

CPT 472

A MESSAGE

ON THE STATUS OF PERSONAL DATA PROTECTION

FOR 2020

Office for Personal Data Protection of the Slovak Republic

March, 2021

Office for Personal Data Protection of the Slovak Republic

Hraničná 12

820 07 Bratislava 27

Slovak republic

<https://www.dataprotection.gov.sk>

Electronic version of the report available at

<https://dataprotection.gov.sk/uouu/sk/content/vyroczne-spravy>

IČO: 36064220

Steuernummer: 2021685985

All rights reserved.

Reproduction for educational purposes

and non-commercial purposes permitted only with reference to the source.

REPORT ON THE STATUS OF PERSONAL DATA PROTECTION 2020

The Office for Personal Data Protection of the Slovak Republic in accordance with the provisions of § 81 par. 2 letter k)

Act no. 18/2018 Coll. on the protection of personal data and on the amendment of certain laws

as amended by Act No. 221/2019 Coll. submits a Status Report to the National Council of the Slovak Republic

protection of personal data for the year 2020. The presented report is an overview of the Office's activities

in the observed period.

According to Art. 59 of the Regulation "Each supervisory authority shall draw up an annual report on its

which may include a list of the types of infringements reported and the types of action taken in accordance with

with Article 58 (2) 2. These reports shall be submitted to the national parliament, the government and others authority designated by the law of the Member State. The reports shall be made available to the public, the Commission and the committee. ".

The said provision was reflected in § 81 par. 2 letter k) of Act no. 18/2018 Coll. about protection personal data and on the amendment of certain laws as amended by Act no. 221/2019 Coll.

"The Office submits a report on the status of personal data protection to the National Council of the Slovak Republic at least once a year; the report on the status of personal data protection is published by the Office on its website the European Data Protection Board and the Commission. ", on the basis of which

I am submitting this report to the National Council of the Slovak Republic on behalf of the Office. After her discussion in the National Council of the Slovak Republic will be published on the website of the Office for Broadcasting available to the media and also submitted to the European Data Protection Board and the Commission.

JUDr. Anna Vitteková

Vice-President of the Office

#### LIST OF ABBREVIATIONS USED

office

Office for Personal Data Protection of the Slovak Republic

NR SR

National Council of the Slovak Republic

a message

Report on the state of personal data protection in 2020

the law

Act no. 18/2018 Coll. on the protection of personal data and on the amendment of certain laws

as amended by Act No. 221/2019 Coll.

Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection

individuals with regard to the processing of personal data and on the free movement of such data

repealing Directive 95/46 / EC (General Data Protection Regulation) (Text with EEA relevance)

Directive 2016/680

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons

persons in the processing of personal data by the competent authorities for the purposes of crime prevention

their investigation, detection or prosecution or for the purpose of enforcing criminal sanctions

and on the free movement of such data and repealing Council Framework Decision 2008/977 / JHA

MPK

Interdepartmental comment procedure

Portal

Legislation Portal Slov - Lex

e-privacy directive

Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 concerning

processing of personal data and protection of privacy in the electronic communications sector

(Directive on privacy and electronic communications)

proposal for an e-privacy regulation

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on compliance

privacy and the protection of personal data in electronic communications and on cancellation

Directive 2002/58 / EC (Directive on privacy and electronic communications)

Convention 108

Council of Europe Convention No. 108 on the protection of individuals with automated processing

personal data

5

Regulation 2018/1725

Regulation (EC) No 1/2003 of the European Parliament and of the Council 2018/1725 on the protection of individuals with

regard to

processing of personal data by the Union institutions, bodies, offices and agencies and on the free

repealing Regulation (EC) No 45/2001 and decision

no. 1247/2002 / EC

Act no. 211/2000 Coll.

Act no. 211/2000 Coll. on free access to information and amending certain

laws (Freedom of Information Act)

EDPS

European Data Protection Supervisor

EU

European Union

EK

European Commission

EEA

European Economic Area

EDPB

The European Data Protection Board established by

Art. 68 Regulations

6

CONTENTS

LIST OF ABBREVIATIONS USED ..... 5

CONTENTS ..... 7

1

INTRODUCTION ..... 9

1.1

Objective of the report ..... 9

STATUS, PERSONNEL SECURITY AND BUDGET OF THE OFFICE ..... 10

2

2.1

Position of the Office ..... 10

2.2

Staffing of the Office ..... 10

2.2.1 Public functions of the Office ..... 10

2.2.2 Personnel of the Office's staff ..... 10

2.3

The Office's budget ..... 12

LEGISLATIVE PROTECTION OF PERSONAL DATA PROTECTION ..... 15

3

3.1

3.2

Interdepartmental comment proceedings ..... 15

Methodological guidelines and information ..... 16

COMMUNICATION OF THE OFFICE WITH THE PUBLIC ..... 18

4

Opinions of the Office on the issues of natural persons and legal entities ..... 18

Provision of information on the basis of requests for access to information in accordance with the law

no. 211/2000 Coll. .... 18

4.3

Office communication with the media ..... 18

4.4

The website of the Office and its attendance ..... 19

4.5

Office website and reporting of personal data breaches ..... 19

4.5.1 Electronic services of the Office for Personal Data Protection of the Slovak Republic .....	20
4.1	
4.2	
5	
6	
RESPONSIBLE PERSON .....	21
APPROVAL AND CONSULTATION ACTIVITIES OF THE OFFICE .....	22
6.1	
Prior consultation .....	22
6.2	
Transfer of personal data .....	22
6.2.1 Transfer to a country guaranteeing an adequate level of personal data protection .....	22
6.2.2 Transfer to a country that does not guarantee an adequate level of personal data protection .....	23
7	
CONTROL .....	25
7.1	
Inspections registered in 2020 .....	25
7.2	
Inspections completed in 2020 .....	26
7.3	
Selection from inspections completed in 2020 .....	27
7.3.1 Controls on the processing of personal data in the information systems by which ensures the practical implementation of the Schengen "acquis" .....	27
7.3.2 Control of processing activities of a company engaged in targeted emarketing and sale of forest fruits .....	27
7.3.3 Control of the processing activities of the rodent trade ...	27

7.3.4 Control of the processing of personal data in a sports association, which is a civic association .....	28
7.3.5 Control of the processing of personal data of the data subjects by an operator who is health care providers in the field of aesthetic-plastic surgery and corrective dermatology .....	28
7.3.6 Control of the operator (legal entity) performing the guard service .....	28
7.3.7 Control in a commercial company mainly engaged in the provision of targeted advertising and creating population analyzes .....	29
7.3.8 Inspection of CCTV systems operated by natural persons .....	29
8	
9	
PERSONAL DATA PROTECTION PROCEDURE .....	31
COOPERATION AND CONSISTENCY MECHANISM .....	33
9.1	
Cooperation mechanism .....	33
9.1.1 Cross-border processing .....	33
9.1.2 Mutual assistance .....	34
7	
9.1.3 Joint supervisory operations .....	35
9.2	
Consistency mechanism .....	35
9.2.1 EDPB opinion .....	35
9.2.2 EDPB Dispute Resolution .....	35
9.2.3 Emergency procedure .....	36
10	
SANCTIONING .....	37

10.1 Fine ..... 37

10.2 Disorder fine ..... 37

10.3 Selected cases from the supervisory activities of the Office ..... 38

10.3.1 Postponements ..... 38

10.3.2 Procedures ..... 39

11

12

REMEDIES AND DECISION-MAKING ..... 44

EUROPEAN AND INTERNATIONAL LEGISLATIVE PROTECTION PACKAGE

PERSONAL DATA .....45

12.1

12.2

12.3

12.4

12.5

12.6

13

MEETINGS WITH PARTNER SUPERVISORY BODIES, CONFERENCES

A WORKSHOPS ..... 48

13.1

13.2

13.3

13.4

13.5

13.6

13.7



13.8	
13.9	
13.10	
13.11	
13.12	
14	
Legislative process at EU level .....	45
European Data Protection Board .....	45
Committee set up under Article 93 of the Regulation .....	46
Cross-border data exchange .....	46
Schengen evaluation .....	47
Convention Consultative Committee 108 .....	47
Good practices for Biometrics at the Borders .....	48
Second meeting of The Hague Forum .....	48
Bitkom Privacy Conference .....	48
IDLaw 2020 - Conference on Innovation and Digitization in Law .....	48
Building Management 2020 .....	49
Cybersecurity for Artificial Intelligence .....	49
QuBit Conference Prague 2020 .....	49
7th AI and Law Breakfasts: Certification of Algorithmic Systems .....	49
eHealth Security Conference 2020 Online Series vol. 2 .....	50
Current challenges of cyber security .....	50
PrivSec Glogal 2020 .....	50
Doing AI the european way: protecting fundamental rights in an era of arificial intelligence.	50
ASSESSMENT OF THE STATUS OF PERSONAL DATA PROTECTION IN THE MONITORED	
PERIOD .....	51

## 1. INTRODUCTION

### 1.1 Purpose of the report

The presented report is the fourteenth in the history of the independent Slovak Republic and the twelfth in the history of existence of a separate office. This is historically the first report submitted in a calendar year, by which the Office fully complies with the Regulation and the other Member States. The period when the Regulation and the law overlapped with the previous legislation, also in terms of monitoring the termination of these processes have been completed in previous reports. Also for the purposes of clarity and compliance with requirements of the Regulation, reporting activities for a calendar year is easier and in the future it will also be more comparable whether there has been an increase or decrease in a particular agenda, or how otherwise developed.

The aim of the report is to provide statistical indicators of the Office's activities, but above all to provide a comprehensive picture of the state of personal data protection in the Slovak Republic and also to point out the Office's activities on an international and European scale. It is no less important description of the actual state of the office with regard to its personnel, material and financial assurance as it was in the monitored period and what is needed on the basis of the above indicators and appropriate to change.

## STATUS, PERSONNEL SECURITY AND BUDGET

### OFFICE

#### 2.1 The position of the Office

The protection of personal data in the Slovak Republic is entrusted to the powers of the Office. The Office is a state administration body with nationwide competence performing supervising the protection of personal data and participating in the protection of fundamental rights and freedoms of natural persons in the processing of their personal data. In exercising its powers, the Office shall proceed independently and in the performance of its tasks, it is governed by the constitution, constitutional laws, laws, others

generally binding legal regulations and international treaties, which is Slovenská

Republic bound. The Office is a budgetary organization according to the provisions of § 21 par. 5 letter a) of Act no. 523/2004 Coll. on budgetary rules of public administration and on amendment certain laws as amended.

## 2.2 Staffing of the Office

### 2.2.1

#### Public functions of the Office

The office is headed by the Chairman, who is elected and removed by the National Council of the Slovak Republic on the proposal of the Government of the Slovak Republic.

The term of office of the President of the Office shall be five years. The position of the President of the Office during the period, its part,

specifically from 01.01.2020 to 29.04.2020 was held by Soňa Pótheová, who was elected to the position

Of the National Council of the Slovak Republic on 14 May 2015 on the basis of the result of the voting of the deputies of the National Council of the Slovak Republic (resolution of the National Council of the Slovak Republic)

Council of the Slovak Republic no. 1736/2015). On the basis of the government's proposal to remove her from office, which was delivered to NR SR on 27.04.2020 (čpt. 74) on 29.04.2020 based on result

of the deputies of the deputies of the National Council of the Slovak Republic on the proposal to remove her from her position, was revoked (Resolution of the National Council of the Slovak Republic)

SR no. CRD-852/2020 of 29 April 2020). She subsequently took over the management of the office in accordance with the law Vice-President of the Office.

In the absence of the President, the Office shall be represented by the Vice-President, who shall be appointed and removed the Government of the Slovak Republic on the proposal of the President of the Office. The term of office of the Vice-President of the Office shall be five

years. Anna Vitteková, who was with effect from

January 2, 2016 appointed by the Government of the Slovak Republic by Resolution no. 658/2015 zo

on 2 December 2015. In connection with the dismissal of the President of the Office for the remainder of 2020, the Office

led by the Vice-President of the Office.

### 2.2.2

Personnel area of the Office 's staff

The employees of the Office perform highly professional tasks in accordance with the law and the Regulation and other operational

activities and obligations under generally binding legal regulations. Securing them

requires the necessary number of qualified staff qualified to carry out professional activities

at expert level, taking into account the necessary degree of substitutability.

In the conditions of the Office, from the point of view of the staff structure, with the exception of one staff member,

who performed work in the public interest, the other employees in 2020 were employees

in civil service. Selection of employees and filling of vacancies

positions is realized according to the conditions stipulated by law for individual functions exclusively on

on the basis of tenders.

As of 1 January 2020, the Office had 49 seats, of which

☐ 48 employees in the civil service relationship,

☐ 1 employee performing work in the public interest.

10

As of 31 December 2020, the Office had 50 seats, of which

☐ 49 employees in the civil service relationship,

☐ 1 employee performing work in the public interest.

Average age of employees

☐ as of 01.01.2020 it was 40.62 years, while

☐ was 41.87 years for men;

☐ in women 40.09 years;

☐ as of 31.12.2020 was 41.56 years, while

☐ was 43.14 years for men;

□ for women 40.91 years.

Overview of the number of employees of the Office

Year

to 01.01.2020

to 31.12.2020

Actual staffing of the Office

Civil service

Performance of work in public

ratio

interests

48

1

49

1

Together

49

50

The protection of personal data has been carried out since 25 May 2018 in accordance with the Regulation and the law, which directly determine to the Office all its rights, obligations and competences. Despite the undisputed the importance of the Office 's work, which depends on the importance and value of personal data, such as sources of information on natural persons, the number of staff of the Office did not change significantly and even in 2020 was not sufficient in the context of the agenda that the Office ensures and that it still has an increasing trend in terms of the volume of work per employee. For the right activities of the Office and also with regard to human capabilities and the pursuit of high-quality work of employees it is essential that the number of employees be significantly increased. This will ensure a redistribution of work and the possibility of higher specialization of individual employees, as many now perform

cumulative activities, each of which requires full concentration and attention.

The Office had a set limit of 51 employees in 2020, and it notified annually

and warns of the need to increase their number, ie to increase the said limit of the maximum number

employees at least 30. Nevertheless, for 2021, the Office's staff limit was reduced

to 461. The Office's agenda, even in the context of the obligations arising from the Regulation, has increased

disproportionately and has

constantly growing trend. On average, there are more than 120 files per employee per

equipment. The current situation is unsustainable in the long run and there is a shortage of skilled people

employees is inevitably reflected in the quality of work, or results in impossibility

compliance with procedural deadlines. In connection with non - compliance with procedural deadlines, the Office was also

contacted

by the Ombudsman, who was approached by two parties precisely because of the disproportionate nature

long duration of personal data protection proceedings. On the basis of an examination of those proceedings

the Ombudsman found that the administrative procedure had been followed by an administrative body, but

non-compliance with the legal deadline for issuing a decision. To this end, the Ombudsman

imposed on the Office measures aimed at streamlining communication with the parties to the proceedings

regarding the time limit of the proceedings themselves. To fulfill the strategic direction of the Office 's activities is

necessary to increase the number of staff to complete and participate on an ongoing basis

The reduction of the limit of the number of employees of the Office occurred on the basis of discussion and approval of the

material "Draft Budget

public administration for the years 2021 to 2023 ", material number: UV-22129/2020; on the basis of which the Resolution was

adopted

Government of the Slovak Republic no. 649/2020 of 14/10/2020. Mandatory consideration of staff reductions in the conditions

of the Office

meant the loss of 5 employees.

necessary educational activities, they expanded their knowledge and were thus able in addition to professional growth should also reflect the requirement to digitize public and state administration.

The Office also needs to be strengthened by information technology experts, as more and more processing activities takes place in electronic form and it is necessary that, as part of the as well as inspections, the Office was able to comment at expert level on the findings on the information technologies used by operators and intermediaries.

The Office also feels the lack of staff dedicated to legislation, both in its area as well as its comments, as this is a lengthy process of examining the submitted proposal legislation or a non-legislative proposal that requires high attention and concentration and it is essential that the employee has sufficient time and knowledge for such work, and not only theoretical but also practical. The undersized personnel side of the office is also reflected in this that the Office at that time could not at all consider setting up seconded workplaces, which would it was also closer to the persons concerned, the operators and the intermediaries.

Underestimation of the number of employees also has the effect that it is not possible to develop what is necessary specialization by creating new departments, which would take over from the existing ones and subsequently develop some agendas to the expert level. We consider it especially necessary for it to be an employee the Office is provided with the necessary training, which will have a positive impact on the performance of their activities, so in terms of speed, but especially expertise.

The very limited possibility of training current employees also seems to be problematic and the inability to obtain and keep erudite in the long run with adequate pay conditions specialists, as a result of which the Office is not in an equal position vis-à-vis operators and their possibilities, which is ultimately always to the detriment of the person concerned. From application practice

The Office has an urgent need to establish at least two seconded workplaces, one at Central and one in eastern Slovakia. The reason for the need for these workplaces is to the employees of the Office were closer to the affected persons also from these areas of Slovakia and also the fact that

that this would make the performance of controls more efficient and significantly reduce the Office's travel costs employees from Bratislava; The Office would also contribute to increasing employment in those regions where there are still enough qualified people who cannot or do not want to move.

### 2.3 The Office 's budget

The Office is a budgetary organization that is tied to the state with its revenues and expenditures budget through the chapter General Treasury Administration, which is administered by the Ministry of Finance of the Slovak Republic.

The budget for the Office was originally approved for 2020 in the amount of EUR 1,859,514.00. In a month October 2020, the Office's budget for capital expenditures for the inter-ministerial element was increased 0EK0W02 - Information technology, financed from the state budget to provide computing technology in the amount of 71,400.00 Eur.

The drawing of the Office's budget as at 31 December 2020 amounted to EUR 1,961,941.93, which represents 99.93% of the Office's total adjusted budget for 2020.

12

Overview of the Office's budget for the period 01.01.2020 - 31.12.2020 in Euros

Approved

budget

to 1.1.2020

Modified

budget

to 31.12.2020

Drawing a budget

from 1.1.2020 to

12/31/2020

1,064,496.00

1,068,288.00



1,067,113.49

Wage premiums (620)

375,598.00

392,749.84

392,749.84

Goods and services (630)

403,420.00

357,485.18

357,392.73

Current transfers (640)

5,000.00

47,463.98

47,463.98

0EK0W02 (630) current expenses

11,000.00

26,000.00

25,998.29

1,859,514.00

1,891,987.00

1,890,718.33

Capital expenditures (700)

0

0

0

0EK0W02 capital expenditures

(710)

0

71,400.00

71,223.60

1,859,514.00

1,963,387.00

1,961,941.93

Pointer

Wages, salaries, service income

and OOV (610)

Total current expenditure (600)

Total expenditure

Similarly, the need to increase the number of employees in the context of increasing activity

and responsibilities

office,

is an

necessary

take into account

increase

agenda

a

needs

material and technical equipment in the Office 's budget. The increase was recorded by the office in the European and other

international agenda, where the staff of the Office is directly involved and must regularly

participate in meetings of the Committee 's expert groups and Council working groups, of which

the subject is important guidelines and documents influencing the activities of the Office on behalf of Slovakia

of the Republic.

The Office carries out activities arising not only from the Regulation and the law, but also from other special ones regulations, for example under REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE Euratom) 2019/493 of 25 March 2019 amending Regulation (EU, Euratom) No 1605/2002 1141/2014, as regards the procedure for verifying infringements of personal data protection rules in context elections to the European Parliament (see Article 10a (2) of that Regulation). If the Office decides in personal data protection proceedings, that a natural or legal person has infringed the relevant rules on the protection of personal data and if it follows from the decision or if others are justified

13

reasons to believe that the breach relates to the political activities of a European political party or a European political foundation in the context of the European elections, so the decision notify the Office for European Political Parties and Foundations.

In the period from 15.07.2020 to 03.09.2020, a Government audit focused on verification was performed compliance with the measures taken to remedy the deficiencies and to eliminate the causes of their identification Government audit during the inspection in 2018. The aim was also to verify and evaluate others facts, if so provided by a special regulation. Government Audit Report dated September 10, 2020 noted that the Office was functioning well for the audited period, but some more needed to be done improvements. Based on the above-mentioned Government Audit Report, the Office prepared a list measures taken and sent to the Office of Government Audit, Bratislava office and the measures were and are subsequently implemented and applied in the application practice of the Office.

14

### 3 LEGISLATIVE PROTECTION OF PERSONAL DATA PROTECTION

#### 3.1 Interdepartmental comment procedures

The Office is a state administration body with nationwide competence performing protection supervision personal data and involved in the protection of fundamental human rights and freedoms in processing personal data of natural persons. The Office fulfills its role in the field of processing supervision personal data also by supervising and commenting on the texts of draft laws and others

generally binding legislation (legislative materials) as well as texts

non-legislative materials (visions, strategies, etc.). He formulates his comments on the proposals through the Portal within the MPK. The purpose of the observations submitted by the Authority is in particular, the quality of the legislation regarding the processing of personal data is high that the legislation subsequently adopted is precise, unambiguous and thus in a relationship to the controller as well as in relation to the data subject whose personal data will be in practice subject to processing.

During the period under review, the Office submitted comments on 23 materials from all submitted to the MPK (regardless of whether the material was legislative or non-legislative nature). In total, the Office submitted 86 comments, 69 of which were substantial.

The Office always strives to improve the legal regulation with the applied comments, or drawing attention to the need to protect and respect the legislation concerning the processing of personal data if the subject of the comment is non-legislative material, such as a concept that has in the future to be the basis for drafting legislation or meeting the set goals.

Minor shortcomings in the legislation can be corrected by ordinary comments that in principle, they clarify or adjust the correct wording of the provisions in a form which, as far as about processing is correct.

The essence of the Office 's observations consists of fundamental observations which refer to more or less fundamental shortcomings of legal norms that need to be supplemented or revised.

During the period under review, many of the Office's key comments were addressed to the responsible authorities determining and specifying the purpose for which the personal data are to be processed, as long as the purposes were formulated very generally or completely absent, which in terms of legal certainty and the enforceability of the legal norm in practice would certainly cause problems and be to the detriment the person concerned. Another often recurring key comment was the requesting one deletion of certain proposed provisions, as their proposed processing in context purpose went beyond necessity and necessity. In the case of such comments, it often happened that

that the office did not receive a satisfactory answer from the manager even at the dispute, why it is extensive necessary or what it results from and what is to be achieved by it. In several

In some cases, the discrepancy was removed by an explanation and the wording adjusted together. To others, still a more frequent recurring commented deficiency on the part of the Office is in terms of content insufficient explanatory statement, especially its special part, when in particular in the provisions concerning reasons for the proposed regulation are missing, the explanations from by the draftsman. The justifications in the explanatory memorandum are often general one sentence from which it is not clear why processing is required and why it is necessary to that extent. A very common recurring remark is the absence of internal references to other special laws that specify and supplement the very purpose of personal data processing in accordance with the legal agenda to which the processing may relate, or refer to a provision another law, where the scope or list of personal data processed is established on established purpose.

In the period under review, the pandemic also had an impact on the drafting of legislation and the manner in which it was adopted

15

Covid 19, which, in terms of legislation and in the opinion of the Authority, has affected its quality rather negative, as many legislative standards have been adopted in abbreviated legislation proceedings, without comment. The Office does not dispute that the protection of human life is paramount, no in its legislative setting in order to prevent the spread of Covid 19 should be fundamental legislative amendments are adopted so that they are also in line with the legislation governing others fundamental human rights so as not to create a situation where legal norms are mutually exclusive compete or collide.

The specific wording of the submitted comments of the Office can be searched on the Portal using a filter institutions and using a comment filter (whether it is a comment from an organization marked as essential, or ordinary).

### 3.2 Methodological guidelines and information

The Office methodically guides operators and intermediaries in the processing of personal data data, raises public awareness of the risks and rights associated with the processing of personal data data and also raises the awareness of controllers and intermediaries about their obligations.

Proven form of operator and intermediary guidance and information

based on the practice of the Office, the methodological guidelines of the Office have become public, especially of the persons concerned

and short ad hoc methodologies published on the Office's website dedicated to issues

and issues that are of public interest or need at the time

to inform.

In the monitored period, among the most monitored were mainly those related to information and opinions

Office to the pandemic situation and the processing of personal data in connection with it, for example:

☐ ÚOOÚ SR and the project of intelligent quarantine [published 16.04.2020, available on this

link

<https://dataprotection.gov.sk/uouu/sk/content/uouu-sr-projekt-inteligentnejkaranteny>]

☐ Statement of the Office on the planned population testing in Covid 19

[published

21.10.2020,

available

on the

this

link

<https://dataprotection.gov.sk/uouu/sk/content/vyjadrenie-uradu-k-planovanemu-plosnemu-testovaniu-obyvateľstva-na-covid-19>]

☐ Cameras of municipalities and cities and their possible use for monitoring the density and number of people before

test sampling point for surface testing - Guideline [published

27.10.2020,

available

on the

this

link

□ Coronavirus and personal data processing Frequently asked questions updated

from 22.10.2020

[published

22.10.2020,

available

on the

this

link

Of course, the Office also monitors developments in the field of personal data protection in the case of judgments

European Court of Human Rights or the Court of Justice of the European Union. All relevant

publishes decisions affecting the protection and processing of personal data on its website

headquarters in the Legislation and case law section. It also informs about important decisions in the form of a short one  
news directly in the news on its website.

During the period under review, the Office published information on the rulings of the Court of Justice of the European Union  
Union:

□ Decision of the ECJ in the Schrems II case [published on 16.07.2020, available at this link

□

see also Frequently Asked Questions on this Decision [published

27.07.2020,

available

on the

this

link

<https://dataprotection.gov.sk/uouu/sk/content/casto-kladene-otazky-v-suvlosti-srozhodnutim-vo-veci-schrems-ii>]

Decision of the ECJ in the case of Orange Romania SA [published on 12.11.2020, available at

this link <https://dataprotection.gov.sk/uouu/sk/content/rozhodnutie-sd-eu-vo-veciorange-romania-sa>].

Subject to publication and indirectly also in the form of education, both operators,

intermediaries, as well as the persons concerned, the disclosure of information and guidelines issued

EDPS and EDPB on the Office's website.

During the period under review, the following EDPB guidelines were published on the Office's website,

of which the Office informed:

□ EDPB guidelines on the processing of personal data by camera equipment

[published

04.02.2020,

available

on the

this

link

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-o-spracuvani-osobnychudajov-prostrednictvom-kamerovych-zariadeni>]

□ EDPB guidelines on the processing of health data for scientific research

in connection with the outbreak of Covid 19 [published April 22, 2020, available at



links

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-o-spracuvani-udajovtykajucich-sa-zdravia-na-ucely-vedeckeho-vyskumu-v-suvislosti>]

□ EDPB Guidelines on the right to be forgotten in search engines (Part 1) [published

15.07.2020,

available

on the

this

link

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-k-pravu-na-zabudnutie-vovyhľadavacoch-1-cast-0>]

□ EDPB guidelines on the relationship of the Second Payment Services Directive in the internal market

and the General Data Protection Regulation [published 22.12.2020, available on this

link

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-ku-vztahu-druhejsmernice-o-platobnych-sluzbach-na-vnutornom-trhu-vseobecneho>]

□ EDPB guidelines on the interpretation of Articles 46 (1) 2 letter a) a 46 ods. 3 letter (b) general

Data Protection Regulation [published on 22.12.2020, available at this link

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-k-vykladu-clankov-46-ods-2pism-46-ods-3-pism-b-vseobecneho-nariadenia-o-ochrane>].

The Office uses the website to keep up to date with current protection events

personal data. As 2020 was a year in which almost the whole world gradually hit

Covid 19 pandemic, much of the information spectrum consisted of

processing of personal data in connection with a pandemic, whether within the Slovak Republic, or

Of Europe. Attention was also paid to other current information concerning the statement

opportunities to participate in commenting on the forthcoming EDPB guidelines or information

on the legal views and positions of the EDPS.

Examples include:

□ Handbook for Eurodac fingerprint authorities [published 28.01.2020,

available at this link

[https://dataprotection.gov.sk/uouu/sk/content/prirucka-preorgany-pri-odoberani-odtlackov-prstov-pre-eurodac\]](https://dataprotection.gov.sk/uouu/sk/content/prirucka-preorgany-pri-odoberani-odtlackov-prstov-pre-eurodac)

□ Information document on Brexit and binding internal rules (BCR)

[published

27.07.2020,

available

on the

this

link

[https://dataprotection.gov.sk/uouu/sk/content/informacny-dokument-k-brexituzavaznym-vnutropodnikovym-pravidlam-bcr\].](https://dataprotection.gov.sk/uouu/sk/content/informacny-dokument-k-brexituzavaznym-vnutropodnikovym-pravidlam-bcr)

17

## COMMUNICATION OF THE OFFICE WITH THE PUBLIC

### 4.1 Opinions of the Office on the issues of natural and legal persons

The issue of personal data protection does not only concern operators or intermediaries, who have a duty to apply personal data protection legislation in practice, but also people, specific natural persons - affected persons having issues arising from normal situations related to their personal data and their processing. In the observed period with respect to

The pandemic was dominated by issues related to the processing of personal health data, temperature measurement, processing data on the health of children in schools and kindergartens with a view to their follow-up attending a preschool or school facility. Again, a fairly large number of questions

formed issues related to the processing of personal data in apartment buildings and the installation of cameras in apartment buildings. Many questions led to extensive testing and processing of personal ones data of tested persons. As many of the issues were within the material scope of the ÚVZ SR, these were to him were transferred to the equipment.

The Office's operators and intermediaries most often address questions of a professional nature related to their obligations arising from the Regulation and the law, or special laws governing processing operations. As municipalities and cities are also operators, several one of them addressed the office in connection with either testing or its preparation and addressed questions the Office, in particular with regard to their position in the testing process or the fulfillment of their information obligations against the persons concerned or the possibility or impossibility of using municipal or city operating cameras for the purpose of monitoring the density of persons in front of the test site.

The staff of the Office dealt with 975 questions during the period under review, taking into account that records are kept on the document, not the number of questions asked in it, so it really was equipped with several times more questions from the public.

#### 4.2 Provision of information on the basis of requests for access to information in accordance with the law no. 211/2000 Coll.

One of the possibilities for public access to information is also the possibility to submit a request within the meaning of Act no. 211/2000 Coll. The Office, as the liable person, will evaluate these applications in accordance with the law no. 211/2000 Coll. equip.

In 2020, the Office received 212 requests for access to information. Of this total

In 50 cases, the Office processed the request by making the required information available, in 44 in some cases, it issued a decision not to disclose the information in part and at the same time which could have been disclosed, in 40 cases the Office issued a decision not to disclose the information, in 30 cases, he postponed the submitted applications because they were not within the deadline specified in the call for completions

supplemented. In 48 cases, the Office forwarded the Office as the relevant application processing department these to another relevant department of the Office of Equipment, as their contents indicated that they were not request for disclosure of information, but for example a question to the public, resp. some advanced on equipping another liable person to whom the competencies belonged on the basis of the assessment of their content.

#### 4.3

## Office communication with the media

The issues raised by the media were specific issues and "cases" in which it was the subject processing or protection of personal data, or journalists' questions have been directed at specification of the rights of the persons concerned, how to exercise them correctly and all that is possible the person concerned may seek redress from the operator. Especially since March of the period under review issues of processing and protection of personal data in connection with the pandemic have come to the fore, and the follow-up and obligations related to the processing of personal data

18

natural persons, in particular where health data have been processed. Also big repeated security incidents involving the National Center have aroused media interest health information; specifically leak information about Covid 19 positive people called. "Covid map "or a breach of My eHealth. The topic of processing and protection of personal data data related to the coronavirus pandemic dominated journalistic issues to the end period and was only exceptionally "interrupted" by another, currently current topic.

### 4.4 Office website and its traffic

The Office's website meets the conditions and technical criteria in accordance with the Decree of the Ministry of Finance SR on standards for public administration information systems, reflects on the new legislation in the field of personal data protection, and is gradually supplemented by new functionalities and up-to-date forms, methodologies and guidelines. The Office also bases its appearance on and the division of its website and tries to make the website more transparent as user-friendly as possible. In the rest During the period under review, the Office sought to improve and supplement, in particular, the English version persons knew how to get information even if they do not speak Slovak and also in the context of that office and the Slovak Republic have been the subject of a Schengen evaluation as regards the protection of personal data data, where the evaluators were also interested in accessing and providing information in English, or another foreign language, or the language of a national minority.

The Office 's website was searched a total of 734 654 times during the reporting period, which is

an increase of more than 300,000 visits compared to 2019.

#### 4.5 The Office's website and reporting privacy breaches

The Office's website is a key source of information related to personal data protection.

At the same time, it is also a basic service according to Act no. 69/2018 Coll. on cyber security

and amending certain laws. Operators and intermediaries must ensure

the continued credibility, integrity, availability and resilience of processing systems and services

and to assess at regular intervals the effectiveness of the technical and organizational arrangements in place

measures. Nevertheless, it may occur (whether due to intentional action, negligence, error or

natural disaster) to a personal data breach which, as a result, may

mean accidental or unlawful destruction, loss, alteration, unauthorized disclosure or

disclosure of personal data transmitted, stored or otherwise processed.

The operator has an obligation under Art. 33 Regulations or to report a violation pursuant to Section 40 of the Act

protection of personal data (so-called "data breach") of the Office. He may do so in relation to the Office

in several ways, one of which, recommended, is the opportunity to take advantage of this

the designated form, published on the Office's website, which was the beginning

during the reference period, so that the Office, on the basis of its details and answers in it

provided all the information necessary to know the breach of protection

personal data.

In the period under review, 159 personal data breaches were formally reported to the Office

(in all specified ways). After examination and evaluation of this number, it was possible as

privacy violations actually mark 107 reports. The remaining 52 reports

represented, for the most part, another of the Office's agendas, such as the request to initiate proceedings, was unfounded

a complaint lodged without relevant information or any other non-compliant document

breach of personal data protection within the meaning of Art. 33 Regulations. Violation report is

obligation for operators, not for the persons concerned. In cases of breach of protection

personal data were reported by the data subjects, they often stated that they had reported a breach

that the operator stated that he would not report it to the office because it was not an incident

19

evaluated as such, which must be reported to the Office. We would also like to appeal this way operators to fulfill their obligations themselves, as if the Office finds that they have occurred to a breach of personal data which has not been reported to the Office and should have been, it may be considered an aggravating circumstance by the Office in any personal data protection proceedings with a direct impact on a possible increase in the fine imposed.

The most frequent violations of personal data protection in the monitored period occurred due to:

- ☐ unauthorized disclosure or disclosure of personal data, a total of 62 cases;
- ☐ cyber attack, a total of 24 cases;
- ☐ theft by burglary and theft of media containing personal data, a total of 6 cases;
- ☐ isolated cases of personal data breaches due to unauthorized use

opening of mail, exchanges of persons and thus also exchanges of personal data.

#### 4.5.1 Electronic services of the Office for Personal Data Protection of the Slovak Republic

In order to achieve full legislative compliance in the field of information and cyber security and also the provision of electronic services of the Office on 17.12.2020 Office and the Ministry of Transport and Construction of the Slovak Republic on behalf of the Ministry of Investment, Regional Development and informatization of the Slovak Republic signed Contracts on the provision of non - repayable financial contribution in the amount of EUR 4,276,620.28 for the implementation of the Office 's Electronic Services Project at protection of personal data of the Slovak Republic.

The aim of the project is to build a comprehensive solution for an information system that will effectively electronically support the Office's processes, thus optimizing process automation office and subsequently streamline the handling of the agenda by staff. Also with the project and accepted facilitate the communication of the external environment with the Office and vice versa.

20

5 PERSON RESPONSIBLE

For supervising the protection of personal data processed in accordance with the Regulation and the law the operator is responsible. The operator and the intermediary may or must not in specified cases (Article 37, paragraph 1, letters a) to c) of the Regulation, or § 44, para. 1 letter a) to c) of the Act) to determine the responsible person by exercising supervision over the protection of personal data obliged to report it to the Office.

Overview of the number of designated responsible persons reported to the Office

Responsible people

Total number of reported responsible persons

Period

01.01.2020 to 31.12.2020

Count

1609

Number of requests addressed by the persons concerned to the Office as operator

In 2020, the Office received in fact 4 applications from the persons concerned, two of them gradually applied by the same person.

In 2 cases, the data subjects exercised the right to erase (forget) their personal data.

In both cases, the requests of the persons concerned were dealt with by sending confirmation that the Office their personal data, other than those available to them at their request before did not process the requests.

In 1 case, the data subject exercised the right of access to his or her personal data. The person concerned a confirmation was sent stating that the Office had not processed her personal data before receiving the application.

The same person subsequently exercised the right to erase (forget) his personal data. This the application was not granted positively due to the fact that the Office is related in accordance with a special regulation with the registry rules of the Office obligated her personal data for the purpose of processing the application of the data subject persons (in its case also for other purposes) to keep for a period of 5 years the closing of the file material.

## 6 APPROVAL AND CONSULTATION ACTIVITIES OF THE OFFICE

### 6.1 Prior consultation

According to Art. 36 par. 1 of the Regulation "The operator shall carry out with the supervisory authority before processing consultation if the data protection impact assessment pursuant to Article 35 shows that this processing would lead to a high risk if the controller did not take measures to mitigation of this risk. "

According to Art. 35 par. 5 of the Regulation "The supervisory authority may also establish and publish a list processing operations for which a data protection impact assessment is not required.

The supervisory authority shall forward these lists to the Committee. "; to the so-called list of processing operations which will not be subject to a personal data protection impact assessment (white list) the republic has not yet acceded.

According to Art. 35 par. 4 of the Regulation "The Authority shall draw up and publish a list of those processing operations that are subject to a data protection impact assessment requirement pursuant to paragraph 1. The supervisory authority shall forward these lists to the Committee referred to in Article 68. "; list processing operations, which are always subject to the impact assessment of the Slovak Republic in terms of of the said article (the so-called black list), is available on the website of the Office "List processing operations subject to a personal data protection impact assessment Slovak Republic". This list of processing operations serves, among other things, for clarification

Art. 35 par. 1 The regulations and operators who intend to carry out such processing are in the event that their intended processing would lead to a high risk to rights and freedoms the persons concerned should the operator fail to take measures to mitigate that risk, shall be required to consult the Authority in advance.

During the period under review, a repeated request for prior consultation was made, submitted in 2019. In the case of this previous consultation, the operator was informed recommended to take sufficient measures in relation to the planned processing activity to minimize the risks associated with the use of the technologies planned by it.



In 2020, the Office received one request for prior consultation, which is currently under investigation is being addressed.

## 6.2 Transfer of personal data

The free movement of personal data is guaranteed within the EEA. However, when transferred to countries outside the EEA or international organizations, additional protection requirements need to be complied with personal data referred to in Regulation and Directive 2016/680. Although some transfer tools personal data under both laws are the same, it is always necessary to examine the factual the scope of the instrument used. A novelty compared to the previous legislation is that it is being amended transmission to international organizations.

Transfers can be divided into two groups:

- ☐ transfer to third countries (international organizations) guaranteeing an adequate level protection,
- ☐ transfer to third countries (international organizations) that do not guarantee an adequate level protection.

### 6.2.1

Transfer to a country guaranteeing an adequate level of personal data protection

When transferring personal data to third countries, a distinction is made between the transfer of personal data to

22

third country guaranteeing or not guaranteeing an adequate level of personal data protection. Status country, which guarantees an adequate level of personal data protection, the EC determines decision. It is necessary for the third country to ensure, by reason of its national law or international agreements it has signed, the level of protection of fundamental rights, which is equivalent to the level of protection guaranteed by EU law.

The EC issues a decision on adequacy separately for the material scope of the Regulation and separately for the material the scope of Directive 2016/680. Decisions on adequacy issued by the EC during its term of office

Act no. 122/2013 Coll., Remain in force until the EC changes, replaces or cancels them

by a decision taken pursuant to the Regulation. These decisions apply only to the transfer of personal data within the material scope of the Regulation, not Directive 2016/680. The Office shall publish adequacy decisions on its website.

During the period under review, the EC did not issue any decision on adequacy under the Regulation or the Directive 2016/680.

## 6.2.2

Transfer to a country that does not guarantee an adequate level of personal data protection

Even when transferred to a country or international organization that does not guarantee an adequate level of protection, it is necessary to distinguish between the instruments offered by the Regulation and those offered by Directive 2016/680.

### 6.2.2.1 Transmission according to the Regulation

If the EC has not issued a decision on adequacy, or annulled the decision on adequacy, the operator or intermediary may also use the following institutes for the transfer:

(a) a legally binding and enforceable instrument between public authorities; or  
public bodies

No such instrument was adopted during the period under review.

(b) binding internal rules

During the period under review, no binding internal rules were adopted by the Office under Regulations.

(c) the standard data protection clauses adopted by the EC

No standard clauses were adopted under the Regulation during the period under review.

(d) standard data protection clauses adopted by the supervisory authority;

During the period under review, no standard clauses were adopted by the Office under Regulations.

(e) an approved code of conduct

No codes were approved during the period under review.

(f) an approved certification mechanism

No certification mechanisms were approved during the period under review.

(g) contractual clauses

No contractual clauses were approved during the period under review.

(h) the provisions to be inserted in the administrative arrangements between the public authorities

or public bodies and include the enforceable and effective rights of the persons concerned

No administrative arrangements were approved during the period under review.

23

(i) exemptions for special situations under Art. 49 Regulations

j) single transfer of personal data according to Art. 49 par. 1 second subparagraph

#### 6.2.2.2 Transmission according to Directive 2016/680

In the absence of a decision on adequacy, Member States shall provide for the transfer of personal data

to a third country or international organization may be carried out using the following instruments:

(a) a legally binding act providing adequate safeguards for the protection of personal data; or

(b) the controller has assessed all the circumstances of the transfer of personal data and concluded that there are adequate guarantees for the protection of personal data,

c) exceptions for special situations pursuant to Section 76 of the Act,

d) transfer to a recipient from a third country pursuant to Section 77 of the Act.

24

## 7 CONTROL

The supervision is mainly focused on the operators and intermediaries who are in the process

personal data must comply with the principles laid down in the Regulation and the law, as well as

the legitimate interests and freedoms of the data subjects whose personal data are the subject of processing.

The Office is authorized to control the processing of personal data within its competence,

control of compliance with the code of conduct approved by the Office pursuant to Section 85 of the Act, control of compliance

processing of personal data with the issued certificate according to § 86 and control of compliance issued a certificate of accreditation pursuant to § 87 and § 88 of the Act. In the territory of Slovakia In the Czech Republic, only processing inspections were carried out in 2020 (hereinafter "assessment period") personal data.

Controls on the processing of personal data by the delegated control authority are always in place focused on a specific operator or intermediary and their results are formulated in the inspection record (if no breach of personal processing obligations has been identified) data) or in the inspection report (if non-compliances were found in general binding legislation). The results of the inspections formulated in the inspection report are initiated initiation of personal data protection proceedings or are used as a basis for issuing a decision in ongoing personal data protection proceedings.

With regard to the protection of the life and health of natural persons representing processing entities personal data (authorized persons of operators and intermediaries) as well as for the protection of life and the health of the Office's employees, the Office's control activities were significantly affected in 2020 adverse conditions resulting from the current pandemic situation (including the accommodation and restaurant facilities, employers of the applied regime of work from home, and so on).

#### 7.1 Inspections recorded in 2020

During 2020, the Office registered 65 new controls on the processing of personal data. Of this number, 10 inspections and 55 inspections were completed in the same year (in various cases) procedural stage of control) was carried over to 2021.

Out of the total number of 65 inspections, 19 inspections were registered in 2020 on the basis of an inspection plan, 34 controls in personal data protection proceedings and 12 suspicions from breach of personal data processing obligations.

Number of checks

34

30

20

19

12

10

0

Based on the inspection plan

In the proceedings

25

Based on suspicion

## 7.2 Inspections completed in 2020

In the evaluated period, the Office completed 39 inspections of personal data processing, of which 9 inspections started in 2020 and 30 controls started in the previous period. Subject to 39 inspections completed in the monitored period were processing activities of state bodies in 10 cases and organizations, in 4 cases processing activities of local self-government bodies (cities and municipalities), in 20 cases the processing activities of other legal entities (including two banks, one insurance company and one health care provider) and sports processing activities union. In 2020, checks on the processing of personal data were also performed on 4 natural persons.

As part of the 14 inspections completed in 2020, no breach of the Regulation was found, as a result these inspections were completed by the inspection record. The performance of the remaining 25 inspections was found conflicts with the requirements of the Regulation, as a result of which these inspections were terminated by the Protocol on control.

Structure of inspected persons and results of inspections completed in 2020

Controlled persons

Deficiencies found

(inspection report)

state authorities and organizations

local authorities

other legal entities

sports association

natural persons

5

2

16

1

1

25

No detected

shortcomings

(inspection record)

5

2

4

0

3

14

Controls on the processing of personal data completed during the period under review were carried out within the framework of personal data protection proceedings, on the basis of a control plan as well as on the basis of suspicion from breach of obligations in the processing of personal data provided for by the Regulation or the law. The focus of controls was on the real state of personal data processing with an emphasis on compliance processing activities with the requirements of legal regulation represented in particular by the Regulation

and the law. In the creation of the inspection plan, as well as in the selection of inspections continuously initiated by the Office on

the Office drew mainly on suspicion of a breach of personal data processing obligations from their own experience gained in the performance of their supervisory tasks.

Structure of incentives for inspections completed in 2020

Number of checks

20

16

15

14

9

10

5

0

Inspection plan

In the proceedings

26

Suspicion

7.3 Selection from controls completed in 2020

7.3.1

Controls on the processing of personal data in the information systems by which ensures the practical implementation of the Schengen "acquis"

The Office regularly includes in the plan of inspections the processing of personal data in information systems to ensure the practical implementation of the Schengen "acquis" competent authorities in the territory of the Slovak Republic, as well as Slovak embassies

Republic abroad. In 2020, 3 inspections started in 2019 (Consular

Department of the Ministry of Foreign Affairs of the Slovak Republic, the Embassy of the Slovak Republic in Cairo and the Embassy of the Slovak Republic to Nicosia) and one

inspection started in 2020 (Central Visa Authority of the Ministry of the Interior of the Slovak Republic). Despite the fact that the Ministry of Foreign Affairs

The Slovak Republic approaches the implementation of the Schengen "acquis" with a high degree of responsibility,

The inspection of two embassies revealed less serious shortcomings in the area

specific safety standards, as a result of which these inspections have been completed

protocol on control. Execution of the remaining two inspections completed by the inspection record

(Consular Department of the Ministry of Foreign Affairs of the Slovak Republic and the Central Visa Authority of the Ministry of the Interior of the Slovak Republic) none were found

shortcomings.

### 7.3.2

Control of the processing activities of a targeted trading company

e-marketing and sales of wild berries

The subject of control of the processing activities of a trading company dealing with targeted

e-marketing and sale of forest fruits was to check the procedures of the inspected person

related to its legal contact database, which was to be used

for targeted marketing. During the inspection it was found that in the databases of the inspected person

they also find personal data of natural persons, which puts the inspected person in a position

operator within the meaning of the Regulation. Another activity of the inspected person was the sale of forestry

which was also associated with the collection and further processing of personal data. Not even

in one of the above cases, the inspected person has not demonstrated the compliance of its processing plants

activities with the requirements of the Regulation, as the persons concerned at the time of obtaining their personal

did not provide the information defined in Article 13 of the Regulation and in breach of the principle of proportionality

data minimization did not address the retention period of personal data either. Subject

the inspection was terminated by an inspection report stating a breach of duty



when processing personal data.

### 7.3.3

Control of the processing activities of a trading company engaged in  
deratization

He carried out an inspection of the processing activities of the deratization company

Office in the framework of personal data protection proceedings. The inspection focused on the principles of processing personal data, lawfulness of processing, fulfillment of the information obligation of the controller towards the data subject, the keeping of records of processing activities and the security of processing personal data within the meaning of the Regulation. In relation to the wording of Article 6 para. 1 letter f) Regulations the inspected person has not demonstrated during the inspection that his or her legitimate interests outweigh the interests or fundamental rights and freedoms of the person concerned which require protection personal data (proportionality test), at the same time did not prove that the retention period of personal data designated by the controlled person is necessary to fulfill the purpose of the processing (controlled data) in addition, the person kept the personal data for a longer period than he / she determined), and the data subjects provided only some of the information, the full scope of which

Article 13 1 and 2 of the Regulation. The inspection was terminated by the inspection protocol

27

### 7.3.4

Control of the processing of personal data in a sports association, which is a civic association  
association

One of the inspections that the Office completed in 2020 was the inspection of personal data processing in a sports association, which is a civic association. The subject of the inspection was the conformity of processing personal data with the requirements of the Regulation in the processing of personal data of the persons concerned. The inspection was focused on the processing of personal data of those interested in membership in the union and members union. The inspected person obtained the personal data of the persons concerned through the application, which also required a photograph of the applicant for membership in the association. The inspected person subsequently

through its website it published a list of its members, including the so-called

an electronic registration card which contained personal data, including a photograph (at the time of electronic registration cards have already been published without a photograph).

The inspection revealed that the person concerned did not have the opportunity to agree or disagree with processing of personal data for the individual purposes of personal data processing and were not provided or unambiguous information on the legal basis of the processing according to the purpose of the processing. At the same time, the inspection found that the inspected person did not meet the condition arising from the article 7 of the Regulation by failing to inform the persons concerned of the possibility of consent prior to granting consent revoke at any time. The audit also found errors related to the provision of information, which the inspected person was obliged to provide to the persons concerned in obtaining their personal data data. Based on the identified deficiencies, the inspection was terminated by the inspection protocol.

#### 7.3.5

Control of the processing of personal data of the data subjects by the controller who:

is a healthcare provider in the field of aesthetic and plastic surgery  
and corrective dermatology

In 2020, the Office checked the processing of personal data of the persons concerned by the operator, which is a healthcare provider in the field of aesthetic-plastic surgery and corrective dermatology, where all procedures (including surgical procedures) are performed on based on the client's request and paid for by the client himself. Personal data of their clients the operator processes them autonomously and does not systematically provide them to any other medical facility or any health insurance company; the only exception is medical laboratory for diagnostic purposes in case of histological examination of a sample taken from the client.

The client's personal data are processed by the operator for the purpose of performing medical procedures as personal data necessary to fulfill the legal obligation of the controller and are processed to the extent that medical records are processed in the provision of healthcare on the basis of the Health Care Act. Data processed for the purpose of providing

healthcare are health-related data, ie a special category of personal data data; the inspection did not reveal any processing of health data other than by law defined purposes. However, the inspection revealed that the operator in obtaining personal data provided to potential clients through an online form on its website outdated information on the rights of the persons concerned, using a single, universal one e-mail address for two different purposes (communication with the public and exercise of rights persons concerned). Based on the identified deficiencies, the inspection was terminated by a protocol on control.

### 7.3.6

Control of the operator (legal entity) who performs the guard service

The subject of control of the operator (legal entity) performing the guard service was compliance of the processing of personal data of the data subjects by the camera system with the requirements Regulations with an emphasis on verifying the processing of personal data of employees for the purpose of the so-called control mechanism of the employer according to the Labor Code. The person inspected had several IP cameras, recording equipment and output display units in operation. Control

28

In carrying out the inspection, the authority focused mainly on the principles of personal data processing, legality processing of personal data, information to be provided in the collection of personal data data from the data subject and the security of the processing of personal data. Personal processing staff data through a camera system for the purpose of the control mechanism employer was presented by the inspected person as his legitimate interest in accordance with Art. 6 para. 1 letter f) Regulations arising from its authorization pursuant to a special law (§ 13 par. 4 Labor Code). However, during the inspection, the inspected person does not in any way (e.g. proportionality test) has not demonstrated that its legitimate interests outweigh the interests of or fundamental rights and freedoms of the persons concerned (own employees). Legal basis processing of personal data of employees for the purpose of the control mechanism was in various

documents submitted by the audited entity formulated differently (once as a legitimate interest, other than § 13 par. 4 of the Labor Code), ie from the point of view of the persons concerned (employees) misleading, non-transparent. At the same time, the inspected person was found to be the inspected person one camera processes employees' personal data to an unreasonable extent (above the scope of necessary to achieve the purpose of the processing), that is to say, in breach of Article 5 (1) 1 letter c) Regulations (data minimization principle). The inspection authorities also found that the inspected person acts in breach of Article 5 para. 1 letter (e) Regulations (principle retention minimization) by retaining the personal data of the persons concerned (employees) after longer than is necessary to achieve the intended purpose. Based on the findings deficiencies, the inspection was terminated by the inspection protocol.

#### 7.3.7

Control in a trading company mainly engaged in providing targeted advertising and population analysis

The Office carried out on the basis of a suspected breach of personal data processing obligations control in a commercial company mainly engaged in the provision of targeted advertising and creating population analyzes. Initiative to verify the lawfulness of the processing of personal data was delivered to the office by a journalist who was interested in one of the audited person's population analyzes.

The inspection focused on the area related to the processing of the location data concerned persons by tracking the location of SIM cards, the purpose of which was to determine the number population migrating for work outside the district or county. This analysis of population movements performed by the inspected person on the basis of an order from another entity that wanted the results of the analysis use in traffic planning. The inspected person created an analysis of population migration within a period of two weeks, on the basis of the data provided to it telecommunications operators under concluded contracts. The data was provided controlled to a person in a form which did not allow their reassignment to the particular person concerned.

The inspection, which did not reveal any non-compliance with the Regulation, was terminated by an inspection record.

### 7.3.8

#### Control of camera systems operated by natural persons

The Office also deals with the processing of personal data of the persons concerned via camera systems operated by natural persons. In the specific case, at the initiative of the inspection it turned out that the inspected (natural) person also monitors the premises he does not own, as a result which cannot be explicitly domestic or personal activities of the natural person to whom the regulation applies does not apply. However, the inspected person declared during the inspection and subsequently also proved that it is a non-functional imitation (dummy) of the camera, as a result of which there is no to any processing of personal data. The inspection was completed by the inspection record.

However, in relation to CCTV systems operated by individuals, it is desirable point out that to monitor one's own home (such as a family house) in many cases may not be exempted from the scope of the Regulation under Article 2 (1). 2 letter c) (processing of personal data in the framework of exclusively personal or domestic activities) on the grounds that

29

the camera system in question even partially monitors the real estate of another person (for example land or neighbor's family house) or public space (for example, part of a street). In such In some cases, the natural person operating the camera system also acquires the status operator, as a result of which it is fully covered by all obligations resulting from the Regulation.

30

#### 8 PERSONAL DATA PROTECTION PROCEDURE

The purpose of personal data protection proceedings is to determine whether the rights of natural persons have been violated during processing of their personal data or there has been a violation of the provisions of the Regulation or the law, and, if justified and appropriate, to remedy the deficiencies, if necessary fine. The provisions of the Administrative Procedure Code apply to personal data protection proceedings.

If the competence of the Office to act and the decision in the case is not given, the Office is obliged to file it forward to the competent administrative authority. In the monitored period, the Office forwarded a total of 34 submissions another competent administrative body for action and decision.

Personal data protection legislation allows the Office to file in an exhaustive manner postponed in certain cases. The Office had to proceed with the postponement of the application in his case unfoundedness, if the matter to which the application relates was heard by a criminal authority proceedings, if the applicant has not provided the Office with the necessary cooperation at its request, without his active participation, it was not possible to settle the matter and, if, since the event to which the more than three years have elapsed on the day of its delivery. The most common reason for the postponement was the unfoundedness of the application, when it was already clear from the evidence submitted, in particular by the person concerned, that there has been no breach of personal data protection law. In the monitored a total of 289 submissions were postponed during the period.

The Office, in the framework of supervisory activities, conducts proceedings on the protection of personal data in order to protect rights individuals against unauthorized interference with their private life in the processing of them personal data, while also examining compliance with the obligations laid down in the Regulation and the law. If it finds that the rights of the data subject have been infringed or that there have been no processing obligations personal data, by decision, if justified and expedient, impose on the controller or the intermediary to take measures to remedy the deficiencies and causes within a specified period or, depending in particular on the gravity of the infringement found, impose a fine. Otherwise, it will stop the personal data protection proceedings.

The personal data protection procedure is initiated on the proposal of the petitioner or on his own initiative office. Proceedings on the Office's own initiative are initiated on the basis of an initiative, on the basis of results inspections which revealed deficiencies or on the basis of the Office's own findings on suspected breaches of personal data protection legislation, such as proceedings

started without a proposal.

In the period under review, the Office initiated a total of 219 administrative proceedings, of which 138 were initiated at proposal of the person concerned, 57 initiated on the basis of the initiative, 16 initiated on the basis of the results shortcomings were identified and 8 proceedings were conducted by the Office on its own initiative suspected breaches of personal data protection law.

Overview of the methods of initiating proceedings within the period under review

Year

2020

Based on

proposal

138

Based on

initiative

57

Based on

inspection results

From my own

initiatives of the Office

16

8

Decision of the Office, as the administrative body at first instance in personal data protection proceedings, it is based on a reliably ascertained state of affairs. For this purpose, the Office is in proceedings for the protection of personal data

authorized to request the co-operation of anyone, and the Office requested it during the period under review for cooperation a total of 972 times. In personal data protection proceedings, there have been three cases where

the entity from which the co-operation was requested did not respond to it and the Office even after being called upon to comply

did not cooperate (in these cases proceedings were initiated against the entities on a fine or a disciplinary fine).

In connection with raising awareness of personal data protection among the public, the cases, resp.

the results of the proceedings were often also of interest to the media. The Institute of Legal Representation was evaluated used in a significant number of cases, with the exception of cases where all the parties were represented by lawyers.

The most common subject of personal data protection proceedings was the examination or processing personal data of the data subjects in the information system of which the cameras were there has been no breach of personal data protection law.

One of the most common violations was the processing of personal data in breach of the principle of non-discrimination legality, when personal data was processed without a legal basis, resp.

contrary to the legal basis and processing contrary to the principles of integrity and confidentiality, which related to the failure to take appropriate security measures.

32

## 9 COOPERATION AND CONSISTENCY MECHANISM

The functioning of the internal market requires that the free movement of personal data within the Union is not impeded restricted or prohibited, not even for reasons related to the protection of individuals during processing personal data, which is also reflected in the provisions of Art. 1 par. 3 Regulations. To that Regulation responds by establishing cooperation and consistency mechanisms to ensure consistency and a similarly high level of personal data protection in each Member State, regardless of place of residence of the person concerned.

### 9.1 Cooperation mechanism

The Regulation regulates cooperation between supervisory authorities, whether the need for mutual cooperation will arise in the framework of the investigation of a specific breach of personal data protection



data or other activities of the supervisory authority (eg addressing legal issues, providing consultations). Given that the rules of cooperation are regulated directly by Regulation, no further specific agreements are required between Member States for this purpose.

#### 9.1.1

##### Cross - border processing

Pursuant to Art. 55 of the Regulation, each supervisory authority performs the tasks and exercises the powers published by regulation in the territory of its State. However, the regulation also specifically regulates the procedure and jurisdiction in proceedings for the cross-border processing of personal data. Cross-border processing makes sense in Art. 4 pt. 23 of the Regulation (a) the processing of personal data which takes place in the Union in context of activities of the operator's or intermediary's premises in more than one Member State where the operator or intermediary is established in more than one Member State; or (b) the processing of personal data which takes place in the Union in the context of a single activity where the establishment of an operator or intermediary in the Union but which significantly affects it or likely to significantly affect the persons concerned in more than one Member State.

The regulation governs cooperation between supervisory authorities, in particular in relation to the mechanism of a single contact point (so-called one-stop-shop) regulated in Art. 56 par. 1. Regulations under which the supervisory authority is the main establishment or the sole establishment of the operator or intermediary authorized to act as lead supervisory authority for cross-border processing carried out by that operator or intermediary.

According to Art. 56 par. 2 of the Regulation, each supervisory authority is competent to deal with a complaint or possible infringement of the Regulation, if the facts concern only an establishment in its Member State or significantly affects the persons concerned only in its own Member State. In accordance with Art. 4 point 22 of the Regulation other supervisory authorities will be for this processing in the positions of the supervisory authorities concerned, if (a) the controller; or the intermediary is established in the territory of the Member State of that supervisory authority; (b) the persons concerned

resident in the Member State of that supervisory authority are significantly affected or will be significantly affected likely to be significantly affected by processing; or (c) the complaint has been lodged with that supervisory authority authority.

The designation of the lead supervisor and the authorities concerned is done in IMI

(Internal Market Informational System), within which

the exchange of information on specific processing takes place between the different supervisory authorities

and a specific suspicion of a breach of personal data protection, resp. if the investigation

started on the basis of a complaint from the person concerned as well as the content of that particular complaint. Exchange information is in English.

33

During the period under review, the Office received 726 identification notifications in IMI

the head and the supervisory authority concerned. Based on a careful assessment of every single thing

assessed that it was the supervisory authority concerned in 154 cases; most often for reasons that

the processing of personal data in question significantly affects or is likely to significantly affect

will affect the affected persons residing in the territory of the Slovak Republic. It went most often

on social network operators, airlines, fitness center operators,

companies providing online games, various e-shops, etc. In some cases, the office was affected

also due to the fact that the operator or intermediary is established in the territory of the Slovak Republic,

ie. has one or more establishments in the territory of the Slovak Republic. If the Office evaluated that

is the supervisory authority concerned, identified this in IMI and followed up the case. In accordance with Art.

60 of the Regulation, the Office had the opportunity to comment on the requests of the Chief Supervisor as required

authority, its procedure and the results of the investigation, as well as to comment on draft decisions.

If the Office is the supervisory authority concerned because it has received a complaint, the Office

would act as a contact point for the person concerned and would notify the manager's decision

supervisory authority.

A total of 39 submissions containing elements were received by the Office during the period under review

cross-border processing and 11 notifications of personal data breaches, so-called data breach.

These submissions were either delivered from foreign persons or directed against foreign ones

operators, including, for example, to operators established in the USA, the Czech Republic

Republic or Ireland. Within each filed submission, the Office first examined (so - called

preliminary examination of the complaint) whether the subject of the application meets the requirements of the application,

resp. initiative

according to § 100 par. 3 of the Act and also whether it meets the conditions for cross-border processing according to Art. 4

point 23 of the Regulation, resp. whether the definition according to Art. 56 par. 2 Regulations. If the subject

filing a reasonable suspicion of a personal data breach, the Office stated

shall also verify the allegations in cooperation with the supervisory authority of the Member State in whose territory

the operator had a principal or sole establishment. In 10 cases, the Office entered the received

IMI submissions and further dealt with them in cooperation with the supervisory authorities that were

processing by the lead supervisory authority. The Office forwarded these complaints via

IMI system to Ireland, Hungary, Sweden, Luxembourg and the Office forwarded three complaints to the

supervisory authority. The Office was designated as the leading supervisory body during the period under review

in 4 cases, based on the location of the operator's headquarters, these complaints

came from citizens of Austria (a total of 3 complaints) and one complaint was lodged by a Slovak citizen

living in Germany.

#### 9.1.2

##### Mutual help

The Office also cooperates with other supervisory bodies outside the one-stop-shop mechanism. This

cooperation also takes place in IMI, which allows specific requests to be sent

selected supervisory authority. However, the Office also continuously handles email or written requests

other supervisory authorities.

During the reporting period, the Authority received 43 requests from other supervisors in IMI

for cooperation within the meaning of Art. 61 Regulations. In the requests in question, the supervisory authorities requested the

Office

for its legal opinion, in particular as regards the interpretation of the provisions of the Regulation. The requests concerned e.g. interpretation of individual provisions, the legal basis for the processing of personal data, responsible persons, the coherence of the Regulation and national protection rules personal data, ascertaining the receipt of a specific complaint, the interpretation of Art. 10 Regulations, scope Regulations on religious societies, processing of personal data during a pandemic, recovery artificial intelligence in the work environment, processing of a special category of personal data, the tasks of the external responsible person, biometric data, the method of handling the complaint, etc.

34

In this way, some supervisory authorities informed the Office of the notification of the infringement received protection of personal data or have used this method to consult a specific case before by launching a one-stop-shop mechanism.

During the period under review, the Office sent 12 requests for cooperation in IMI pursuant to Art. 61 Regulations. The requests concerned information on specific cross-border cases, consultations individual cases or the legal opinion of other supervisory authorities on interpretation Regulations. For example, the Office asked other supervisory authorities about the interpretation of Art. 2 par. 2 letter c) Regulations, deadlines for cameras that capture public space, identification operator, resp. provider of the Internet domain, territorial scope in connection with codes of conduct. The Authority has also asked other supervisory authorities to cooperate, for example also in connection with the interpretation of Art. 18 par. 1 letter d) Regulations or responsibilities of the responsible person persons. The Office also used other forms for mutual cooperation with other supervisory authorities communications such as IMI (email, written and telephone communications) in which it used contacts acquired in the course of its activities, including contacts acquired under the membership of the Committee's expert groups.

9.1.3

Joint supervisory operations

Under the cooperation mechanism, pursuant to Art. 62 Regulations may also carry out joint operations supervisory authorities in the field of joint investigations and joint actions in the field enforcement. During the period under review, the Office did not initiate or accept a request for the implementation of such joint operations of supervisory authorities.

## 9.2 Consistency mechanism

An important attribute of the Regulation is its consistent application. In order to achieve this objective, The Regulation provides for a consistency mechanism, which can be understood as cooperation between EEA supervisory authorities and, where appropriate, the EC.

### 9.2.1

#### EDPB opinion

The purpose of Article 64 of the Regulation is for the EDPB to issue an opinion in cases where the competent supervisory authority

the authority plans to take specific measures. To that end, the supervisory authority should notify the EDPB of its draft decision. The Regulation regulates cases where the supervisory authority is obliged to apply to the EDPB for an opinion (Article 64 (1) of the Regulation) and when it has the opportunity to request an opinion (Article 64 (2) of the Regulation)

Regulations). The Authority did not request an opinion from EDPB during the period under review.

### 9.2.2

#### EDPB Dispute Resolution

Dispute resolution The EDPB allows for binding decisions to ensure consistency application of the Regulation in the following cases:

- ☐ The relevant reasoned objection was raised by the supervisory authority concerned or rejected by the lead supervisory authority (Article 60 of the Regulation);
- ☐ Disagreement with the appointment of the head of the supervisory body (Article 56 of the Regulation);
- ☐ Absence of consultation of the EDPB (Article 64 of the Regulation);
- ☐ The Authority did not follow the opinion of the EDPB (Article 64 of the Regulation).

EDPB did not resolve any dispute during the period under review.

35

### 9.2.3

#### Emergency procedure

Article 66 of the Regulation provides for an urgency procedure. In exceptional in cases where the supervisory authority concerned considers it urgent to protect rights and freedoms concerned, it may take interim measures having legal effect in its territory. Validity these measures may not exceed three months. In this case, the supervisory authority concerned is concerned obliged to inform the other supervisory authorities, the EDPB and the EC.

If the Authority considers that definitive action is needed urgently, it may request it EDPB for an urgent opinion or an urgent binding decision. Each supervisory authority may request an urgent opinion or a binding decision from the EDPB in cases where the competent authority the supervisory authority has not taken appropriate action and there is an urgent need for action. In the evaluated period, the Office did not apply this article.

36

## 10 SANCTATION

Sanctions for violations of the Regulation and the law are fines and disciplinary fines. Sanctions are in place optional legal standards, ie. that not every detected violation has to be done automatically result in the imposition of a sanction. The Office imposes fines and disciplinary fines depending on the circumstances each individual case. When deciding on the imposition of a fine and determining its amount taking into account, in particular, the nature, gravity and duration of the infringement, the number of persons concerned, the extent of the damage, if any, the possible breach of personal data protection and the measures taken to mitigate the damage suffered by the persons concerned. The Office also takes into account the previous ones breaches of personal data protection, the degree of co-operation with the Office in rectifying breaches and mitigating them possible adverse consequences of the breach, the category of personal data to be breached

and the way in which the Office learned of the personal data breach.

10.1 Fine

In the monitored period, the Office for violation of legislation on personal data protection imposed 54 fines in the aggregate amount of EUR 103,300. In the period under review, the Office selected fines totaling 126 432 euros. The average fine was EUR 1,913. The lowest fine in the amount of EUR 300, the Office imposed on the operator in connection with the unauthorized disclosure of personal data data (in connection with a mandatory contract). The Office legally imposed the highest fine in the amount of EUR 20,000 to the operator for violating the principles of transparency and minimization storage.

Overview of fines imposed and collected in the monitored period

Watched

period

Count

fines

2020

54

Total height

Average height

Total selected on

legally

fines rounded to the nearest euro

fines imposed in Euros

whole Euro up

103 300

1 913

126 432

The fine, as a type of sanction, served a repressive as well as a preventive function in the period under review. At its imposition by the Office took into account, inter alia, the status of the entity and its activities, as well as possible the impact of the amount of the fine on its continued existence. In connection with the imposition of fines during the assessment

period for breaches of personal data protection legislation can be stated,

that the fines imposed did not have liquidating effects.

On the margin of the collection of fines, it should be noted that the revenue indicator was binding for 2020 for the office of the Ministry of Finance of the Slovak Republic determined in the amount of 81,778 EUR. Regarding with the pandemic situation was reduced to EUR 60,000 in July 2020. Because the office in the monitored period, he collected fines in the total amount of 126,432 euros, which he exceeded established revenue indicator.

## 10.2 Ordinary fine

The disciplinary fine serves to ensure a dignified and undisturbed course of supervisory activity office. The Office may impose a disciplinary fine on the operator or intermediary, where appropriate, to the operator's or intermediary's representative if he obstructs the inspection or if does not provide adequate conditions for its performance. The Office may also impose a disciplinary fine to a person who is not an operator or intermediary for failing to provide the requested

37

cooperation of the Office in the performance of supervision. In the period under review, the Office imposed two disciplinary fines

in the total amount of 2,500 euros, both for failure to cooperate.

## 10.3 Selected cases from the supervisory activities of the Office

### 10.3.1 Postponements

#### 10.3.1.1 Processing of personal data by a natural person

In 2020, the Office accepted the proposal of the affected person addressed to a natural person - an official the city police, which was supposed to violate the protection of personal data by sending documents containing



personal data of the data subject in the range of name, surname and signature of various branches. Office

After examining the application of the person concerned and the documents annexed to it, he found that he was not authorized not only to conduct personal data protection proceedings against an individual, but is not the same entitled to impose a fine on such a natural person. Authority of the Office to initiate protection proceedings personal data against entities (exhaustively) determined by law is defined in § 99

para. 3 of the Act (operator, intermediary, certification body, monitoring body),

whereas by law it is not possible for a natural person in personal data protection proceedings for breach of personal data protection rules and therefore fined the case. The office subsequently

the matter was resigned for assessment by the relevant part of the Police Force of the Ministry of the Interior

Of the Slovak Republic with suspicion that the case does not meet the factual elements of the crime

Unauthorized handling of personal data under the Criminal Code.

#### 10.3.1.2 Disclosure of personal data by the media

In 2020, the Office received several submissions in which applicants objected to the disclosure of personal data data of the persons concerned through the press or news reports broadcast on television and later available on the operators' websites. Based on the operator of the personal data published thus made it possible to identify the natural person.

In case

disclosure

personal

data

media

occurs

to meet

rights

protection of personal data with the right to freedom of expression and the right to information, both

represent fundamental rights in a democratic society. It follows from the Regulation that Member States

to harmonize the right to the protection of personal data and the right to liberty under national law speech and the right to information, including processing for journalistic purposes, and to provide for exceptions or derogations from certain chapters of the Regulation. Such national rules in the conditions Of the Slovak Republic is the law. In relation to the submissions in question, the Office found that when publishing personal data, the operators proceeded in accordance with § 78 par. 2 of the Act, according to whose controller may process personal data without the consent of the data subject, even if the processing of personal data is necessary for the needs of informing the public media and if personal data are processed by the controller to whom it is processed results from the subject of the activity. Operators process personal data of the persons concerned for the purposes of informing the public, it resulted from the subject of the activity. Operators are in the sense of the right to obtain truthful, timely and comprehensive information in order to obtain information to the public and are not responsible for the content of the information provided by the defined area persons. However, it is also true that operators by processing the personal data of the persons concerned on journalistic purposes according to § 78 par. 2 of the Act must not violate the right of the person concerned to protection her personality or the right to privacy. Assessment of fact or disclosure personal data of the persons concerned by means of communication for journalistic purposes the right to protection of the personality and privacy of the persons concerned has been infringed General Court (protection of the individual). In the case of disclosure of such personal data by the media, which could cause an unauthorized interference with the right to protection of the personality and privacy of the data subject, the data subject has the right to seek protection against

38

in court.

### 10.3.2 Procedures

#### 10.3.2.1 Jubilants - congratulations of the village on its life anniversary

In 2020, the Office adopted several proposals to initiate proceedings on personal data protection affected persons who have challenged the publication of personal data in the magazines of the municipalities in the sections

"Anniversary congratulations" in the name, surname, age of the person concerned, as well as in a section such as "Married, Married" in the scope of personal data name, surname, title and date of marriage of the person concerned. Office examining the case in the proceedings on the protection of personal data found that none of the operators against whom it has not proved that the personal data in question were processed on an appropriate legal basis pursuant to Art. 6 para. 1 of the Regulation, and therefore the Office assessed such conduct of the operator as contradictory with the basic principle of lawfulness of personal data processing according to Art. 5 par. 1 letter a) Regulations. Several controllers have claimed in the privacy proceedings that they are processing personal data for the purpose of congratulating the persons concerned in the magazine or on its website on the legal basis of Art. 6 par. 1 letter e) Regulations, or in the legitimate interest operator according to Art. 6 par. 1 letter f) Regulations, which, however, were not a correct statement. In order for the operator to proceed in accordance with Art. 6 par. 1 letter e) Regulations, would have to in the given in this case exist at the same time according to § 6 par. 3 of the Regulation provisions of a special law governing the legal authorization of the controller to process the personal data in question to the extent necessary to given purpose (for example, for the purposes of important life events of its citizens). None of the special laws used by municipalities, for example for the purposes of registry registration, population registration, or Act on Municipalities, however, this legal condition, resp. legal authority to process personal concerned for the above purpose. The Office also stated in this case that the municipality as an operator, it needs to have the legal basis for two processing operations with personal data, for the processing of personal data to a certain extent on the purpose of congratulating the inhabitants of the municipality and the processing operation of publishing personal data to a certain extent. Under the current legal status, the municipality is entitled to process personal data on this purpose on a legal basis, which is the consent of the person concerned under Art. 6 par. 1 letter (a) Regulations, namely: thus in relation to the acquisition of personal data from the population register or the register register by the municipality, as well as in relation to the publication of the data in question by the municipality in a general journal or on the web the seat of the municipality. The Office also found that the operators (municipalities) following the violation

At the same time, the principles of legality infringed the principle of limitation of the purpose of the processing of personal data under

Art. 5 par. 1 letter (b) Regulations where the personal data of the persons concerned have already been obtained on the basis of

a special regulation stipulating the specific purpose of obtaining personal data, they also used

to another, resp. another purpose, thereby exceeding the originally intended purpose of the processing of personal data, for which a fine was imposed on them.

10.3.2.2 Requiring a verified signature of the data subject in exercising his / her right to

access to personal data pursuant to Art. 15 Regulations

During the period under review, the Office accepted the person concerned's request for a breach of the right of access to personal data, as it has asserted its own with the financial service provider

the right of access to personal data, which subsequently referred her to a standardized form

"Request for the exercise of the rights of the data subject under the GDPR". This request showed that

the operator requires their verified signature when exercising the rights of the persons concerned. From the background

acquired in the proceedings on personal data protection, the Office expressed its non-compliance with Art. 12 par. 5 of the Regulation,

because the operator has requested the right of access from the person concerned for the purposes of exercising it verified signature, which, in accordance with Recitals 59, 63 of the Regulation, as well as Art. 12 par. 1 Regulations complained

by imposing conditions which were undoubtedly of a financial nature,

39

exercise of rights under the Regulation. The operator this disproportionate condition during

personal data protection proceedings, it was therefore not necessary to impose measures on

elimination of identified deficiencies.

10.3.2.3 Illegal collection of personal data by a financial institution for the purpose of addressing

persons concerned with an offer of financial intermediation or advice

During the period under review, the Authority accepted the proposal of the person concerned who claimed that the operator (financial institution) without its legal basis processes its personal data to the extent of name, surname, telephone number, the specific product, so that the authorized person of the operator by telephone contacted in order to submit a call or an offer of financial intermediation, or financial advice. The Office found from the documents obtained that the person concerned had never been the operator's client, as confirmed by the operator itself. However, the operator stated that processed the personal data of the data subject on the legal basis of his or her legitimate interest, namely purposes of direct marketing according to Art. 6 par. 1 letter (f) Regulations, also referring to Recital 47 of the Regulation. With these claims of the operator and his determination of the legal basis However, the Office did not identify a legitimate interest because, as stated in Recital 47 of the Regulation, the which, incidentally, the operator himself has pointed out, the legitimate interest of the operator as the legal basis for the processing of personal data can only exist if they exist reasonable expectations of the person concerned based on their relationship with the operator, such a legitimate interest of the operator could exist, for example, if between the parties concerned there was a relevant and reasonable relationship between the person and the operator (the person concerned in the client's position vis-à-vis the operator or in its services), which, however, in the given case was not met. As the petitioner has never been a client of the operator, moreover alone confirmed by the operator, ie that he does not register any contract with the proposer in the databases, the person concerned (the petitioner) could reasonably never have expected such processing, resp. contact by the operator's subordinate financial agent.

For this reason, the Office alleged a violation of the principle of legality of personal data processing according to Art. 5 par. 1 letter (a) Regulations, as the operator has not shown in the proceedings that he has adequate legal basis for the processing of personal data pursuant to Art. 6 par. 1 Regulations on for this purpose and imposed a fine on the operator.

#### 10.3.2.4 Publication of birth numbers of applicants for study in the results list

The Office accepted the complaint of a natural person against the operator, which was the school. According to its content

and the attached evidence, the school should have published the results on its official website order from the admission procedure for the school year 2020/2021 ranking, points and birth numbers applicants for a four-year study at school. The Office examined the school's website to find that the given result list with birth numbers is no longer published. However, the Office the facts set out in the complaint and the accompanying evidence began against the school as to the operator on his own initiative. The Office investigated the case in question written cooperation with the school. According to § 78 par. 4 last sentence of the law applies to publish a universally applicable identifier is prohibited; this does not apply if the universally applicable identifier published by the person concerned. Section 78 of the Act supplements the special processing rules personal data provided for in the Regulation. Specifically, it is also a special processing arrangement national identification number, namely the generally applicable identifier which is currently time in the Slovak Republic birth number of a natural person. The office had found the school as the operator processed in his information system the birth numbers of natural persons - applicants for a four-year study for the school year 2020/2021 for the purposes of the admission procedure, which was authorized to process, following the operator's procedure in announcing the results the birth numbers were published in the results list on its website page. The publication of birth numbers was stopped on the operator's own initiative

40

before the commencement of the proceedings. In view of this finding of the end of the publication of birth numbers and ensuring compliance with the law, as well as the circumstances surrounding this one-off procedure operator in identifying candidates on the basis of their birth numbers (lack of time for distribution of identification codes for study applicants with regard to the situation that has arisen pandemic COVID-19) the Authority did not impose corrective measures on the operator. However, the Office to the operator for violation of the provisions of § 78 par. 4 of the Act when publishing birth numbers imposed a fine on the persons concerned.

10.3.2.5 Requiring the employee's consent to the processing of personal data at work

contracts

The Office accepted the person's proposal against the operator, which was the employer the person concerned. The person concerned had an employment relationship with the operator, and argued that the controller requires her to consent to the processing of personal data directly in the employment contract. The data subject considered that requiring consent to his processing personal data when concluding an employment contract is in this case contrary to the Regulation. Office at Based on the assessment of the proposal and the attached employment contract, he initiated proceedings against the operator. Office the case was investigated in writing. The Office found in the investigation that the petitioner had an employment contract concluded with the operator for the effectiveness of the Regulation and personal data of the petitioner were processed for the purposes of the personnel and payroll agenda. Legal basis processing of the petitioner's personal data in the conclusion of employment and fulfillment of obligations resulting from the employment contract was not the consent of the person concerned within the meaning of Art. 4 par. 11 Regulations in conjunction with Art. 7 Regulations. In this particular case, the employment contract should not have included a statement of the employee's consent as the data subject, as the legal basis for the processing was performance of the contract (employment contract) or legal obligation (special laws). The Office also found that even the form of consent was given in the declaration, as the consent was not given free (there was no free choice to give or not to give consent). The operator 's procedure by: the employment contract with the employee contained his statement of consent to processing personal data by an employer who, on the one hand, was not obtained freely or was appropriate legal basis for the processing of the claimant's personal data for the purposes of the conclusion employment contract, there was a violation of the principle of legality under Art. 5 par. 1 letter (a) Regulations. Based on the findings, the Office imposed a corrective measure on compliance with the operator which the operator has informed the Authority in writing within the specified time limit.

10.3.2.6 Breach of confidentiality of personal data of the operator's clients

The Office, as the supervisory body, received a notification of a personal data protection violation pursuant to Art. 33 Regulations

responsible person of the operator. The Office had proven that there was a breach of personal protection operator's client data. The operator's notification contained all the Regulations

the requisites and the breach of personal data protection were notified to the Office within 72 hours. from his findings. The confidentiality of personal data pursuant to Art. 5 par. 1

letter f) Regulations by giving unauthorized access to the personal data of the data subjects

third parties who should not have access to them. These were the personal data of the persons concerned to the extent name, surname, address, gender, email, times and dates of flight connections, ie. about a common category

personal data. The Office did not find that the infringement also concerned a specific category of personal considered to be sensitive personal data and no breach of integrity or breach has been identified

availability of personal data. The operator proved that he had received before the incident

security measures to prevent this type of security incident, but in a specific

Insufficient compliance with the measures taken should have led to a human factor failure.

The operator informed the persons concerned about the occurrence of the incident in accordance with Art. 34 Regulations.

Office at

based on the assessment of the collected documents, he assessed that there was no reason to impose corrective ones measures, as the operator has complied with Art. 33 and Art. 34 Notification regulations

41

privacy violations, incident investigated, documented, accepted technical

and organizational measures to prevent recurrence of the infringement in the future as well as measures to mitigation of potential adverse consequences for the persons concerned. Office in this particular

in breach of the principle of confidentiality of the personal data of the persons concerned

fine.

10.3.2.7 Processing of personal data for the purpose of debt recovery and exercise of the right to erasure

personal data



The Office accepted the person's proposal against the operator with whom the person concerned previously concluded loan agreement. The operator contacted the person concerned in connection with the waiver of part of the debt. The data subject objected that the controller was not authorized to process it personal data for the purpose of recovering the amount due in its view. The Office found that the operator, as a creditor, asserts a claim against the person concerned and processes it in that context her personal data which are necessary for the performance of the contract. The operator had to obtain personal data for a specifically and explicitly stated legitimate purpose. As the case concerned a contractual dispute relationship between the operator and the affected person, which is not according to § 81 par. 5 of the Act subject to personal data protection supervision and whose negotiation and decision-making they are competent courts or other authorities under special regulations, the Office of the person concerned in this section postponed as manifestly unfounded. However, the Office initiated proceedings against the operator in part of the proposal, in which the person concerned objected that he had not received a reply to his request from the operator on the deletion of personal data. According to Art. 17 Regulations right to achieve the deletion of personal data concerning the operator without undue delay and the operator is obliged to delete them without undue delay if any of the the six reasons set out in Art. 17 par. 1 of the Regulation. The operator of the Office with respect to the period delivery of the application of the person concerned (March 2020) pointed to Act no. 62/2020 Coll. about some emergency measures in relation to the spread of dangerous contagious human disease COVID-19 and in the judiciary and amending certain laws (zákon Law No 62/2020 '). Z. z. "), According to which the deadlines do not run from the date of entry into force of this Act until 30 April 2020. In connection with the situation, the operator did not send the person concerned a notification within 30 days. Due to the fact that the controller processed the personal data of the data subject person due to the existence of the claim, was obliged to promptly and at the latest within one month from the request of the person concerned, to inform him in particular of the reasons for non-action. From the adjustment Act no. 62/2020 Coll., Nor did it follow from the explanatory memorandum to this Act that should concern the suspension of the time limits laid down in the Regulation in Art. 12 in connection with the procedure

operator in processing the requests of the persons concerned. The Office stated in the given case breach of the principle of transparency under Art. 5 par. 1 letter a) Regulations to operators by that in processing a request from the data subject for the erasure of personal data concerning him or her electronically, did not proceed in the manner and within the time limit pursuant to Art. 12 Regulations. Because of that the operator processed the request of the person concerned during the proceedings and also took measures for ensuring compliance with Art. 12 Regulations for communication with the persons concerned, corrective office did not impose the measure on the operator.

#### 10.3.2.8 Publication of the name and surname for the purpose of text authorization

The Office conducted personal data protection proceedings on the basis of a petition lodged by the petitioner processing of his name and surname by his employer so that he the job email was placed on the proposers by a notice formulated as if it were a notice the petitioner and terminated by the petitioner's name and surname. The operator justified the procedure was intended to ensure the organization and use of the proposer name and surname was based on the provisions of § 78 par. 3 of the Act, which allows the employer to provide the name and surname of the staff member, if necessary in connection with the performance of his staff

42

job responsibilities. The Office stated that § 78 par. 3 of the Act does not entitle the employer to without the employee's knowledge and consent, publish his name and surname for the purposes of text authorization, whose employee is not the originator and does not express his will or interest, such processing personal data is contrary to the fundamental principles of justice and transparency and cannot meet no condition of lawful processing according to Art. 6 par. 1 Regulations, as well as purpose the functioning of the organization monitored by the content of the notification could be achieved in this case without processing of the personal data of the applicant. The Office found that the operator by processing the name and surname of the petitioner, as the subject of the petition, violated the principles justice, transparency and legality under Art. 5 par. 1 letter (a) Regulations and decisions imposed corrective action on the operator.

#### 10.3.2.9 Publication of the interior of the applicant's dwelling

The Office conducted a personal data protection procedure on the basis of a petition where the petitioner objected that the police force provided the media in connection with the information about the burglary to the petitioner's apartment also a photograph of the crime scene where the interior was thus published the applicant's residence. The operator stated that the photograph of the residential interior itself was provided by the media and subsequently published without identification data the petitioner and is therefore not personal data, the purpose of which was to provide prevention crime. The Office shall, on the basis of an assessment of the full set of information provided and published together with the photograph, stated that, using this information, the petitioner was physical the person to whom the apartment in the photo belongs, reliably identifiable for a certain group of people, and thus the photograph of the residential interior was, in the present case, personal data concerning the petitioner. At the same time, the Office stated that there was no such interference in the purpose of crime prevention the petitioner's privacy, such as the view of his residence, necessary or necessary and the operator by providing the photograph of the residential interior capturing the portrait (photo) of the injured party (the petitioner) violated the principle by the media data minimization according to § 8 of the Act.

43

#### REMEDIES AND DECISION-MAKING

Against the decision of the Office in the matter of personal data protection proceedings, as well as against the decision on non-disclosure of information resp. a decision not to disclose the information may be made in part ordinary remedy - dismissal, while the provisions on remedies apply in the alternative provided for in the Administrative Procedure Code. The chairwoman decides on the submitted appeals of the Office, after its dismissal, the Vice-President of the Office decides on them on the basis of the appellate's recommendations the appellant may extend or supplement the appeal points only within the time limit set for filing an appeal, i.e. within 15 days of the date of notification of the decision.

The President, later the Vice-President of the Office, was presented with 51 during the reporting period appeals. During the period under review, it ruled in 38 cases as an appeal authority. Also in the monitored period, 5 more decisions on the dissolution were issued, when there was a dissolution submitted to the President of the Office for a decision in 2019. Within the monitored period there was one review of the decision outside the appeal proceedings. Together in the following 44 decisions were issued by the appellate body during the period.

Of these, in 24 cases the amount of the fine was also subject to decision; in 4 cases it occurred reduction, in 10 cases the fine imposed by the decision was confirmed, in the remaining 10 cases the case was referred back to the first instance body for a fresh decision.

In the remaining 20 cases, in 8 decisions were decided on the legitimacy of the termination of the protection proceedings personal data, while in 3 cases the suspension of the proceedings was confirmed, in 5 cases it was a matter returned for a re-decision.

In 4 cases, the decision on non-disclosure was the subject of a decision on dissolution / non-disclosure of information in part in accordance with Act no. 211/2000 Coll .; in all cases confirmed the decision.

In the remaining 8 appeal proceedings, these were proceedings where they were imposed by the first instance authority remedial action only; by decision on appeal, 4 cases were returned for re - decision in cases, in 2 cases the imposed measures were confirmed by the decision on dissolution, in two cases they were the decision has changed.

A party to the administrative proceedings may, against a valid decision of the President of the Office and from 29.04.2020 after her appeal, against the valid decision of the Vice-President of the Office, to file an action for review of the legality of the decision within two months of its notification.

Within the scope of material and local jurisdiction, the Regional Court in Bratislava has jurisdiction over the proceedings.

In the monitored period, 5 lawsuits were filed with the Regional Court in Bratislava for review legality of the Office's decisions, the Office commented on all of them upon request (file no .: 2S / 225/2020, 2S / 159/2020, 6S / 79/2020, 5S / 30/2020, 6S / 3/2020). Three were also issued during the period under review

judgments in the matter of reviewing the legality of the Office's decisions, two were issued by the Regional Court in Bratislava (file no. : 1S / 243/2017, 2S / 124/201) and one was issued by the District Court in Žilina (file no. : 2C / 71/2019).

The Regional Court in Bratislava decides on an administrative action by a judgment against which they can parties to an administrative proceeding to lodge a cassation complaint. The Supreme Court of the Slovak Republic, as a court of cassation, it examines the judgment as well as the proceedings on the basis of the filed cassation complaint the regional court that issued it.

In the period under review, the Office provided 2 comments on filed cassation complaints in the proceedings held at the Regional Court in Bratislava (file no. : 2S / 141/2018, 2S / 43/2017). In court proceedings conducted at the Regional Court in Bratislava under file no. file number: 6S / 96/2019 is also filed for cassation complaint.

44

12 EUROPEAN

AND INTERNATIONAL

PROTECTION OF PERSONAL DATA

LEGISLATIVE

PACKAGE

12.1 Legislative process at EU level

On 10 January 2017, the EC submitted a proposal for a regulation on respect for privacy and protection personal data in electronic communications and repealing Directive 2002/58 / EC (Directive on privacy and electronic communications) in order to ensure consistency with the common approach to protect personal data throughout the EU. The draft e-privacy regulation will be in relation to the Regulation lex specialis. For this reason, the Office is co-responsible in the legislative process of adopting the proposal e-privacy regulations at European level. The aim of the draft e-privacy regulation is to ensure strict privacy rules for users of electronic communications services and a level playing field for all market participants. Electronic communications data understands their content, such as the content of private messages, but also metadata, which includes e.g.

numbers called, websites visited, geographical location, time of the call or

news.

The European Parliament adopted its opinion on the draft e-privacy regulation on 26 October 2017.

At the same time, negotiations took place between the representatives of the individual states in the Council of the EU, which, however, did not

did not reach a joint agreement on the text during the period under review. Croatian and German Presidencies

At the end of their term in 2020, the EU Councils presented a progress report. This

the report points to the efforts of both countries to offer solutions to problematic issues in the proposal

e-privacy regulations. This is, for example, the creation of new reasons for which it will be possible to process

electronic communications data such as legitimate interests or other compatible

processing of this data. The draft e-privacy regulation remains the subject of ongoing negotiations

on EU soil with a view to reaching an agreement on its text as soon as possible.

On 10 September 2020, the EC submitted a proposal for a Regulation of the European Parliament and of the Council

on a temporary derogation from certain provisions of Directive 2002/58 / EC of the European Parliament and of the Council regarding the use of technology by interpersonal communication service providers

independent of numbering for the processing of personal and other data for the purpose of combating sexual

child abuse online. The reason for the proposed regulation was the entry into force

European Electronic Communications Code, which introduces, among other things, a new definition

electronic communications services, which also includes service providers without a number

(applicable from 21 December 2020). The provisions of the e-privacy directive will take effect on this date

also apply to providers of interpersonal communication services independent of

numbering, making it difficult / impossible for them to continue using technology for combat purposes

against child sexual abuse online. At the end of October 2020, the EU Council approved a mandate for

start negotiations on this proposal with the European Parliament. Due to fundamentally different

comments on the draft regulation from both institutions, the negotiations were not concluded by 21 December

2020a will continue in the form of trialogues.

## 12.2 European Data Protection Board

The EDPB is an independent EU body with legal personality that contributes to consistency application of data protection rules throughout the EEA and encourages cooperation between EEA personal data protection.

The EDPB is represented by its chairman, the chairman of the Austrian supervisory authority, Andrea Jelinek. It consists of the head of one supervisory authority of each Member State EEA and EDPS. The EC has the right to participate in EDPB activities and meetings without voting

45

rights.

The EDPB operates in accordance with the Rules of Procedure, which were amended twice during the period under review.

EDPB's activities are divided between 12 expert subgroups and 3 working subgroups

groups (task forces), which are thematically divided. E.g. Technology Expert Group

finances, cooperation, and others. These expert subgroups are working on documents that

contributes to the consistent application of the Regulation. The Office participates in the work of 11 experts

subgroups and 2 working groups by personal participation, by sending written comments,

by participating in video and body conferences, possible related workshops.

The documents on which the expert subgroups are working are approved by the EDPB Plenary.

During the period under review, 2 personal plenary sessions were held in Brussels and 25 online plenary sessions

meeting. The Office did not attend 3 online plenary sessions during the period under review.

The greatest benefit to the public is the issuance of guidelines and recommendations by the EDPB on various issues questions. During the period under review, the EDPB issued 15 guidelines and recommendations, 9 following a public consultation

and 8 for public consultation. EDPB also issued several documents focused on the evaluated period

for the processing of personal data in connection with the disease COVID-19, Brexit and for transfers

personal data to third countries in the light of the conclusions of the CJEU decision in the Schrems II case.

The guidelines (as well as other documents) are published on the EDPB website. Office on its

The website also publishes these guidelines and recommendations in Slovak and English language.

The Committee shall, in accordance with Art. 71 of the Regulation draws up its own annual report.

#### 12.3 Committee set up under Article 93 of the Regulation

According to Art. 93 Regulations and Art. 53 of Directive 2016/680, the EC is entitled to adopt implementing acts.

The Committee provided for in Article 93 of the Regulation shall meet on an ad hoc basis as necessary. In the evaluated period

The Committee met once and was presented with two draft EC implementing decisions aimed at standard contractual clauses between the operator and the intermediary according to Art. 28 GDPR and standard contractual clauses for transmission under Art. 46 par. 2 letter c) GDPR.

#### 12.4 Cross - border data exchange

The EU has set up a number of European large-scale information systems and agencies, which it oversees is shared between the national data protection authorities and the EDPS. In order to ensure high and a consistent level of protection, national data protection authorities and supervisors shall cooperate official in the coordination of supervision.

The EDPS is the EU's independent supervisory body responsible for ensuring respect for fundamental rights and freedoms of natural persons, and in particular their right to data protection by the Union institutions and bodies.

The EDPS is responsible for monitoring and ensuring the application of the provisions of the Regulation 2018/1725 and any other acts of the Union relating to the protection of fundamental rights and freedoms natural persons with regard to the processing of personal data by an institution or body of the Union and for advice to the Union institutions and bodies and to the persons concerned on all matters relating to processing of personal data.

The national supervisory authorities and the EDPS cooperate to ensure coordinated supervision. On the To this end, representatives of national data protection authorities and the Supervisor shall report regularly meet - usually twice a year - to discuss common issues concerning supervision. Activities include, but are not limited to, joint inspections and investigations and work on joint inspections



methodology.

These are specifically the following groups:

- ☐ Europol Cooperation Council,
- ☐ Joint Supervisory Body for the Customs Information System,
- ☐ SCG Working Group on the Coordination of Schengen Information Surveillance system II,
- ☐ Working Group for the Coordination of Supervision of the Visa Information System,
- ☐ Eurodac Supervisory Coordination Working Group
- ☐ Coordinated Supervisory Committee.

A representative of the Office attended a meeting of all the above groups. Meetings took place online.

## 12.5 Schengen evaluation

In October 2019, the Schengen evaluation of the Slovak Republic in the field of protection took place personal data. The processing of the results of the Schengen evaluation of the Slovak Republic 2019 was not even completed by the end of 2020. Slovakia will be duly adopted and approved Republic informed through a report with the results of the evaluation.

## 12.6 Convention Consultative Committee 108

The Consultative Committee established by the Council of Europe on Convention 108 shall consist of representatives of the Contracting Parties

Parties to the Convention supplemented by observers from other States (members or non-members) and international organizations. The committee is responsible for interpreting the provisions and for improvement implementation of Convention 108 and for drawing up reports, guidelines and guidelines in such areas such as contractual provisions governing data protection in the transfer of personal data to third parties who did not guarantee an adequate level of data protection or data protection with regard to biometrics, profiling and automatic decision-making or data protection in the field

health. These areas are only an exemplary part of the work of the committee. Meeting

The Advisory Committee shall be regularly attended by representatives of the Office, whether in plenary meetings or narrower meetings of the Committee.

The Council of Europe issued documents aimed at combating the disease during the period under review COVID-19 and digital contact tracking, the right to the protection of children's personal data in the context of education, on the international movement of personal data, on profiling, on political campaigns and digital identity.

47

## 13 MEETINGS WITH PARTNER SUPERVISORY AUTHORITIES

### CONFERENCES AND WORKSHOPS

#### 13.1 Good practices for Biometrics at the Borders

In April, the Office's representatives attended a one-day online conference called Good Practices for Biometrics at the Borders. Speakers such as eu-LISA, UNCTED, FRA as well as the representatives of the governments of the various states made their contributions, the main message of which was to share experience in the field of biometric data processing in the context of borders. It was discussed in particular on the protection of data subjects and ensuring the security of the processing of personal data, and on safeguards to be applied when considering the introduction of technology which: uses biometric data in response to public health. These include clear and detailed legal framework, rigorous testing of necessity and proportionality and the intended purpose of the application, incorporation of fundamental rights into technical specifications and procurement of technology and use fundamental rights impact assessments.

#### 13.2 The Hague Forum's second meeting

A representative of the Office attended a second meeting organized by the EDPS in July and the Dutch Ministry of Justice. The EDPS presented the shortcomings identified in the contracts that the EU institutions and agencies have with Microsoft in terms of protection of personal data. The aim of the meeting is to help with experience and findings

by the organizers to other states when concluding contracts and agreeing conditions on protection personal information when using Microsoft packages and cloud services from various companies.

### 13.3 Bitkom Privacy Conference

A representative of the office attended a two-day online conference called Battle in September Privacy Conference 2020. The conference was opened by the European Commissioner for Justice D. Reynders. In his speech, he gave a detailed presentation on data strategy and data economics.

The first panel discussion focused on how data protection could become a driver force for the data economy. The EDPS, W. Wiewiórowski, emphasized that trust and security are necessary for the success of data-based business models. It would not be without data protection no IT security can be achieved. Without it, data protection would be difficult to achieve without IT security. The role of supervisors has also been crucial for the development of new ones business models. The second day of the conference was opened by Professor U. Kelber - Federal Commissioner for data protection and freedom of information of Germany. In his speech, he looked at the first assessment Regulation and pointed to the unfavorable fragmentation in national interpretations of the Regulation. Once one of the main topics of the second day was the international transfer of data - also with a view to the decision CJEU in the Schrems II case and the related uncertainty, possible impacts of Brexit on data transfers and possible solutions on the road to legal certainty.

### 13.4 IDLaw 2020 - Conference on Innovation and Digitization in Law

A representative of the office attended a one-day online conference called IDLaw in September 2020 - Conference on Innovation and Digitization in Law, organized by the University of Vienna. The conference focused on an urgent issue in data protection law, namely discussion of anonymisation or pseudonymisation, or general requirements for removal of identity in the regulation. Re-identification is a basic concept according to Regulation because it determines the scope by setting the boundary between personal and non-personal data

applicability of European data protection law. Although the text of the regulation proposes different levels of identifiable, does not clearly set out the spectrum of identifiable what it creates uncertainty as to the specific steps to be taken by organizations. From a technical point of view, it is In addition, the selection and implementation of the most appropriate re-identification technique is comprehensive exercise.

### 13.5 Building Management 2020

In September, a representative of the Office attended a three-day 9th international conference entitled Building Management 2020. The conference was also held under the auspices of the Minister of Transport and Construction of the Slovak Republic.

A representative of the Office spoke in the Legislation, Finance and Informatics section focused on the processing of personal data in the field of building management. The conference brought practical issues and new stimuli in the field of personal data protection in the environment of apartment buildings. The conference is attended by a representative of the Office on a regular basis and thus also by communication from the administrators

Apartment buildings are more open and communicative, and aim to find solutions in this no a simple area that handles personal data and interpersonal relationships very much touches.

### 13.6 Cybersecurity for Artificial Intelligence

In September, a representative of the Office took part in a one - day online workshop entitled Cybersecurity for Artificial Intelligence. The workshop was organized by ENISA. The aim of the workshop was discuss cyber security challenges related to artificial intelligence. Although it is artificial intelligence is undoubtedly beneficial for everyday life, it should not be forgotten that intelligence and its application in automated decision-making - especially in critical deployments in terms of security - could open new avenues in methods of manipulation and attack, while creating new challenges for personal data protection. Cyber security therefore has paramount importance for the reliable and credible deployment of artificial intelligence.

### 13.7 QuBit Conference Prague 2020

A representative of the office attended a two-day online conference called QuBit in September Conference Prague 2020. The conference covered current security issues and threats such as as well as new trends and threats in cyberspace. The lectures focused on traditional ones emerging technologies and related threats. Wide shot in the area cyber security covered topics from ransomware and other malicious code attacks, cryptography, threats related to new technologies 5G, IoT, artificial intelligence and ways to reduce the risk of these threats to the organization and the individual.

### 13.8 7th AI and Law Breakfasts: Certification of Algorithmic Systems

Representatives of the Office attended a one-day webinar called 7th AI and Law in October Breakfasts: Certification of Algorithmic Systems. The conference was under the auspices of the Council of Europe in collaboration with the University of Strasbourg. The webinar focused on algorithmic certification systems, including those relating to the latest developments in artificial intelligence. At the time it is public opinion is very concerned about the specific consequences of some applications of artificial intelligence, such as discrimination or weakening of human rights, are sought by regulators specific solutions to build trust between users. The purpose of the certification webinar algorithmic systems was a practical examination of opportunities as well as practical issues such a proposal.

49

### 13.9 eHealth Security Conference 2020 Online Series vol. 2

ENISA has organized a series of virtual security conferences on eHealth in collaboration with the Danish Health Data Office on cyber security issues related to health care sector. In October, a representative of the Office took part in a part focused on cyber security when monitoring COVID-19 by mobile applications. Mobile applications they can assist monitoring authorities at national and EU level and restricting the spread of COVID-19. Many countries have announced a launch since the pandemic

virus support applications. The EU toolkit was issued on the basis of a recommendation

EC on contact tracking applications as a means of combating and mitigating the crisis

COVID-19. Representatives of the teams that developed these applications shared experiences and challenges from a cyber security perspective.

#### 13.10 Current challenges of cyber security

In November, a representative of the Office attended an online conference with international participation entitled

Current challenges of cyber security. The conference was organized under the auspices of the Rector

Academy of the Police Force in Bratislava. The main goal of the conference was to define

and analysis of current issues related to cyber security, generalization

theoretical approaches and practical experience of competent subjects of individual

security forces as a prerequisite for developing a systematic approach

to the field of cyber security and design of education system in state and public administration.

Other goals of the conference included the identification of assumptions and theoretical links to

linking theory with application practice, as well as ensuring the transfer of relevant knowledge

into the practice of state and public administration subjects for empirical research of specific problems

and current security practice needs to increase cyber security

SR.

#### 13.11 PrivSec Glogal 2020

A representative of the Office attended the online conference at the turn of November and December

called PrivSec Global 2020. It is the largest conference where over 10,000 experts met

in the field of personal data protection and security. The four-day conference provided a cross-section

in individual areas of security and data protection. The main topics were data protection,

privacy and security in industry. The individual lectures focused on the new

emerging technologies, but also the latest developments in security and threats

in the cyber world.

#### 13.12 Doing AI the european way: protecting fundamental rights in an arifical era

intelligence

In December, a representative of the Office attended a one-day online conference called IDLaw 2020

- Conference on Innovation and Digitization in Law. The conference was under the auspices of Germany

Presidency of the Council of the EU in cooperation with the FRA. This conference focused on how they can

evidence from specific cases to support policy makers in designing regulatory frameworks that

will shape the development and use of artificial intelligence in the coming years. Policy makers

at EU, national and international level to discuss whether and how to move forward

in the regulation of risk-based artificial intelligence in order to realize its enormous potential and at the same time

ensure that people can trust this technology.

50

## 14 ASSESSMENT OF THE PROTECTION STATUS

### IN THE MONITORED PERIOD

#### PERSONAL

#### DATA

2020 was a year that probably none of us were ready for and did not expect that in that period

will affect several fundamental human rights to the extent that this has happened as a result

the outbreak of the Covid 19 pandemic and the efforts of the competent authorities to stop it, or

minimal slowdown in its spread. It was a year in which the pandemic affected not only human health but

was also reflected in the legislative activity of the state. Especially in terms of trying to prevent its spread

personal data were processed on a massive scale and this processing also became the subject

general debate and the focus of the public, as so massively and so often on the physical

persons have not processed health data in the history of the independent Slovak Republic even once.

Also, abbreviated legislative procedures have in some cases led to swift but fundamental ones

amendments to laws, the subject of which was also the regulation of personal data processing, where without

the previous interdepartmental comment procedure did not have an office or other institutions

dedicated to the protection of fundamental human rights and freedoms

comments to correct the proposed changes, which in a context is sometimes quite radical

interference with the provisions of certain laws has led to such changes with which the Office within the meaning its scope is not always identified.

The year 2020 can be characterized, especially from the outside, as a year when the office figuratively in other words, he stood on one side of the barricade and other state authorities on the other, among them were legal norms, provisions, decrees, which by their obligations also apply to processing personal data aroused the passions of the public and the office was repeatedly overwhelmed several times a year these legal norms and the obligations arising from them. It was necessary respond to questions from the public, both lay and professional, about the legality of the provisions and how they are to be met in practice, or not at all. This hectic period was so challenging for the public, as well as for the staff of the Office, who sometimes dealt with all their might their agenda and the growing outrage of the public seeking a response, with the Office within its material competence, it could provide only some. Also based on this experience there is a need to learn from them in the future and to try to make legislation, in particular in this difficult period, a collegial work, not an individual creation, which after a short time application practice inevitably leads to subsequent amendments. Office, though in terms of The staffing is undersized and has professionals who are willing and able to participate their knowledge of law-making.

The processing and protection of personal data reached a completely new level in 2020 as a result of the pandemic dimension created by the transition of work and private life to the online environment.

Over the last year, huge changes have taken place in this direction, and many people are influencing their own "Online" life to the extent that their personal data is subject to need and interest.

Only in the last year have many recognized the need to protect and inform about the processing personal data much more attention, as personal data are not just the subject of trafficking and interest, but the online environment as a whole is also attacked in terms of security. Also based on continuing distance education of pupils and students are also their learning outcomes, their



personal data much more vulnerable. All these newly created aspects of life were highly perceived by the office also in its work in 2020. Only the questions of the public were so wide-ranging that they responded it required them to know and describe many times the knowledge and connections between several laws, to which they concerned.

In conclusion, the year 2020 can be evaluated as a year when the protection of personal data, their processing have come to the fore at some point, whether in terms of newly adopted legislation, or

51

obligations imposed by this legislation and their implementation in practice has been linked with personal data.

2020 can be seen as a year that has not only affected our lives, but also changed our perspective society on personal data and the need to protect them, as in spite of all the measures and responsibilities are also needed to protect the highest value of life protect other fundamental rights and freedoms and not diminish their value and importance.

52