for the Board.

It should be pointed out that although the Czech Republic now has a comprehensive framework for personal data protection thanks to the adoption of the Act on Personal Data Processing, this does not mean that all aspects of personal data protection in the individual areas or activities involving data processing have been completely resolved to everyone’s satisfaction.

From the viewpoint of the General Regulation, it can be noted that the individual areas are going through gradual cultivation at an unequal rate. The Office is aware of this fact and keeps adapting its activities to the actual state of affairs, with the view to contributing to gradual improvement of the state of personal data protection in the Czech Republic.

The interconnection between the Office’s activities and the development of personal data protection in the EU is undeniable in this respect. As an independent supervisory body, the Office is not here only to perform supervision, but also to provide advice and help set up the environment in accordance with personal data protection principles.

⁹ Pursuant to Article 68 of the General Regulation, the European Data Protection Board is a body of the European Union with legal personality. The Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. The Board is represented by its Chair.

¹⁰ https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

1. BIOMETRICS

Biometrics was one of the areas to which the Office paid systematic attention in 2019 in terms of designing future solutions conforming to the requirements of the General Regulation. This is caused by the fact that in recent years, there has been an increase in the use of biometric devices by private entities, often without the controller having considered personal data protection requirements or dealing with these requirements only formally. This includes e.g. the use of dynamic biometric signature by banks and insurance companies, in delivery of goods and conclusion of contracts by large vendors.

However, it should be noted that before acquiring such equipment, the relevant controller should first consider certain questions. In particular, it should clearly examine what exactly are biometric personal data, what are the associated risks, whether their use in the specific situation for which they are intended is possible and appropriate, what legal grounds for processing may be taken into account and what technical and organisational measures must be introduced. It must also provide advice to persons whose personal data will be processed, ideally based on its own initiative within an active duty to provide information, or in relation to other rights of data subjects under Chapter III of the General Regulation.

Below, we provide some examples of issues in the area of biometrics that should be of interest to controllers/processors and data subjects:

What are biometric personal data, how and where are they defined?

Biometric data can be defined as information on biological properties, physiological characteristics and features of an individual or repetitive actions where these characteristics and/or actions are measurable and unique for the given individual, even if the samples used are subject to a certain margin of error. Typical examples of such biometric data include fingerprints, facial features, voice, as well as hand geometry, vein samples or some deep-rooted behaviour patterns or other characteristics (e.g. handwritten signature, the manner of typing, a distinctive gait or manner of speaking, etc.).

A definition of biometric data is also provided in Art. 4 (14) of the General Regulation and reads as follows: *“biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”*.

Biometric data have long been considered personal data. However, it remains disputable whether they are “sensitive data”.¹¹ The General Regulation resolved this problem when it included them among special categories of personal data, i.e. such data that are, by their nature, particularly sensitive and merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms of individuals. The General Regulation contains tools for the protection of biometric data that controllers are obliged to use. In particular, it should be pointed out that biometric data are usually subject to data protection impact assessment.¹²

¹¹ WP Opinion 3/2012 on developments in biometric technologies of 27 April 2012.

¹² Article 35 of the General Regulation and Recital 91 of the General Regulation.

What are the risks associated with the use of biometric personal data? What are the advantages and disadvantages of biometric systems?

As regards the impact on personal data protection and privacy, biometric systems have not yet been subject to systematic professional examination or public discussion in the Czech Republic. Similar to other technologies, they were put to use prior to resolution of the relevant legal and ethical consequences.

In general, it can be stated that biometric data are associated with advantages as well as disadvantages. The main advantages of the use of biometrics include effective proof of the real identity of users, comfort for the relevant natural person who thus cannot forget or lose the identifier or password, as well as the fact that it is very difficult to forge or falsify such personal data.

However, biometric systems are also connected with numerous negatives, which need not be obvious at first sight. The risks posed by biometric systems follow from their nature.

Firstly, they cannot guarantee full accuracy; there is always a risk of incorrect identification, i.e. the possibility of baseless denial. In general, their primary risk lies in the fact that they are based on the relationship between one's body and identity, allowing "machine-readability" and further use of physical characteristics of the human body.

Potential risks include the possibility of covert collection, storage and processing of data, as well as collection of materials containing sensitive information, which could interfere with the individual's private sphere. Leakage of biometric data can affect the rights and freedoms of natural persons, e.g. human dignity, privacy and the right to data protection. This applies especially to vulnerable persons, such as children, the elderly and persons who are unable to provide all the required data for some reason.

How to proceed when using biometric data?

When an entity begins considering the use of biometric devices, it is always necessary to first consider whether the situation really requires the use of biometric technologies and processing of biometric data. Such considerations are especially appropriate if the processing concerns any of the groups considered vulnerable by the General Regulation, e.g. children and employees. If the use of personal data it is not necessary, some other alternative must be used. The frequently used justification that the use of biometric data is comfortable for the customers, as they need not remember any credentials, does not suffice.

It should also be noted that biometric technologies, despite their growing availability (both in terms of technology and finance), do not fully replace other security solutions and do not ensure greater security in themselves. From this point of view, it is always preferable to consider a combination of various security measures. The higher the planned level of security, the smaller the potential of the biometric data to achieve such a goal – precisely due to the above-specified risks associated with them, i.e. due to the fact that they are not 100% reliable.

As stated above, biometric data are newly classified as a special category of personal data whose handling is subject to stricter requirements. This is based on the assumption that they are of a sensitive nature and, therefore, their handling entails risks. Thus, they require more sensitive handling than other personal data. The processing of such data is prohibited by Art. 9 (1) of the General Regulation, unless some of the exceptions specified in paragraph 2 of the same Article applies.

As regards the approach to the processing of biometric data as such, it holds in general that now that the GDPR is in effect, it is always necessary to ensure and check compliance with its requirements. Firstly, it is always necessary to assess conformity with the general data protection principles. They are set out in Art. 5 of the General Regulation, and include, in particular, lawfulness, fairness and transparency, as well as purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability of the controller. Application of technical and organisational measures is also envisaged in this respect.

At the same time, none of the measures in the area of personal data protection are set in stone, and must be updated as necessary.

Most frequent risks associated with the use of biometric personal data Nejčastější rizika uváděná ve spojitosti s používáním biometrických osobních údajů

- Biometric technologies cannot guarantee full accuracy; there is always a risk of incorrect identification.
- There is a risk of discrimination of persons who are “rejected” by the system or unable to provide biometric data for any reason (e.g. handicapped persons).
- Identity theft based on the use of falsified or stolen sources of biometric data may result in serious damage.
- Unlike with other identification systems, an individual cannot be provided with new identification data if the existing ones are compromised.
- Some biometric data may reveal information on physiology that the affected individual did not intend to provide.
- Many biometric technologies enable automatic monitoring of persons or creation of their profiles.
- Biometric technologies, despite their growing availability (both in terms of technology and finance), do not fully replace other security solutions and do not ensure greater security in themselves. The higher the planned level of security, the smaller the potential of the biometric data to achieve such a goal.
- Biometric systems often contain more information than necessary for matching purposes, which increases the risks associated with their processing.

2. CAMERA SURVEILLANCE

Another issue with which the Analytics Unit dealt is camera surveillance. This is due to the increased frequency of use of camera surveillance systems by both private entities and public bodies in recent years, while the rapid development of camera equipment and increase in its availability were faster than the development of the associated legal regulations.

This area is covered by the General Regulation and is also dealt with by the Guidelines of the Board concerning video surveillance, whose final wording incorporated inputs from the public debate. Although not generally binding, the Guidelines are an important interpretation tool; they are formulated in such a way as to be comprehensible to the maximum possible extent and provide clear instructions to their addressees (controllers, processors, data subjects).

The Board’s Guidelines state that the use of cameras has a far-reaching impact on the protection of privacy and personal data. This has led to an ongoing discussion within the EU and individual Member States aimed at setting the conditions and limitations concerning the

installation of camera surveillance equipment as well as adopting the necessary measures for the protection of data subjects. In this respect, it was necessary to balance several competing rights. Justifiably or not, the public considers security camera surveillance to be one of the most effective methods of crime prevention. The cameras' purpose is to discourage potential violations of privacy and, if such a violation has already occurred, obtain evidence for the purposes of administrative, criminal or infraction proceedings. On the other hand, camera surveillance seriously invades privacy and interferes with personal data protection and it is necessary to clearly determine its limits.

The current legislation in the area of camera surveillance in the Czech Republic,¹³ its principles and setting of the associated technical and organisational measures are governed especially by the General Regulation. The Board's Guidelines concerning camera surveillance can be used as a suitable practical foundation for application of specific rules.

The Office considers the Guidelines, in the formulation of which it was involved¹⁴, an important tool that will help overall cultivation of the environment in the Czech Republic where cameras are often used excessively, and often also at variance with the legal regulations. However, similar to other technologies whose use is currently rapidly expanding, there must be limits to the use of video surveillance. The right to privacy and protection of personal data of natural persons forms the imaginary boundary and criterion for establishing whether and when the interests or fundamental rights and freedoms of data subjects take precedence. As regards cameras, their registration in the Czech Republic was terminated after Act No. 101/2000 Coll. had been repealed.

In view of the fact that there is no special law dealing with cameras in the Czech Republic, camera surveillance is subject only to the provisions of the Civil Code and the General Regulation. There is no clear boundary between the scope of application of the two regulations, but in principle, they should supplement one another. While camera surveillance could not have been punished before the effect of the GDPR due to the fact that there was no special law regulating cameras in the Czech Republic, the General Regulation now enables application of general principles in this area.

Although some pieces of regulation in this respect had actually existed, they had not been applied. The GDPR then brought certain changes to the use of cameras. Similarly to processing of other personal data, it holds in processing of personal data by means of camera surveillance that the controller is fully liable for the surveillance it performs. Controllers are obliged to proceed pursuant to the provisions of the GDPR and its principles, including transparency, fairness and lawfulness of processing, purpose limitation, minimisation of stored data, their accuracy and updating, limitation of the duration of processing for the necessary period of time and integrity of the processing.

The controller is subject to the obligations laid down in Chapter IV of the General Regulation if it can be reasonably required to perform them. With the exception of processing in the course of a household activity, which permits processing of personal data on the owner's private premises, the controller is not authorised to monitor public spaces. Any exemptions from this

¹³ There are special laws in force in some countries.

¹⁴ Not all of the Office's proposals were implemented.

prohibition, as follows from the case-law of the CJ EU in the case of *Ryneš*¹⁵ and the related case-law of the Supreme Administrative Court¹⁶, are very narrow and must always be assessed individually. Naturally, the controller is obliged to not only assert, but also prove, all the circumstances related to the camera surveillance performed by the controller. This is also related to the fact that the controller is obliged to keep and submit records of personal data processing unless it falls under the exemption for household purposes mentioned above.

As regards the experience of the supervisory authority in the area of camera surveillance, the most frequent complaints raised by citizens concern unauthorised surveillance. The Office usually evaluates the situation and its seriousness. In some cases, it sends an information letter to the owner of the camera surveillance system and informs the owner of the legislation and the associated duties, if appropriate. This is often the only intervention necessary. The information letter is also important because it provides the person affected by surveillance with evidence that s/he can use in case of litigation.

If the case develops further, the Office applies individualised procedure depending on the competences under the law (concerning personal data, not privacy), severity of the matter and the evidence provided. In some cases, the Office proceeds in cooperation with other authorities, e.g. municipalities. The use of supervisory and corrective powers is limited to a certain degree by the fact that since the Office usually cannot verify the actual state of affairs and the facts of the case on site, it can rely only on the (mutually contradictory) statements of the parties to the procedure. This is because the legislation does not allow the Office to enter a home and land of a private individual;¹⁷ this is only possible in case of an entrepreneur's home.

Nonetheless, the Office does not abandon its role in the area of camera surveillance. In connection with publication of new instructions for camera surveillance, it will also inform the public from time to time of any changes.

¹⁷ Section 7 of Act No. 255/2012 Coll., on inspection (the Inspection Rules).

International cooperation

• CODES OF CONDUCT

Codes of conduct serve as voluntary accountability tools stipulating specific rules for personal data protection, i.e. a set of norms for behaviour in a sector that are best from the legal and ethical point of view. Similar to personal data protection certification, such codes of conduct belong among the tools that help controllers and processors achieve compliance with the General Regulation.

In June 2019, the Board approved the document titled Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, which provided for the contents of the codes of conduct, the approval (including criteria) thereof and requirements for accreditation of bodies entrusted with the monitoring of codes of conduct.

At the end of the year, the individual countries were invited to submit accreditation criteria for codes of conduct. The Office submitted the accreditation requirements to the Board in November. Subsequently, discussions were held on their final form.

Due to certain ambiguities in the approach to the issue and requirements of the *Compliance, eGovernment and Health* Expert Subgroup, it will be necessary to modify the text and re-submit it next year.

• PERSONAL DATA PROTECTION CERTIFICATION

Issuance of a Personal Data Protection Certificate is one of the tools for the controller or processor of personal data through which they can demonstrate compliance of the processing carried out by them with the General Data Protection Regulation.

Pursuant to Section 15 of Act No. 110/2019 Coll., on personal data processing, the responsibility for accreditation has been bestowed on the Czech Accreditation Institute, which is the national accreditation body. However, this is not to say that the Office has no competence in this area. Primarily, it remains the responsibility of the Office to create requirements for accreditation of certification bodies and criteria for issuing certificates.

In December 2017, the Office published the criteria for issuing certificates (including requirements for accreditation and certification criteria) which were subject to a public debate in early 2018.

In June 2019, the European Data Protection Board (hereinafter the "Board") approved a document titled Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), whose Annex 1 modified the accreditation requirements for certification bodies.

Subsequently, in July 2019, the Office provided to the Board's *Compliance, eGovernment and Health* Expert Subgroup the document Criteria for the issuance of certificates, and in October of the same year, the Office officially submitted the criteria for assessment to ensure compliance within the consistency mechanism. Currently, discussions are held on their final form.

Filing an application for a certificate pursuant to the General Regulation is up to a voluntary decision by the controller or processor aimed at demonstrating compliance with the General Regulation, rather than a new duty. Until the Board approves the accreditation requirements and certification criteria, filing of applications for accreditation or certification with the Office is not possible.

At the present time, the Board's Expert Subgroups are evaluating the accreditation requirements and discussing whether the accreditation requirements, as well as certification criteria, should be individualised for specific areas of personal data processing and/or specific products and services, or whether they could be of general nature.

• DATA PROTECTION IMPACT ASSESSMENT (DPIA)

In 2018, the Office submitted to the Board a list of the kind of personal data processing operations which are subject to data protection impact assessment. The final version of this document was finally adopted in January 2019.

Office also submitted to the Board a list of personal data processing operations which are not subject to data protection impact assessment. After its approval (recently, the Board's comments were incorporated and a new version of the material submitted), both lists will be consolidated into a single document. This document will be published at the Office's website in early 2020.

To facilitate controllers' activities, the Office has also prepared and published the Guidance for General Data Protection Impact Assessment for public discussion. Submission of comments and suggestions was concluded on 15 December 2019. Publication of the amended version is expected in the first quarter of 2020.

● TRANSFER OF PERSONAL DATA ABROAD

In 2019, the Office issued one authorisation for the transfer of personal data to third countries that do not guarantee an adequate level of data protection pursuant to Art. 46 (3) of the General Regulation. Specifically, this authorisation was issued to the Czech National Bank, which submitted to the Office for approval an administrative arrangement for transfer of personal data between the financial supervision authorities in the European Economic Area and the financial supervision authorities outside the European Economic Area.

The aforementioned administrative arrangement was jointly drawn up by the European Securities and Markets Authority (ESMA) and the International Organization of Securities Commissions (IOSCO). This took place in close cooperation with the Board's International Transfers Expert Subgroup, with which the authors have been consulting the wording of the administrative arrangement in the long term.

By means of an official letter, ESMA and IOSCO submitted the final wording of the aforementioned administrative arrangement to the Chair of the Board, who subsequently asked the Board for an opinion pursuant to Art. 64 (2) of the General Regulation. On the basis of this request, the Board drew up opinion No. 4/2019 of 12 February 2019, where it stated that the submitted administrative arrangement would ensure appropriate safeguards for the transfers of personal data. The transfers shall take place on the basis of this administrative arrangement within the meaning of Art. 46 (1) and (3)(b) of the General Regulation.

The Office could thus base its decision on the said opinion of the Board, where it concluded that in the case at hand, the Czech personal data protection legislation did not require any further guarantees and no other facts suggesting specific risks for the Czech Republic were known. For this reason, it authorised the use of the above administrative arrangement as an instrument providing for and setting appropriate safeguards for the transfers of personal data to third countries or to international organisations pursuant to Art. 46 (1) and (3)(b) of the General Regulation.

The establishment of the above administrative arrangement and the approval procedure applied are, to a large extent, precedents and model examples of the preparation of other non-binding "administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights" pursuant to Art. 46 (3)(b) of the General Regulation.

The above-described example of the development of administrative arrangements clearly showed that the remaining authorisation powers of the Office are significantly dependent on the opinions of the Board.

As a result of the effects of the General Regulation, the core of the Office's activities in the area of transfers of personal data to third countries thus shifted from its own independent interpretation and decision-making activities to cooperation with the Board, especially with the International Transfers Expert Subgroup.

Within the International Transfers Expert Subgroup, the Office actively participated in the preparation of a document aimed at clarifying the relationship between application of Art. 3 and Chapter V of the General Regulation. The document should explain the conditions under which controllers and processors in third countries who are directly subject to the GDPR may process personal data transmitted or transferred from the European Union.

At the same time, the document should include the fundamental matter of the definition of transfer of personal data to a third country. However, in view of the different backgrounds of the individual national delegations, reaching consensus requires plenty of effort and time, so the work on the document will be completed in the following period.

In the position of co-author, the Office also participated in the preparation of Board's Opinion No. 16/2019 of 12 November 2019 on the draft decision of the Belgian Supervisory Authority regarding the Binding Corporate Rules of ExxonMobil Corporation. Together with the Board's Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc., these were the very first two opinions within the procedure of approval of binding corporate rules under the General Regulation.

The favourable Opinion of the Board issued in accordance with Art. 64 (1)(f) of the General Regulation, is in fact the final step in the approval of the binding corporate rules. Such an opinion is to be supplemented only by the opinion of the head of the lead supervisory authority by which the specific binding corporate rules are finally approved, and no other authorisation procedure by other supervisory authorities takes place.

It should be noted in this respect that several dozens of draft binding corporate rules are currently awaiting discussion within the International Transfers Expert Subgroup and the opinion of the Board.

Issuance of the Board's opinion is preceded by several phases of evaluation of the specific draft binding corporate rules conducted by the lead supervisory authority and one or two supervisory authorities as co-evaluators (see WP263 Working Document Setting Forth a Cooperation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the General Regulation). In 2019, the Office, as the co-evaluator, commented on revised draft binding corporate rules within three approval procedures.

In addition to working on specific draft administrative arrangements and binding corporate rules, preparation of the annual joint evaluation of the American privacy shield and other tasks, the International Transfers Expert Subgroup focused on formulating more general interpretation materials. Most of these will be finished next year.

In addition to the above-mentioned document on accord between Article 3 and Chapter V of the General Regulation, the Subgroup is currently finalising

- Guidelines for transfers of personal data between public bodies [Art. 46 (2)(a) and (3)(b) of the General Regulation];
- guidelines on codes of conduct and certification as tools for the transfer of personal data to third countries [Art. 46 (2)(e) and (f) of the General Regulation].

Another task awaiting the Commission and the Subgroup next year is to review all thirteen Commission decisions on adequate level of personal data protection under Article 45 (3) of the General Regulation, The decisions concerned were adopted under the system laid down by Directive 95/46/EC.

● SCHENGEN COOPERATION

Processing of personal data by extensive European information systems is an important part of Schengen cooperation in the areas of freedom, security and law. Protection of personal data processed in these information systems requires special attention, and corresponding legislative changes are indispensable.

The relevant systems include:

- Second generation Schengen Information System (SIS II);
- Visa Information System (VIS);
- fingerprint database Eurodac;
- Customs Information System (CIS).

The Office and other national supervisory authorities acting within the scope of their respective competences cooperate with the European Data Protection Supervisor (EDPS) and, with a view to coordinated supervision over information systems, they meet at least twice a year within coordination groups related to these systems – SIS II SCG, VIS SCG, Eurodac SCG, CIS SCG.

In addition to representatives of the supervisory authorities and EDPS, the meetings are regularly attended by representatives of the European Commission, together with the European Data Protection Officer of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA). They inform the representatives of the Member States present of the current situation, legislative developments and the relevant statistics with regard to the individual systems.

Within its competence in connection with the Schengen cooperation, the Office fulfils the role of the national supervisory authority, which supervises compliance with the applicable regulations and further contributes to the protection of the fundamental rights of persons whose personal data are being processed within the Schengen Area. Moreover, an authorised representative of the Office regularly participates in meetings of the above-mentioned coordination groups, where the Office shares with other Member States its experience from supervision. For the purposes of this cooperation, the Europol Cooperation Board was established and has been operating since 2017.

In addition to supervision and inspection related to the fulfilment of the requirements for legal processing of personal data by the controller within the above-mentioned information systems, the Office also dealt in 2019 with transformation of the existing model of coordinated supervision pursuant to the new Regulation (EU) 2018/1725 of the European Parliament and of the Council. This model should be fully supervised by the European Data Protection Board by 2021 at the latest.¹⁸

Number of submissions, complaints and inquiries and manner of their handling

The Office's duties also include processing of data subjects' submissions concerning the processing of their personal data in SIS II. In 2019, the Office received a total of 58

¹⁸ REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (specifically Art. 62).

submissions concerning personal data processing in SIS II; in 26 cases, the Office reviewed personal data processing by the Czech Police. In most cases, the complaints were concerned with a suspicion of breach of the statutory deadline for informing applicants for access to personal data processed in SIS II. In two cases, the Office participated in cross-border cooperation with other supervisory authorities.

Furthermore, the Office received a total of 13 submissions in which the petitioners inquired about the Czech Republic's visa policy or the course of processing of their visa applications. Since these matters do not fall within the Office's competences stipulated by law, the individual applicants were referred to the Ministry of Foreign Affairs and the relevant embassies abroad. In this respect, the Office has regularly clarified the competences entrusted to it by the Act on Personal Data Processing, as well as the EU legal regulations.

The Office's statistics concerning the increase in the number of submissions concerning SIS II clearly show an increasing trend in the number of requests for access to personal data in SIS II, where the number of such submissions increased by more than 100% compared to 2018 (especially from citizens of the former Soviet Union). On the other hand, there was a slight decrease in submissions relating to visa policy of the Czech Republic and issuance of visas.

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. These include:

- Schengen Information System;
- visa policy, police cooperation;
- external borders;
- returns;
- 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 usually includes a visit to the police departments that provide for operation of the national component of the Schengen database, the data protection authority, and other affected institutions, as well as other on-site investigations.

In 2019, the Czech Republic was evaluated along with four other states. The week-long evaluation mission brought valuable recommendations to the Office, which were subsequently implemented into practice or included in the plan of inspections to be carried out by the Office in 2020.

In 2019, an employee of the Office took part in an evaluation mission in Hungary as a national expert (October 2019).

● INTERNATIONAL ACTIVITIES

Based on the Office's competences, its international activities took place on several levels:

- within inspections (investigation of cases involving a foreign element);
- within the matters of data transfers abroad;
- last but not least, on the grounds of membership in the Board.

This section deals primarily with the involvement of the Office in the structures of the European Union and activities in the Board, while the matters belonging to the first two levels are dealt with in the preceding chapters.

The Board was established by the General Regulation. Its members include, in particular, the heads of the supervisory authorities of each Member State. National supervisory authorities thus have the opportunity to directly participate in the activities of the Board in various forms, especially in the creation of specialised materials.

With the exception of August, the members of the Board meet at the plenary session in Brussels once a month.

In addition, activities are continuously performed by several Expert Subgroups to which the data protection authorities may appoint their permanent delegates or participate in their activities by submitting written comments. These specialised thematic groups meet as required and regularly communicate within their own electronic platform:

- Key Provisions Expert Subgroup
- International Transfers Expert Subgroup
- Technology Expert Subgroup
- Cooperation Expert Subgroup
- Borders, Travel & Law Enforcement Expert Subgroup
- Compliance, e-Government and Health Expert Subgroup
- Financial Matters Expert Subgroup
- Enforcement Expert Subgroup
- IT Users Expert Subgroup
- Social Media Expert Subgroup

Each of the subgroups works on the basis of an activity plan approved by the plenary session. Most often, their activities result in creation of materials in the form of guidelines or opinions. These documents are drawn up by research teams created within the Expert Subgroups on a voluntary basis. In the year under scrutiny, the delegates of the Office participated in the creation of documents as members of a research team nine times. This included preparation of the following materials, of which the first two were already approved and published:

- Opinion concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (Art. 70.1.b))
- Guidelines on the territorial scope of the GDPR (Article 3)
- Draft opinion on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment
- Draft guidelines on processing of personal data through video devices
- Draft guidelines on the rights of data subjects – under preparation (preparation agreed in September 2019)

- Draft guidelines for personal data monetisation
- Draft document explaining the mutual relationship between Article 3 and Chapter V of the General Regulation
- Analysis of lists of the kinds of processing operations not subject to data protection impact assessment (Art. 35 (5) of the General Regulation) submitted by some national authorities as part of the consistency mechanism and preparation of the Board's opinions on these lists
- Analysis of binding corporate rules submitted by the ExxonMobil Corporation and preparation of the Board's opinion

The Office also participates in the activities of the Consultative Committee (T-PD) to the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and sends its delegate to regular plenary sessions twice a year. In the year under evaluation, the Committee dealt e.g. with artificial intelligence and examination of the impacts of this phenomenon on the privacy of an individual and the aspects of including data protection in school syllabi.

Employees of the Office participate in selected, mostly regularly organised, conferences and seminars. The most important of them are the European Conference of data protection authorities of EU Member States and the International Conference of Data Protection and Privacy Commissioners (ICDPPC, newly GPA), which provides the opportunity to meet and share findings with data protection authorities from other continents. Each of these events takes place once a year.

Other events worth mentioning include bi-annual seminar organised by the European Commission on the exchange of experience from supervisory practice (Case Handling Workshop) and meetings of the International Working Group on Data Protection in Telecommunications, which is one of the working groups at ICDPPC (newly GPA).

Free access to information

- **PREPARATION FOR PERFORMANCE OF NEW COMPETENCE OF THE OFFICE PURSUANT TO ACT NO. 106/1999 COLL., ON FREE ACCESS TO INFORMATION**

On 24 April 2019, Act No. 111/2019 Coll., amending certain laws in connection with the adoption of the Act on Personal Data Processing, was published in the Collection of Laws. This introduced, inter alia, an amendment to Act No. 106/1999 Coll., on free access to information, as amended (hereinafter the "Information Act"), stipulating new competence of the Office in the area of the right to information with effect from 2 January 2020. As from that date, the Office will be competent to handle submissions and conduct review proceedings and will become the appellate body for those obliged entities in respect of which a superior authority pursuant to Act No. 500/2004 Coll., the Code of Administrative Procedure, cannot be determined, and will also provide protection against inactivity of superior authorities.

The Information Act introduces for the first time the possibility to conduct review proceedings concerning a decision on both types of appeal under Czech law (in Czech: *odvolání* and *rozklad*). The competence to assess submissions to initiate review proceedings and conduct review proceedings in all



cases falls within the competence of the Office. The petitioner for information whose application was rejected by the obliged entity, or whose appeal was dismissed, will be able to turn to the Office with a submission requiring review of the decision. The use of this instrument is exclusively up to the applicant for information and it shall in no way prejudice his/her right to challenge the given decision by means of a court action.

Furthermore, the Office has the competence of a superior body for the obliged entities where the appeal or complaint have so far been dealt with by their heads. Appointment of superior authority pursuant to the Information Act is possible only in respect of obliged entities in respect of which a superior authority cannot be determined pursuant to Section 178 of Act No. 500/2004 Coll., the Code of Administrative Procedure. Typically, these are companies 100% owned by the State, Free access to information/82

regions, cities and municipalities, but also other entities. The number of the thus-defined obliged entities for which the Office will perform the role of superior authority cannot be determined. Its competence will have to be determined on a case-by case basis.

The Office will also address submissions and requests for protection against inactivity of superior bodies of obliged entities in proceedings on appeals and handling of complaints. The Office is also competent to enforce compliance with information orders issued by the Office as the superior authority or within the review proceedings.

In view of the adoption of the aforementioned amendment to the law, preparations were commenced to ensure that the Office will be able to perform the new competence in the area of right to information shortly after its publication in the Collection of Laws. As for the review proceedings, it was necessary, in particular, to assess the potential number of new submissions, as this will be a completely new task for the Office. Based on statistical data for selected obliged entities, a basic estimate of the volume of this new work was determined. The Office also preliminarily established for what obliged entities it would be a superior authority. However, a binding assessment in this respect can only be made after the effective date of the adopted changes.

The new competence was supplemented to the legal regulations on the basis of an amending motion during the discussion in the Chamber of Deputies of Parliament and it was therefore necessary to determine the financial requirements of the Office for its performance, especially to increase the personnel capacity and propose a corresponding change in the systemisation. Since November 2019, a new Right To Information Unit has been providing for matters concerning right to information.

Some applicants for information have already been making submissions to the Office since June 2019. In addition, the Office received requests for opinion as to whether or not it will be their superior body from a number of obliged entities.

Although the said changes have been effective only since January 2020, the Office thus commenced work in the entrusted matters already in the second half of 2019.

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

In the area of provision of information pursuant to Act No. 106/1999 Coll., on free access to information, the effect of the General Regulation fully developed in 2019. Although it had already entered into effect in 2018, it began significantly affecting the Office's workload concerning free access to information only in 2019. This was due to the fact that most requests for information were made in order to obtain information from the Office's supervisory activities in relation to the General Regulation. This fact thus affected both the contents of the applications and their number compared to previous years.

In terms of contents, the applicants of all age and professional groups were interested especially in general statistical information on the supervisory activities of the Office in relation to the General Regulation, i.e. how many fines were imposed, in what amount, for breach of which provisions, and how many cases of personal data breach were reported.

Other information requested by the applicants included, for example, the amount of the budget, provision of organisational or work rules, annual reports in hard copy, information on whether and in how many cases the Office dealt with recourse pursuant to Act No. 82/1998 Coll., on liability for damage caused in the exercise of public authority by a decision or incorrect official procedure.

The increased interest of the public in the supervisory activities of the Office, or rather its specific results in relation to the General Regulation, also led to an increased number of applications concerned with the provision of inspection records or decisions of the Office. There was also increased interest in inspection protocols and decisions of the Office within supervisory activities in the area of sending of commercial communications pursuant to Act No. 480/2004 Coll., on certain services of the information society.


These outputs from the inspection and decision-making activities of the Office were provided to the applicants, but without information whose provision is excluded under Act No. 106/1999 Coll., such as personal data (e.g. of the complainants), as well as information falling under Section 11 (2) and (3) of Act No. 106/1999 Coll., specifically information on the manner of securing personal data by the inspected entities or other important information obtained by the Office from the inspected entity.

In accordance with Section 17 of Act No. 106/1999 Coll., compensation of costs of extraordinarily extensive search, including the necessary exclusion of information from the provided documents, was required of three applicants who requested the provision of a large number of inspection records or decisions or provision of other information requiring extraordinarily extensive search. The relevant costs were paid in all three cases, amounting to CZK 4,950 in total.

Compared to 2018, when the Office received 56 applications, it dealt with a total of 90 applications in 2019.

Of which:

- the required information was provided to the full extent in 63 cases;
- the Office partially refused to provide the required information in 24 cases;
- the Office refused to provide the required information completely in 3 cases.



ORG information system in the system of basic registers

Since 2012, the Office has been operating the ORG information system as part of the system of basic registers and since 2018 as part of the critical information infrastructure of the State and part of the e-government of the Czech Republic. This is a separate competence and its implementation is separated from other agendas in the Office's internal organisation.

The basic registers are unique sources of the data most frequently used in the performance of public administration. They provide high-quality, up-to-date and verified data that are effectively used in public administration. Basic registers collect and store basic information on natural persons, legal persons, natural persons operating a business, addresses and public authorities. The ORG information system connects the individual registers and keeps a list of agendas that can use the system. For the purposes of basic registers, the Office creates source identifiers of natural persons and agenda identifiers of natural persons and provides for the transfer of the agenda identifier of a natural person within the agenda to the agenda identifier of that natural person in some other agenda.

The operation of the system itself, still provided for by the TESCO SW a.s. system integrator, did not experience any communication failures or data outages in 2019. At the end of 2019, 427 agendas were registered in the system. In all, 91-100 source identifiers were newly generated in 2019.

The ORG IS has always been operated on the same infrastructure. 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, not only with regard to the development plans of the system of basic registries. The operation of the system is strongly dependent on communication lines suppliers.

The necessary operation and development of the system is conditional on the following: annual 20% increase in basic register load through 2021, 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 and ensuring cyber security.

At recommendation of the Administration of Basic Registers, the ORG IS is certified according to CSN/ISO 27001:2014.

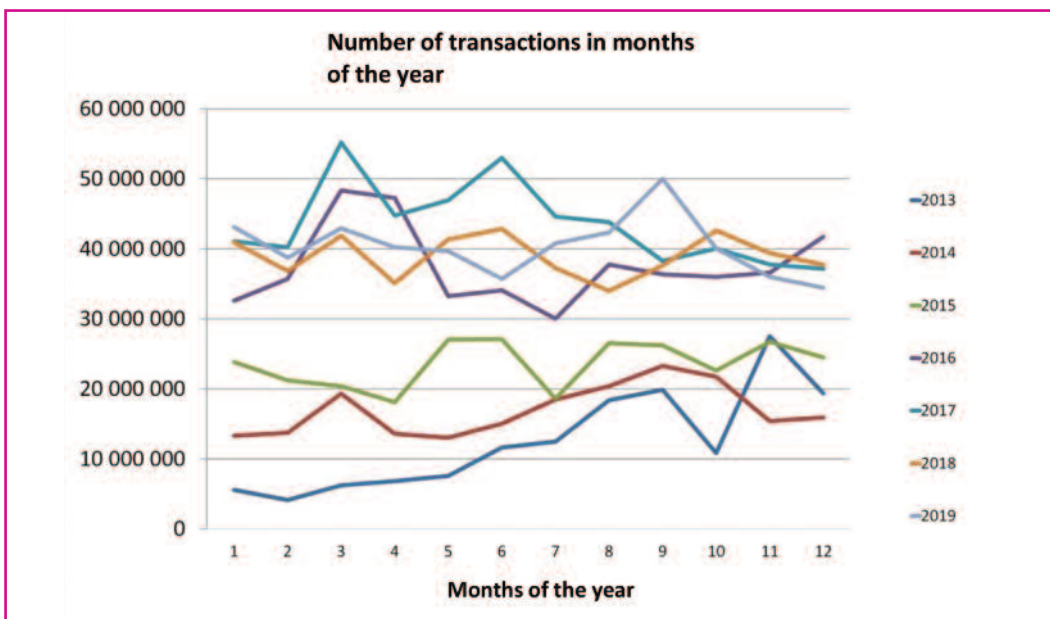
In December 2019, it was re-certified for another three years without any reservations. This year, the ORG IS was also inspected by the National Cyber and Information Security Agency. This inspection, as well as an internal audit, were also concluded without reservations. The inspection concerned e.g. the guidelines for managing access to data centres, operating rules, security policies, risks and assets register, recovery plan, etc. The security documentation required by the Cyber Security Act was updated.

Tools for monitoring access to the system for security purposes were newly set up and adjusted in 2019. These tools report and register probable and actual cyber attacks on the ORG IS.

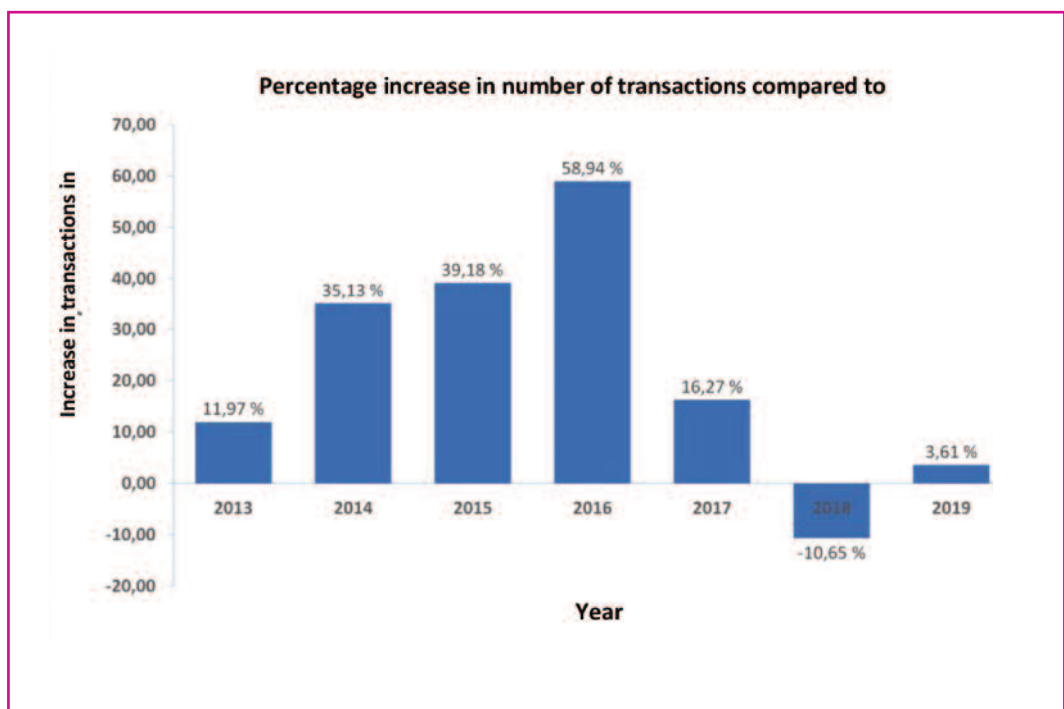
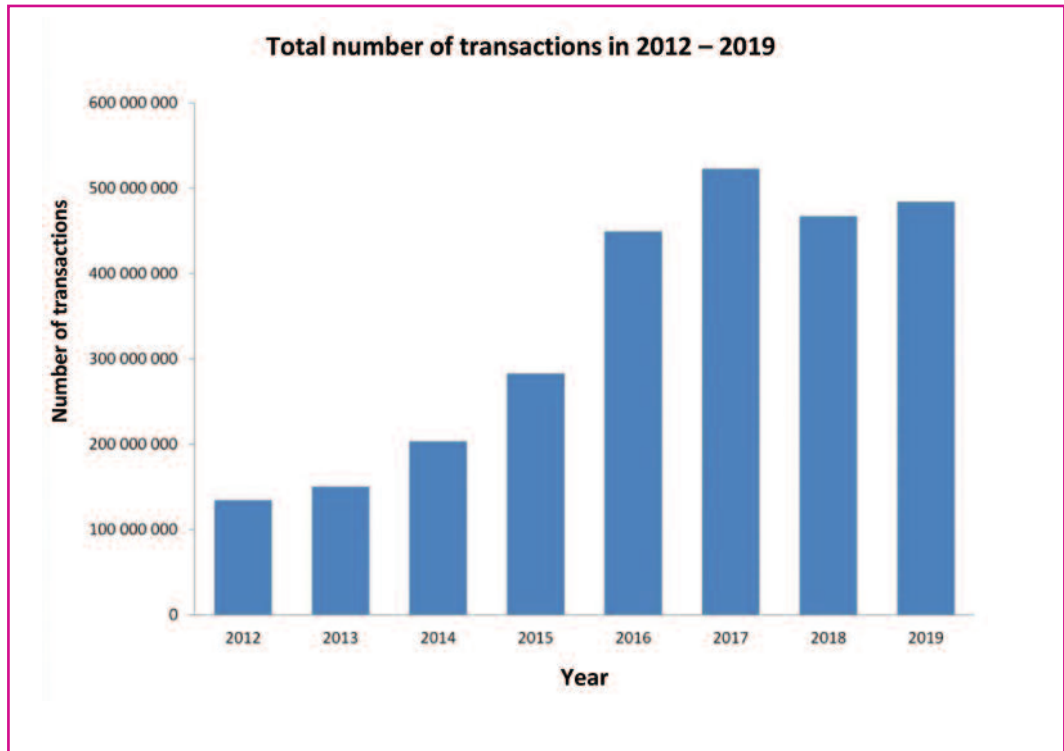
In contrast to previous years, when the maximum load was recorded in the spring months of March and April, the peak month in 2019 was September. This year's daily maximum load on the ORG IS was 2,155,924 transactions on 4 September 2019. In contrast, the daily minimum of 140,869 transactions was recorded on 6 September 2019. The monthly maximum of 50,023,694 transactions was recorded in September and the monthly minimum of 35,000,469 transactions in November. In comparison with the previous year, the number of transactions dropped by 3.98%.

V This is a decrease by 18,607,059 transactions in absolute numbers.

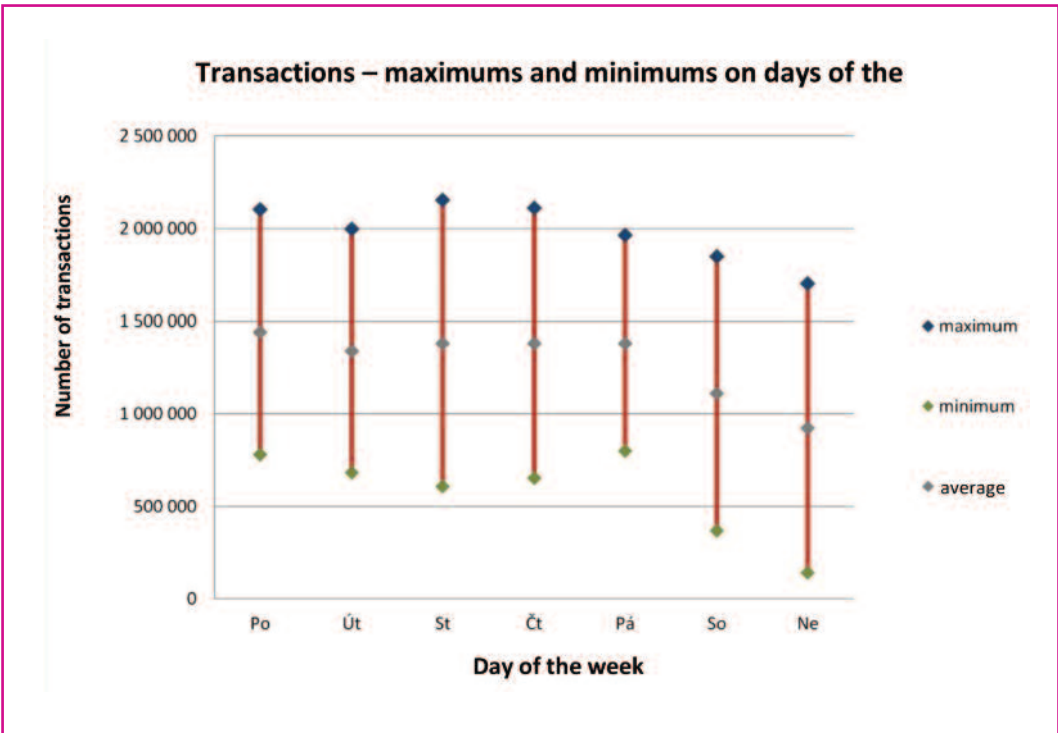
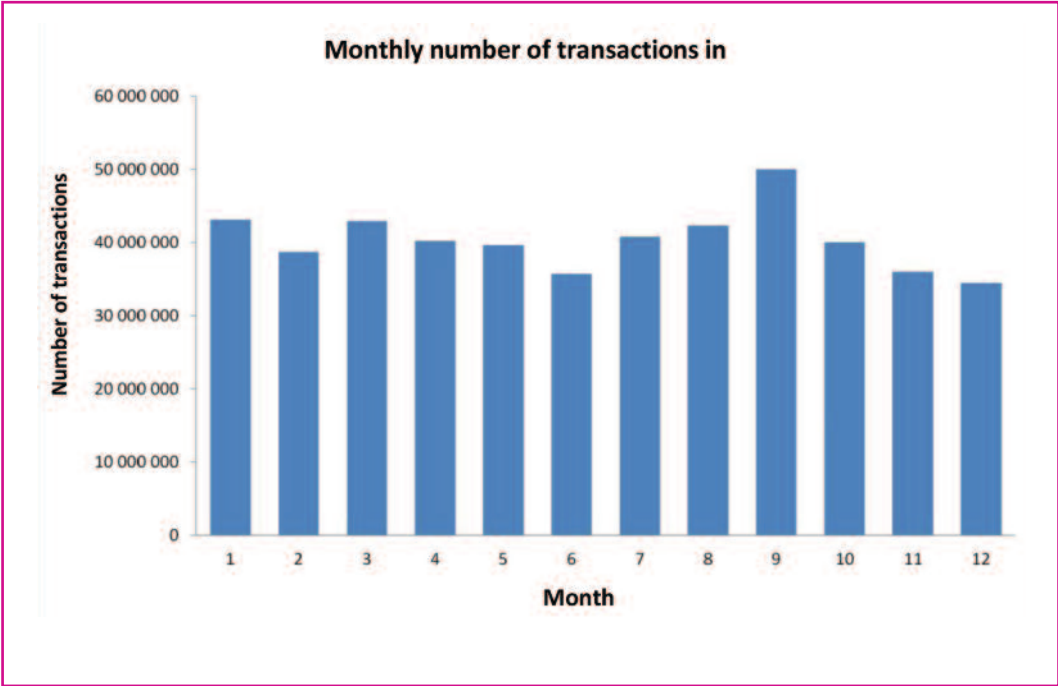
Same as every year, we provide an overview of the usage of the ORG information system; inter-annual comparison is provided for selected parameters.



The use of the ORG IS is apparent from the graph "Total number of transactions in 2012 – 2019";



Changes in the number of transactions compared to previous years in percent are shown in the previous graph "Percentage increase in number of transactions compared to previous year". The distribution of requirements on the system of basic registers during the year is shown in the graph "Monthly number of transactions in 2019".





Media and communication tools

From the perspective of media, the year 2019 saw an anniversary (one year from the effect of the General Regulation), as well as new events (effect of the new Czech personal data protection legislation).¹⁹ Important matters in terms of media coverage also included leakage of data from large internet entities and security breaches in the form of cyber attacks.²⁰

Other issues that were of interest to journalists in 2019 included the operation of cameras and camera surveillance systems, telemarketing, inspections by the Office, cookies, shared transport, biometric data, unsolicited commercial communications and publication of data on the internet in general. The Office also had to respond frequently to inquiries concerning zero administrative punishment for public authorities and public entities, even in cases of violation of the law.

Same as in previous years, the Office promoted the international Data Privacy Day and also joined the celebrations of the Safer Internet Day to promote safe internet. The Office also traditionally acknowledges the importance of the Czech Secondary School Competition on Cybersecurity aimed at checking students' knowledge and skills in cybernetics. For this reason, the Office once again supported the 2019 rendition, both in terms of expertise and in material terms.

2019 was also no exception in terms of awareness raising. The Office has prepared events for both the general and professional public with a view to

¹⁹ Act No. 110/2019 Coll. of 12 March 2019, on personal data processing, which has replaced the now-ineffective Act No. 101/2000 Coll., on personal data protection.

²⁰ Illegal attacks by IT experts. They penetrate systems without authorisation, usually through malicious software, in order to gain access to internal data. Cyber attacks often come in the form of flooding the system with superfluous page requests.

increasing awareness about data protection. Seminars aimed at sharing practical findings by data protection officers were especially popular. Five such meetings were held in the Office's premises last year.

The Office also continued publishing its own unofficial translations of materials of the European Data Protection Board. It also focused on providing consultancy through all available communication channels.

MEDIA IMAGE

From the viewpoint of media, the Office did not receive any negative publicity in 2019. However, journalists became increasingly interested in the amounts of fines imposed in relation to the General Regulation. The Office therefore needed to emphasise that fines for violation of the General Regulation are supposed to discourage continued violations, but not to threaten the existence of the fined entity, which was reflected in the amount of the fines imposed during the year.

LIBRARY

From the viewpoint of media, the Office did not receive any negative publicity in 2019. However, In 2019, the Office's library grew by 90 new publications, four of which were donated. In most cases, these materials were necessary for everyday work of the Office's employees. In addition, the Office continued its efforts to make the library a "temple of knowledge" with respect to personal data protection. Therefore, all publications published in the Czech Republic in the relevant year concerning data protection were acquired. The Office also purchased some specialised books published abroad (e.g. *Post-Reform Personal Data Protection in the EU; Privacy, Data Protection and Cybersecurity in Europe; The EU GDPR General Data Protection Regulation: Answers to the Most Frequently Asked Questions, and Internet of Things Security and Data Protection*).

In 2019, the Office granted all requests for visits to the library and lending of books by the public with only one exception caused by incompatibility of the request with the fact that the library offers to the public only on-site loans of documents based on prior agreement. In the remaining cases, the users visited the library and obtained the necessary information for their work or study. In some cases, the library services were also used by persons interested in passing the official civil servant examination in field 60 – Personal Data Protection.

Two theses, one Doctoral and one Bachelor's, were donated to the library. The Bachelor's thesis was awarded the title of best 2019 Bachelor's thesis within the ESOP 2019 competition (Excellent Students' Professional Work), announced by the Prague University of Economics and Business.

At the end of 2019, the Office's library had almost 2,600 volumes. The list of professional publications on personal data protection and related topics is permanently available on the Office's website.

WEBSITE

The website remains the primary communication channel used by the Office to publish information intended for the general public, including the youth. The website is also subject to continuous updates and gradual changes in its structure with a view to offering clearly arranged and quickly available up-to-date information. While the section GDPR (General Regulation) remained on the top of the menu, the Office focused on the development of the related Consultation section, where the public can find a number of valuable information and practical advice for dealing with everyday life situations.

At the end of the year, a new section “Right to Information” describing the new competence of the Office following from the amendment to the Act on Free Access to Information was included.

Operation of the Office

● PERSONNEL

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

The total number of systemised positions as of 1 January 2019 was 109. As of the last day of 2019, the number was 115.

Thus, in 2019, the fluctuation of employees increased from 9% to 11.8% in comparison with the preceding year.

The Office's HR processes continued to run smoothly in connection with the development of the Civil Service Act and other relevant legislative changes. Based on a resolution of the Senate of Parliament of the Czech Republic, Mgr. Josef Prokeš was appointed to discharge the newly established position of Vice-Chairman of the Office.

With effect from 1 October 2019, five new systemised positions were opened at the Office as part of the preparation for the discharge of new competences following from Act No. 106/1999 Coll., on free access to information, from 2020.

"Service evaluation" of the civil servants assigned to serve at the Office took place in early 2019. Twenty-eight civil servants were evaluated as excellent and thirty as good. No public servant was evaluated as unsatisfactory.

Eight new public servants were newly hired and nine employees terminated the service relationship. Three civil servants were assigned or appointed to another civil service office. Employment relationship was commenced with two new employees and terminated with three existing employees.

A total of 35 candidates took part in a special part of the civil service examination for the service specialisation "personal data protection" arranged by the Office; 31 of them passed the test successfully and four failed.

As of 1 January 2019, there were 101 employees “kept in records” (for statistical purposes) in the Office for Personal Data Protection, and that number was the same as of 31 December 2019.

The average recalculated number of employees kept in records in 2019 was 102.636.

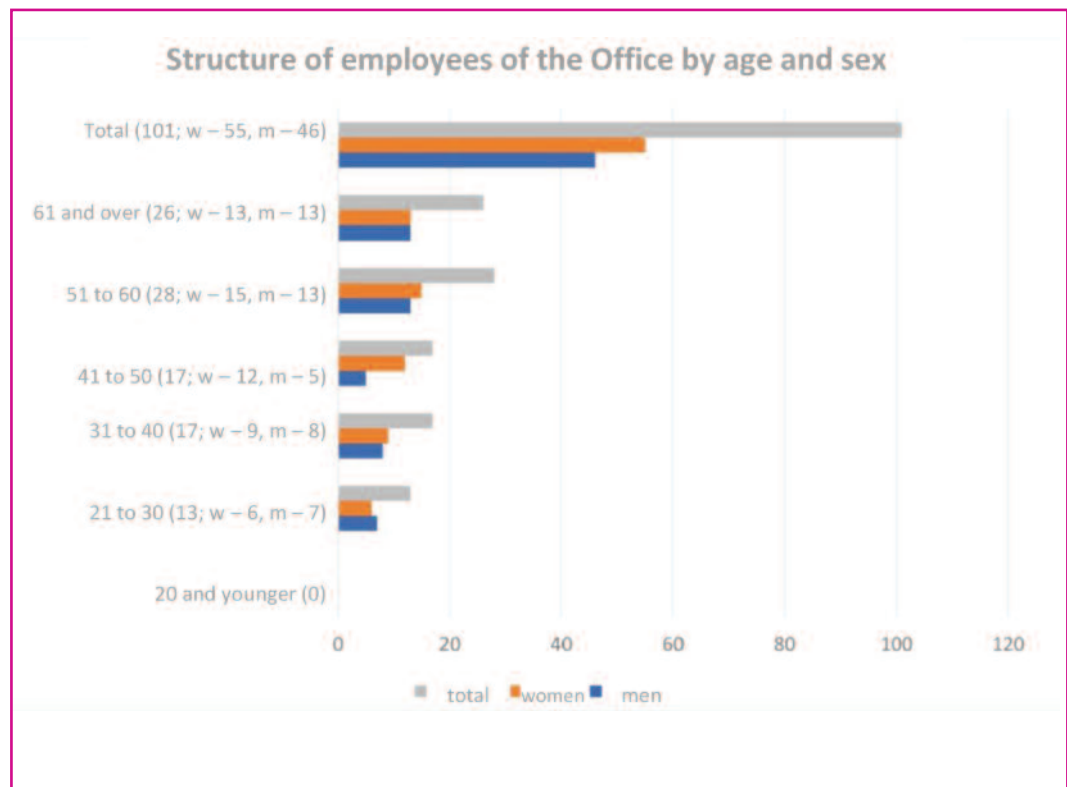
Another 31 persons performed activities in the Office on the basis of agreements on work performed outside an employment relationship.

The graph titled “Structure of employees of the Office by age and sex” shows that the Office employs predominantly employees aged 50 and above. In addition to adequate training, these employees also have a long-term extensive experience. Many of them have worked in the Office for a long time and pass their experience over to new employees who are hired to vacant positions.

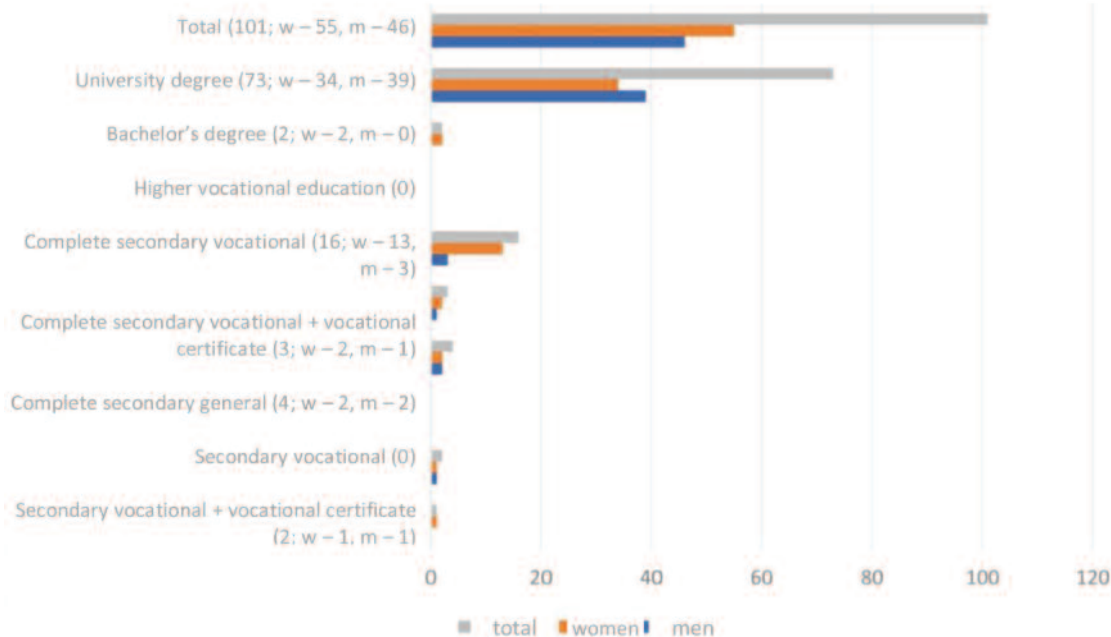
Two thirds of the functional positions at the Office require a university education, while complete secondary education is required for the remaining positions.

The Office allows and provides for professional development of its employees. It ensures that they deepen and, if necessary, increase their professional qualifications. Employees of the Office may also attend English, German and French courses. They can then use the acquired language competences in the performance of their work or service, where language skills are becoming increasingly important due to the new European concept of data protection and privacy. The Office offers internships to students of secondary schools and universities. This promotes interest in topics concerning personal data protection and, at the same time, facilitates search for promising new employees.

The following statistics were valid as of 31 December 2019:



Structure of employees by education and sex



● ECONOMIC MANAGEMENT

The Office's budget was approved by Act No. 336/2018 Coll., on the State budget of the Czech Republic for 2019.

Utilisation of Chapter 343 of the State budget – Office for Personal Data Protection

in CZK thousand

Summary indicators

Total income	2 398,53
Total expenditures	169 618,88

Specific indicators – income

Total non-tax income, capital income and transfers received	2 398,53
of which: total income from EU budget not including CAP	0,00
tother non-tax income, capital income and transfers received	2 398,53

Specific indicators – expenditures

Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	169 618,88
--	------------

Cross-cutting expenditures indicators

Employee salaries and other payments for work performed	67 726,64
Mandatory insurance premiums paid by the employer*)	22 765,48
Basic allocation to the cultural and social needs fund	1 324,29
Salaries of employees in an employment relationship except those in service positions	13 112,93
Salaries of employees in service positions under the Act on Civil Service	41 921,20
Salaries of employees in an employment relationship derived from the salaries of constitutional officials	11 180,27
Total expenditures financed, or co-financed, from the EU budget not including CAP	0,00
of which: from the state budget	0,00
contribution from the EU budget	0,00
Total expenditures recorded in the EDS/SMVS (Subsidy Registration System/Administration of state-owned property) information system	17 443,20

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

1. Income

No income for 2019 has been determined by the approved budget.

The income of Chapter 343 of the State budget – Office for Personal Data

Protection equalled CZK 2,398,530.

This included especially the following:

- refunds of business trips abroad by employees of the Office provided by the European Commission;
- penalties imposed pursuant to Act No. 480/2004 Coll., on certain services of the information society;
- penalties imposed pursuant to Act No. 101/2000 Coll., on personal data protection, or pursuant to Act No. 110/2019 Coll., on personal data processing, and other laws;
- reimbursement of the costs of the proceedings;
- income from 2018 (payment of the balance of the deposit account after payment of salaries and allocation to the cultural and social needs fund for December 2018).

2. Expenditures

Expenditures in the amount of CZK 169,618,880 include:

- all costs of salaries and related expenditures;
- capital expenditures related to the Office building, restoration of information systems, both the Office's system and the ORG information system in the system of basic registers;
- other usual expenditures related to the operation of the Office, i.e. especially items related to the purchase of minor tangible assets, material, IT services, services related to the operation of the building and other services, travel expenditures, education and maintenance;
- expenditures related to non-investment purchases.

The aforementioned amounts correspond to the requirement for purposeful and economic operation of the Office.

3. Platy zaměstnanců a ostatní platby za provedenou práci, vč. souvisejících výdajů

Utilisation of the budget for employee salaries, other payments for work performed and related expenditures, including the basic allocation to the cultural and social needs fund and compensation during sickness in the amount of CZK 92,039,330, corresponds to the qualification structure and compliance with the personnel plan.

As of 31 December 2019, the Office had **101 employees**.

4. Expenditures recorded in the EDS/SMVS (Subsidy Registration System/Administration of state-owned property) information system of the Ministry of Finance

In accordance with the approved documentation of programme 043V10 "Development and renewal of the material and technical resources of the Office for Personal Data Protection since 2017", a total of **CZK 17,443,200** was utilised.

Overview of budget utilisation in 2019

Category	Description	Approved budget for 2019 in CZK thous.	Final budget for 2019 in CZK thous.	Actual state pursuant to the accounting records as 2019 in CZK thous.	Actual final budget in %
2211, 2212, 2322, 2324, 4132	Other non-tax income	0,00	0,00	2 398,53	
	TOTAL INCOME	0,00	0,00	2 398,53	
501	Salaries	65 531,78	69 445,92	66 214,39	95,33
5011	Salaries of employees in an employment relationship except those in service position	12 665,27	13 212,93	13 112,93	99,24
5013	Salaries of employees in service positions under the Act on Civil Service	39 640,11	42 721,20	41 921,20	98,13
5014	Salaries of employees in an employment relationship derived from the salaries of constitutional officials	13 226,40	13 521,80	11 180,27	82,68
502	Other payments for work performed	1 890,91	2 056,23	1 512,25	73,54
5021	Other personnel expenditures	1 890,91	2 056,23	2 512,25	73,54
503	Mandatory insurance premiums paid by the employer	22 923,72	25 415,65	22 765,48	89,57
5031	Mandatory social security premiums	16 855,67	18 774,38	16 686,71	88,88

5032	Compulsory social insurance premiums	6 068,04	6 641,27	6 078,77	91,53
512	Expenditures for certain modifications of tangible assets and acquisition of certain rights to tangible assets	40,00	11,00	9,90	90,00
513	Purchase of materials	1 115,00	1 400,25	1 262,68	90,18
514	Interest and other financial expenditures	30,00	40,00	33,21	83,02
515	Purchase of water, fuels and energy	1 580,00	1 629,54	1 580,64	97,00
516	Purchase of services	41 532,29	54 818,07	51 333,63	93,64
517	Other purchases	2 930,50	4 149,94	2 666,91	64,26
518	Expenditures for non-transfer allocations within the organisation, mandatory payments and deposits	485,00	35,00	0,00	0,00
519	Expenditures related to non-investment purchases, contributions, compensations and gifts in kind	4 503,50	4 131,75	3 240,58	78,43
534	Transfers to own funds and in relation to entities without full legal personality	1 310,64	1 366,73	1 324,29	96,89
5342	Basic allocation to the cultural and social needs fund and social funds of municipalities and regions	1 310,64	1 366,73	1 324,29	96,89
536	Other non-investment transfers to other public budgets, tax payments and other				

	mandatory payments	22,00	15,50	8,80	56,79
542	Compensation paid to citizens	200,00	228,53	222,93	97,55
5424	Compensations during sickness	200,00	228,53	222,93	77,55
	Total current expenditures	146 569,86	161 320,40	148 594,10	92,11
611	Acquisition of long-term intangible assets	11 300,00	11 300,00	3 615,24	31,99
612	Acquisition of tangible fixed assets	11 800,00	20 034,04	13 827,95	69,02
	Total capital expenditures	23 100,00	31 334,04	17 443,20	55,67
	TOTAL EXPENDITURES	167 195,34	196 088,15	169 618,88	86,50

The figures were obtained from reports compiled as of 31 December 2019.

INTERNAL AUDIT

The basic laws and regulations governing the internal audit processes in the Office in 2019 were as follows:

- Act No. 320/2001 Coll., on financial audits in public administration and on amendment to some related laws (the Financial Audit Act);
- Decree No. 416/2004 Coll., implementing Act No. 320/2001 Coll.;
- International Professional Practices Framework of the Institute of Internal Auditors; and
- internal guidelines of the Office.

In organisational terms, internal auditing is separated from management and executive structures; it is functionally independent and directly subordinated to the President of the Office.

The annual plan of internal audit for 2019 was approved by the President of the Office on 15 January 2019. It was based on the following:

- medium-term internal audit plan for the period from 2019 to 2021;
- results of previous internal audits;
- requirements of senior employees of the Office;
- performance of duties following from the Financial Audit Act; and
- available capacities of internal auditing.

Based on the approved annual plan for 2019, internal auditors performed a total of two audits. In compiling the schedule of the individual audits and in selecting the sample of operations to be audited, the division focused primarily on setting the management and control mechanisms and on possible risks in the audited areas and their potential impacts.

Internal audits were focused on verification of the following:

- below-the-threshold public procurement;

The audit evaluated correctness of the procedures for awarding below-the-threshold public contracts pursuant to the law and internal regulations, and reviewed the funds expended on purchases of up to CZK 100,000 in terms of economy, purposefulness and effectiveness.

- management of the property of the Czech Republic;

The audit evaluated correctness of the procedures applied and the performance of the basic duties in management of the property of the Czech Republic on a selected sample of services purchased.

The audit covered postal services, telecommunication and radiocommunication services, financial institutions services, rent, consultancy, legal and advisory services, training and education services, data processing and other services.

- functionality and effectiveness of the internal audit system;

The audit must verify, at least once a year, the effectiveness of the internal audit system pursuant to Section 30 (7) of the Act on Financial Audit.

The results of audits completed in 2019 were discussed with the senior employees of the audited departments and with the President of the Office. Their findings brought added value contributing to a more efficient functioning of financial management, compliance with generally binding legal regulations and internal regulations, and established how the selected audited systems were set up and whether they were sufficiently functional.

In terms of internal audits, nothing indicates that the financial statements of the Office would not provide a true and fair view of the accounting.

Specific measures with defined deadlines were adopted based on the findings. Compliance with the adopted measures is regularly monitored and evaluated by the internal auditors.

No significant findings within the meaning of Section 22 (6) of the Act on Financial Audit were identified in the performance of the internal audits. No possible corruption or fraud has been detected.

In 2019, the internal audit division also:

1. provided consultancy and guidance especially in the area of risk management, internal regulations, property records and implementation of measures;
2. organised training of internal auditors.

Based on the results of the audits, the auditors are able to confirm that in the audited period, the audit mechanisms concerning the selected individual areas of internal operational and financial management were appropriate and effective, with the exception of medium- and low-significance shortcomings. However, these shortcomings were not of such nature that would fundamentally affect the performance of financial management and functioning of the set internal control system. The audits performed contribute to improvement of the quality of the auditing environment, updating internal regulations and compliance therewith, employee education, and protection of legitimate rights and interests of the Office.

FINANCIAL STATEMENTS

The financial statements for 2019 shall be approved and information on their submission provided by the ordinary deadline on 31 July 2020 pursuant to Annex 4 to Decree No. 383/2009 Coll., on accounting records in the technical form used by selected accounting entities and their submission to the central system of accounting information of the State and on requirements on technical and mixed forms of accounting records (the Technical Decree on Accounting Records). In accordance with the communication of the Ministry of Finance concerning application of certain provisions of Act No. 221/2015 Coll., amending Act No. 563/1991 Coll., on accounting, and in connection with Act No. 101/2000 Coll., or Act No. 110/2019 Coll., on personal data processing, the Office is not obliged to have the financial statements approved by an auditor.



Annual report of the Office for Personal Data Protection for 2019

Office for Personal Data Protection

Pplk. Sochora 27, 170 00 Prague 7

E-mail: posta@uouu.cz

Website: www.uouu.cz

On the basis of the duty imposed on it by Section 54 (3)(a) and Section 57 of Act No. 110/2019 Coll., on personal data processing, the Office for Personal Data Protection published this Annual Report on its website in February 2020.

Editor: Mgr. Tomáš Paták, telephone 234 665 286

Editorial review: Mgr. Vojtěch Marcín

Graphic design: Eva Lufferová

Proofreading: Mgr. Eva Strnadová, Andrea Sklenářová

Printed by: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno

Issued for the Office for Personal Data Protection by Masaryk University, Brno, 2020

ISBN 978-80-210-9548-9