print 1662

PERSONAL DATA PROTECTION STATUS REPORT

FOR THE PERIOD MAY 25, 2018 TO MAY 24, 2019

Office for Personal Data Protection of the Slovak Republic

September, 2019

Office for Personal Data Protection of the Slovak Republic

Hraničná 12

820 07 Bratislava 27

https://www.dataprotection.gov.sk

Electronic version of the report available at

https://dataprotection.gov.sk/uoou/sk/content/vyrocne-spravy

IČO: 36064220

Steuernummer: 2021685985

REPORT ON THE STATUS OF PERSONAL DATA PROTECTION PERIOD

May 25, 2018 to May 24, 2019

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

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

of the Act submits a Report on the Status of Personal Protection to the National Council of the Slovak Republic

data for the period 25 May 2018 to 24 May 2019. The report primarily reflects the assessment

its activities in the period under review and also contains observations from its activities, reflecting some

his personnel and material needs, which are much more obvious and their need much more

evident during this period, when it carries out activities under both the Regulation and the law.

"On the basis of the above provision, I am submitting the Report on the Status of Personal Protection

data for the period from 25 May 2018 to 24 May 2019, which will be discussed in the National Council

Of the Slovak Republic in accordance with Act no. 18/2018 Coll. on the protection of personal data and on change

and amendments

some

laws

published

on the

web

headquarters

office,

https://www.dataprotection.gov.sk for the general public. At the same time it will be provided to the press

and electronic media and the European Data Protection Board and the Commission. ".

Soňa Pőtheová

President of the Office

LIST OF ABBREVIATIONS USED IN THE REPORT

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 for the period from May 25, 2018 to May 24, 2019

the law

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

Act no. 122/2013 Coll.

Act no. 122/2013 Coll. on the protection of personal data and on the amendment of certain

of laws as amended by Act no. 84/2014 Coll.

CIS

Customs Information System

Directive 95/46

Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on protection

natural persons in the processing of personal data and on the free movement of such data

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

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

EEA)

Directive 2016/680

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

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

criminal offenses, their investigation, detection or prosecution or for the purpose of

sanctions and on the free movement of such data and repealing the 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)

5

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

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

movement of such data, repealing Regulation (EC) No 45/2001 and decision

no. 1247/2002 / EC

decision no. 1247/2002 / EC

Decision of the European Parliament, the Council and the Commission 1247/2002 / EC of 1 July 2002

on the rules and general conditions governing the performance of the European

the Data Protection Supervisor

Act no. 211/2000 Coll.

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

certain laws (Freedom of Information Act)

supervisory officer

European Data Protection Supervisor

EU

European Union

EK

European Commission

EEA

European Economic Area

WP29

The working group set up under Art. 29 of Directive 95/46

Committee

The European Data Protection Board established by

Art. 68 Regulations

Europol

European Police Office

CONTENTS

1. INTRODUCTION

1.1 Purpose of the report on the state of personal data protection

In a time of massive electronization and data sharing as widely as possible, including

personal data protection, personal data protection, in the context of privacy protection, gets on

the imaginary top of the ranking of fundamental human rights and freedoms, which are one of the pillars

democratic society. Pursuant to the provisions of § 81 par. 2 letter k) of the Act is submitted by the Office

NR SR this report. It is a summary of information about the Office's activities and its findings

period.

1.2 Follow - up to the previous report on the state of personal data protection

The presented report is the twelfth in the history of the independent Slovak Republic and the tenth

in the history of the existence of a separate office.

The report follows the last report on the application side, as from 25 May 2018

The regulation came into practice and the law became effective. So it can be said that into this

At that date, the Regulation and the law were a "training ground", and from that day on they were a real "battlefield".

The previous report was delivered to the National Council of the Slovak Republic on September 27, 2018. Committee of the

National Council of the Slovak Republic for Human Rights

rights and national minorities discussed and took the previous report on 16 October 2018

note. Subsequently, the Chairwoman of the Committee of the National Council of the Slovak Republic informed the Chairman of the National Council of the Slovak Republic of the adopted

Resolution no. 109, by which the Committee of the National Council of the Slovak Republic took note of the report. The previous message was not

subject to voting by deputies of the National Council of the Slovak Republic.

9

STATUS, PERSONNEL SECURITY AND BUDGET

OFFICE

2.1 The position of the Office

The protection of personal data in the Slovak Republic is entrusted by law and Regulation

within the remit of the Office. The Office is a state administration body with nationwide competence

supervising personal data protection and participating in the protection of basic data

rights and freedoms of individuals with regard to the processing of their personal data. In the exercise of its powers

the Office acts independently and in the performance of its tasks it follows the constitution, constitutional laws,

laws, other generally binding legal regulations and international treaties,

by which the Slovak Republic is bound. The Office is the budgetary organization according to the provision

§ 21 par. 1 and par. 5 letter a) of Act no. 523/2004 Coll. on budgetary rules of public administration

and on the amendment of 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. Soňa holds the position of President of the Office Pőtheová, who was elected to the position of the National Council of the Slovak Republic on 14 May 2015 by a resolution of the National Council

Of the Slovak Republic no. 1736/2015.

In the absence of the President of the Office, he shall be represented by the Vice-President, who shall appoint and dismiss him 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 effective, holds the office of Vice-President of the Office

from 2 January 2016 to the position appointed by the Government of the Slovak Republic by Resolution no. 658/2018

of 2 December 2015

2.2.2 Personnel area of the Office 's staff

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

activities and obligations under generally binding legal regulations. Securing them

requires the necessary number of qualified staff qualified to perform professional

activities at a high required level. In the conditions of the office, in terms of structure

employees, with the exception of one employee performing work in the public interest,

the others are civil servants. Selection of employees

and filling of vacancies is carried out in accordance with the law

conditions for each function.

As of May 25, 2018, the office had 39 seats, of which

 38 employees in the civil service relationship,

 1 employee performing work in the public interest.

As of January 1, 2019, the office had 46 seats, of which

 45 employees in the civil service relationship,

 1 employee performing work in the public interest.

Average age of employees

 as of May 25, 2018 it was 40.1 years, while

 was 43.2 years for men;

 in women 38.6 years;

 as of 1.1.2019 it was 39.9 years, while

 was 41.6 years for men;

 for women 39.1 years.

Overview of the number of employees of the Office

Actual staffing of the Office

Year

to 25.5.2018

to 01/01/2019

Civil service

ratio

38

45

Performance of work in public

interests

1

1

Together

39

46

The protection of personal data has been carried out since May 2018 in accordance with both the Regulation and the law,

which

directly set out all the responsibilities of the Office. Despite the undeniable importance of its activities,

which is constantly increasing, as is the importance and value of personal data as a resource

information on natural persons, the number of staff of the Office is essentially unchanged and is already oscillating

several other years around the number 40. In particular since the period of application of the Regulation Office

feels that the current number of staff is insufficient and that it is necessary

number significantly increased. Many employees currently perform some functions

cumulatively, which does not contribute to their work comfort and mental demands

work, it is not right and sustainable. To illustrate, the number of "live proceedings."

per head ”in the department of administrative proceedings is for some employees of this department almost

100, which is an alarming situation that is unsustainable in the long run. From application practice

more than ever before, there is a need for at least two

detached workplaces, one in central and one in eastern Slovakia. The reason

The need for the establishment of these workplaces is that in this way the employees of the Office would be more closely

affected

persons from these areas of Slovakia and also the fact that, for example, the performance of inspections would be as follows

streamlined, as it would not be necessary to spend such large sums of money on

travel of employees always from Bratislava to central or eastern Slovakia. About time

saving employees, speeding up and streamlining procedures, not to mention.

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.

For the year 2018, a budget of EUR 1,163,853.00 was originally approved for the Office, which is

during 2018 it was adjusted several times, until finally its final amount was 1,318,252.00

Eur.

The budget for 2019 was originally approved for the Office in the amount of EUR 1,442,263.00, which was

adjusted for valorisation to the amount of EUR 1,561,419.00.

Overview of the Office's budget for the period 1.6.2018 to 31.12.2018 in Euros

Pointer

Approved budget

for 2018

to 01/01/2018

Adjusted budget

to 31.12.2018

Drawing from

6/1/2018

to 31.12.2018

673 121.00

773 377.00

551 626.32

237,498.00

287 469.00

206 143.63

237 234.00

224 245.00

128 172.24

5,000.00

13,161.00

11,168.16

11,000.00

20,000.00

19,571.33

0.00

0.00

0.00

1,163,853.00

1,318,252.00

916,681.68

0

0.00

0.00

Wages, salaries, service

revenue and EO (610)

Wage premiums (620)

Goods and services (630)

Current transfers (640)

EKW02 (630) common

expenses

EKW02 capital

expenses

Total current expenditure

(600)

Capital expenditures (700)

Overview of the Office's budget for the period 1.1.2019 to 31.5.2019 in Euros

Approved budget for the year

2019 to 1.1.2019

Pumping

to 31.5.2019

879,575.00

301,384.37

309 654.00

111 135.54

Goods and services (630)

237,034.00

133,603.10

Current transfers (640)

5,000.00

3,499.45

11,000.00

3720,31

1,442,263.00

553 342.77

Pointer

Wages, salaries, earnings and OOV

(610)

Wage premiums (620)

EKW02 (630)

Total current expenditure (600)

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

and responsibilities of the Office, due account must be taken of the growing agenda and material needs

technical equipment also in the Office's budget. The office also saw an increase in Europe

and the 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 matter is important guidelines and documents affecting the Office's activities on behalf of

Slovak 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 they are

12

other reasonable grounds to believe that the infringement is linked to European political activities

political party or European political foundation in the context of the European elections

Parliament, the decision shall be notified to the Office for European Political Parties and Foundations.

13

3 LEGISLATIVE PROTECTION OF PERSONAL DATA PROTECTION

3.1 Interdepartmental comment procedures of generally binding legal regulations

The Office is a body with nationwide competence supervising the protection of personal data

data protection and involved in the protection of fundamental human rights and freedoms with regard to the processing of

personal data

data of natural persons. The Office fulfills its role in supervising the processing of personal data

data and by supervising and commenting on the texts of draft laws and others in general

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 Office 's observations is in particular to:

the quality of the legislation on the processing of personal data was high, so that

the legislation subsequently adopted was precise, unambiguous, and thus in relation to

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 commented on 14 materials. Together with these materials

submitted 48 comments, 33 of which were substantial. The comments made

requested an adjustment of the list or scope of the personal data processed in relation to the purpose

processing, the Authority also often fundamentally required that they be included in the draft legislation

clarified and clarified responsibilities for the processing of personal data. Specific wording

The submitted comments of the Office can be viewed on the Portal using the filter of institutions that

comment and using the comments filter (whether it is an organization comment)

marked as essential or ordinary).

3.2 Methodological guidelines of the Office

According to § 81 par. 2 letter d), e) and f) of the Act, the Office methodically guides the operators

and intermediaries in the processing of personal data, raises public awareness in the area

risks and rights associated with the processing of personal data and also raises awareness

operators 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 ah hoc methodologies published on the Office's website. The office is within it

published methodologies addressed issues and issues that were the subject at the time

the greatest interest of the public and operators.

Another area that the Office has addressed and is dedicated to helping those affected for whom

some nuances of personal data processing in the context of the new legislation were nevertheless

foreign and it was appropriate to explain and clarify some information.

In its methodologies, the Office also dealt with the processing of personal data by social networks

and operators, these social networks and also addressed some areas

business environment and the processing of personal data within the sector

(processing of personal data by e-shops).

To illustrate, we draw attention to some of the Office's methodologies

Methodology for notifying the designation of the responsible person

Methodology for when the Regulation applies and when the law

14

Methodological guidelines of the Office on the obligations of the controller in the processing of personal data

e-shop

Methodological guidelines of the Office on the lawfulness of processing

Methodology of compliance of personal data processing in the environment of schools and school facilities

The Office published one of the most important methodologies, which was also an obligation for the Office

so-called "Black list" of processing operations which, if the operator intends to carry them out

and process personal data within them, he is obliged to carry out an impact assessment before starting them.

The Office also dealt with other issues and issued short ad hoc methodologies to current ones

processing issues, these, as well as all previous methodologies, can be traced to

the Office's website in the part of the Office's methodology.

The Office has focused much of its methodological work on assisting the persons concerned, while

primarily aimed at assisting data subjects in exercising their data subject rights when

prepared and published the forms available to the persons concerned in this regard when applying them

are usable.

15

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 is not limited to operators or

intermediaries who are obliged to apply personal data protection legislation

in practice, it also affects people affected who have issues arising from common situations

related to their personal data.

The Office's operators and intermediaries most often address questions of a professional nature

related to their obligations under the Regulation and the law, as specific to it

provisions to be applied in practice.

Recently, there has been an increase in questions from the law firms representing

operators who address to the Office often to answer entire case studies to the Office

answered the questions and assessed the processing of the personal data of the "client" of the law firm.

If the subject of the question is only a specific part concerning processing, when is it also proposed

solution, or solution to the problem, such a question is acceptable, provided that it is the subject of the question

the entire processing or assessment of the operator's position without the proposed consideration

solutions, the Office generally does not respond to such questions, as it is not correct and possible for it to provide

legal service to law firms, moreover, such its activity goes to the detriment of others, which

has an obligation to perform. At the expense of an increasing number of such complex issues office

He also responded to this activity by publishing a notice on his website, giving the opinion of the Office

reflects the views of the Commission, the European Parliament and the Council.

The Office also continued in contact with the public through a limited regime

telephone consultations. In the monitored period, the Office provided up to 200 telephone calls

consultations, mostly during 2018. In 2019, the Office already consulted by telephone in

did not provide the time allowed, as this activity was very burdensome and within the activities

carried out in the context of the Regulation, the number of other activities required by it has increased

to cover.

The Office replied to the public's written and e-mail questions during the period under review

more than 1500 such questions.

4.2 Communication of the Office with the media

Over the period under review, media interest in personal data protection has increased as

Regulation and law, ie both legal norms bringing new rules in the field of protection

personal data have started to apply. In the period under review, the Office provided 67 statements for

media (print, radio and television together).

Media interest initially focused on describing the main differences between the newcomers

and the "old" legislation, then, over time, focused on quantification

proceedings, or to fines already imposed under the new legislation.

In 2019, media interest calmed down and gradually focused on specific issues and "cases"

in which the processing or protection of personal data was also the subject, or there were questions

journalists aimed at specifying the rights of the persons concerned, how to exercise them correctly and what

everything can be claimed from the operator as a person concerned.

16

4.3 Privacy Day

The Day of Personal Data Protection, January 28, is the date of the signing of Convention 108, which was

signed in Strasbourg in 1981. This day has been declared by the Committee of Ministers of the Council of Europe

for Privacy Day.

In this context, the Office strives every year to contribute to the popularization of personal data on this day

data and their protection to the general public. The year 2019 was no exception to this plan.

As it has been a year since the Regulation came into practice and the law entered into force

the office wanted to make this anniversary special and bring an activity that would be a one-year anniversary

Regulations and law adequate. The choice eventually fell on organizing an interactive one

workshop held on 28 January 2019; was divided into 4 topics with separate

presentations by the staff of the Office. The choice of topics answered the questions that the public considered

period were most interesting. The workshop turned out better than expected, with a hall with a capacity of 100

The seats were filled within a few minutes of its opening, and they also attended the workshop

affected persons, or responsible persons from eastern Slovakia, despite the extreme

adverse weather, which we appreciate very much and we are pleased with such interest.

4.4 Office website and its traffic

The Office's website meets the conditions and technical criteria in accordance with the Ministry's Decree

Finance of the Slovak Republic on standards for public administration information systems, reflects on the new

legislation in the field of personal data protection, and is gradually being supplemented by new ones

functionality and forms.

The operator and the intermediary are obliged to notify the Office of the contact details specified

responsible person. As the responsible person acts as a contact point for the Office, he is

the operator and the intermediary are also obliged to notify the Office of the identity of the responsible person

persons. For easier reporting of responsible persons, already before May 24, 2018 office for

for this purpose, as a public service, created a new contact form for administrative reasons

relieving operators and intermediaries.

The Office has updated the form for the application for personal data protection proceedings, which

the person concerned may use or be inspired by it, in particular as regards mandatory particulars

request to initiate personal data protection proceedings.

The Office's website was searched a total of 828 907 times during the reporting period, namely

most often through the websites and browsers listed below.

17

An overview of the websites through which the website is accessed

office

An overview of the websites through which the Office's website is accessed

TOP 10

The order

URL

Impressions - Count

1

https://www.google.com/

329992

2

https://www.google.com/

81 209

3

https://www.bing.com/

12 952

4

https://www.google.com/

8 472

5

http://m.facebook.com

7 666

6

http://www.vlada.gov.sk/

2 429

7

https://www.google.de/

2 284

8

https://www.google.co.uk/

1 913

9

https://l.facebook.com/

1 351

10

https://www.google.at/

1 221

4.5 The Office's website and reporting privacy breaches through a designated

form (reporting data breach)

Operators and intermediaries must ensure the continued credibility, integrity,
availability and resilience of processing systems and services and at regular intervals
assess the effectiveness of the technical and organizational measures in place. Nevertheless, it can
(whether due to willful negligence, negligence, error or natural disaster)
security of personal data which, as a result, may involve accidental or
unlawful destruction, loss, alteration, unauthorized provision or disclosure,
personal data transmitted, stored or otherwise processed.
The operator has an obligation under Art. 33 Regulations or according to § 40 of the Act to report
data breaches can do so in a number of ways,
one of which is the possibility to use the form created to fulfill this obligation.
The obligation to report a personal data breach during the reporting period was
performed a total of 95 times. Reporting is an obligation for operators
and intermediaries, not for the persons concerned.
In the monitored period, we registered a total of 95 personal data breaches reported
of the Office, of which 6 applications were reported by the persons concerned and 89 by the operators. In this
In this context, we would like to state that in cases where data breaches have been reported by the persons concerned, these
they also stated in their notification that they had reported data breaches on the grounds that the operator had stated that
he will not report data breaches or incidents for data breaches that need to be reported
the Office. We would also like to appeal to the operators to get theirs
obligations themselves, as if the Office finds that there have been data breaches that did not
reported to the Office, this may, for example, be of a personal data protection nature
An "aggravating" circumstance which the Office will take into account in the proceedings.

5 PERSON RESPONSIBLE

He is responsible for supervising the protection of personal data processed in accordance with the law
operator. The operator and the intermediary may or may not set out in the specified

cases (Article 37 (1) (a) to (c) of the Regulation, or § 44 (2) 1 letter a) to c) of the Act)

to determine the responsible person by exercising personal data protection supervision, while being obliged to do so

report it to the Office.

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

Resposible people

Total number of reported responsible persons

Period

5/25/2018 to 5/24/2019

Count

8431

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

During the period under review, the Office, as the operator, received one application from the data subject

a person who has been provided positively by the responsible person of the Office, ie the request of the person concerned

person was complied with.

6 APPROVAL AND CONSULTATION ACTIVITIES OF THE OFFICE

6.1 Prior consultation

Pursuant to Art. 36 par. 1 Regulations shall be made by the operator with the supervisory authority before

consultation, if the data protection impact assessment pursuant to Art. 35 shows that

such processing would lead to a high risk to rights and freedoms if

the operator has not taken measures to mitigate this risk.

The Office received 5 requests for prior consultation from operators. After

examination of their content, two applications were excluded, and were assessed as applications for legal

advice in relation to prior consultation and impact assessment. So the real office

has carried out 3 previous consultations.

6.2 Transfer of personal data

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

Transfers can be divided into two groups:

- transfer to third countries (international organizations) guaranteeing an adequate level protection a
- transfer to third countries (international organizations) not guaranteeing adequate level of 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 a third country guaranteeing or not guaranteeing an adequate level of personal data protection.

The status of the country that guarantees an adequate level of personal data protection is determined by the EC decision. It is necessary for a country or international organization to provide for its own sake national law or international agreements it has signed, the level of protection fundamental rights, which is essentially equivalent to the level of protection guaranteed in the legal order EU.

The EC issues a decision on adequacy separately for the material scope of the Regulation and separately for the material scope of Directive 2016/680. Adequacy decisions issued by the EC over time scope of Act no. 122/2013 Coll., Remain in force until the EC changes them, does not replace them or not annulled by a decision taken under the Regulation. Those decisions shall apply only to transfer of personal data within the material scope of the Regulation, not Directive 2016/680. Office publishes adequacy decisions on its website.

During the period under review, the EC issued a decision on adequacy under the Japan Regulation,

which concerns only the transfer of data within the private sector, which is regulated by the Japanese

The Act on the Protection of Personal Information.

At the same time, Japan adopted a decision on adequacy for the EU / EEA. These two decisions

20

together they create the largest area of secure and free transfer of personal data in the world

based on a high level of protection. Both decisions apply from 23 January 2019.

During the period under review, the EC did not issue any decision on adequacy under 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

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

Those adopted under the previous legislation remain valid as long as

do not amend, replace or revoke the supervisory authorities. They were not accepted during the period under review

no binding internal rules under the Regulation.

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

Those adopted under the previous legislation remain valid as long as

do not amend, replace or repeal the EC. None were accepted during the period under review

standard clauses under the Regulation.

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

It is a new tool for transferring personal data. None were accepted during the period under review

standard clauses adopted by the Office under the Regulation.

(e) an approved code of conduct

It is a new tool for transferring personal data. None were approved during the period under review

codes.

(f) an approved certification mechanism

It is a new tool for transferring personal data. None were approved during the period under review

certification mechanisms.

(g) contractual clauses

It is a new tool for transferring personal data. None were approved during the period under review

contractual clauses.

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

authorities or public bodies and include enforceable and effective rights

persons concerned

It is a new tool for transferring personal data. The Committee delivered its opinion during the period under review

4/2019 on the draft administrative arrangement on the transfer of personal data between the

financial supervision within the European Economic Area (EEA) and the financial authorities

supervision outside the EEA. The Office did not approve such arrangements during the period under review.

(i) a judgment of a court / tribunal or a decision of an administrative authority of a third country

(j) exceptions for special situations under Art. 49 Regulations

In addition to these exceptions, the Committee adopted Guidelines no. 2/2018

on exemptions under Article 49 of Regulation (EU) 2016/679.

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

Also regulated in Guidelines no. 2/2018 on exemptions under Article 49 of Regulation (EU)

2016/679.

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 has come to a conclusion,

that there are adequate guarantees for the protection of personal data,

c) exceptions for special situations pursuant to Section 76 of Act 18/2018,

d) transfer to a recipient from a third country pursuant to Section 77 of Act 18/2018.

22

7 CONTROL

In the period from the beginning of the application of the Regulation and the Act (ie from 25.05.2018), the Office is within

authorized to carry out control of the processing of personal data, control

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

personal data with the issued certificate according to § 86 and control of compliance with the issued

accreditation certificates pursuant to § 87 and § 88 of the Act.

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 report (if no breach of obligations has been identified

in the processing of personal data) or in the inspection report (if discrepancies have been identified

with the requirements of generally binding legislation). Results of inspections formulated

in the control protocol, initiate the initiation of personal data protection proceedings or are used as

basis for issuing a decision in ongoing proceedings.

7.1 Checks carried over from the period before 25.05.2018

In the evaluated period, the Office completed 9 inspections of personal data processing, which were initiated

at the time of the effectiveness of Act no. 122/2013 Coll. (ie before the application of the Regulation and the law).

In two cases, the inspected persons were natural persons operating cameras

systems, one public institution, two inspections focused on two different workplaces

the same state authority, two inspections of school facilities and, in the remaining two cases

were controlled persons of the company.

It has not been established in relation to CCTV systems operated by natural persons

violation of law no. 122/2013 Coll., As a result of which both inspections were terminated by a record

on inspection as well as inspections of two workplaces of a state body, inspection of one school

equipment and control of one trading company. The remaining three inspections were carried out

identified discrepancies with the requirements of Act no. 122/2013 Coll., As a result of which these inspections were

terminated by the inspection protocol.

Summary of the structure of inspected persons and results of inspections:

Controlled persons

Deficiencies found

(inspection report)

natural persons

public institution

state authority

school facilities

trading companies

0

1

0

1

1

No detected

shortcomings

(inspection record)

2

0

2

1

1

7.2 Inspections initiated during the period under review

Controls of personal data processing started from 25.05.2018 (ie controls started at

application of the Regulation and the effectiveness of the law) were carried out in the period under review

personal data protection proceedings, on the basis of a control plan as well as on the basis of suspicion

from a breach of personal data processing obligations laid down in the Regulation, or

by law. The focus of the controls was on the real state of personal data processing

23

with an emphasis on the compliance of processing activities with the requirements of the new legislation

represented by the Regulation and the law, which resulted in time and professional demands

implementation of the controls themselves.

In the creation of the inspection plan, as well as in the selection of inspections initiated by the Office on an ongoing basis

The Office drew mainly suspicions of breaches of personal data processing obligations

from own experience gained in the exercise of supervision in the previous period and trends

further development, ie he applied the empirical-intuitive method.

By delivering the notification of the inspection to the inspected person, the Office started in the evaluated period

51 inspections, of which 6 on the basis of a plan of inspections, 26 on the basis of a suspected breach of obligations

in the processing of personal data and 19 in the framework of personal data protection proceedings.

The inspected person was the operator in 45 cases, and the intermediary in one case

and in 5 cases an entity as both an operator and an intermediary. In terms of type

of the inspected operator or intermediary, 7 inspected persons are natural

person and 44 controlled persons other than natural persons, while non-natural persons are

in 7 cases by a municipality or city.

In the evaluated period, the Office began the performance of a total of 51 inspections, of which until 24.05.2019

completed 21. The 21 inspections were completed in 11 cases by the inspection protocol

and in the remaining 10 cases an inspection record. In terms of the incentive to inspect, there were 12

checks carried out on suspicion of a breach of personal processing obligations

data protection and 9 controls in the framework of personal data protection proceedings.

Out of a total of 51 inspections initiated in the period under review, it was up to the forthcoming period

30 controls transferred.

Stage 51 inspections started after 24.05.2018

40

30

20

30

10

11

10

0

checks completed by the protocol

checks completed by the record

inspections not completed by 24.05.2019

7.2.1 Checks in the framework of personal data protection proceedings

The performance of checks in the framework of personal data protection proceedings is ex lege preferred over

inspections carried out on the basis of the inspection plan as well as prior inspections

on suspicion of a breach of personal data processing obligations.

7.2.1.1 Selected inspections - camera systems

As part of the personal data protection procedure, five camera inspections were carried out

systems operated by natural persons. Inspections of camera systems were focused

on the principles of personal data processing, provision of information in the collection of personal data

from the persons concerned, the definition of the legal basis for the processing and the examination of the processing

in terms of the material scope of the General Data Protection Regulation. All checks were

completed by the inspection record. Of this number, one check was completed

the withdrawal of the application by the applicant, and in the other two

In some cases, the monitoring of private land was classified as personal processing

data in the framework of exclusively personal or domestic activities which do not fall within the scope

general data protection regulation. The cameras were installed in most cases

natural persons, in particular because of repeated attacks on themselves and out of concern for themselves

safety and health. In the remaining two cases, individuals did not use real

camera system, but they had dummy cameras installed, as a result of which there was no

for processing personal data by a camera system, resp. these natural persons did not acquire

operator status.

7.2.2 Inspections based on the inspection plan

The inspection plan for 2018 was in order to create sufficient time

to harmonize the practices of operators and their intermediaries with the requirements

Regulations and the law targeted at compliance with the provisions of Act no. 122/2013 Coll.,

thus for the period up to 24.05.2018.

The control activities included in the control plan for 2019 are focused on the compliance of processing

personal data with the requirements arising from generally binding legal regulations

and international agreements by which the Slovak Republic is bound. In the intent of the inspection plan

for 2019, the office placed particular emphasis on the compliance of processing activities with the principles

processing of personal data, lawfulness of processing, conditions of processing special

categories of personal data, the rights of data subjects and the management of information security risks including the possible effects of the processing of personal data on rights and legally protected interests data subjects (personal data protection assessment), as the adoption appropriate technical and organizational security measures and their provision Continuous updating under the conditions of the operator or intermediary are essential preconditions for successful minimization of security risks, resp. prevention personal data breaches (such as unauthorized disclosure or disclosure of personal data) and other undesirable processing operations with personal data data.

The inspection plan, which is divided into two parts according to the focus of each inspection (focus to the Schengen acquis and focus on the type of processing activity), includes processing activities carried out by public and private entities. The first part of the inspection plan is aimed at identifying the status of personal data processing in national districts (with the exception of the Europol Information System) selected personal information systems data to ensure the practical implementation of the Schengen acquis on the territory of the Slovak Republic and on the premises of the embassies of the Slovak Republic abroad. Checks consist of continuous monitoring of competence authorities to process personal data securely and lawfully in specific information systems used to protect the Schengen area (eg SIS II, VIS, Eurodac, Europol). The second part of the control plan focuses on the consistency of the processing of personal data with the requirements of the Regulation and the law. The part of the control plan in question also reflects the risks involved with specific processing activities or with the use of new technologies and procedures.

25

As part of the implementation of the inspection plan, an inspection notice was delivered during the period under review The inspected person initiated a total of 6 inspections, one of which (focused on Schengen

acquis) ended on 16.07.2019.

7.2.2.1 The Schengen acquis

The Office regularly includes personal data processing controls in the control plan
to ensure the practical implementation of the Schengen acquis by the competent authorities in the territory
Of the Slovak Republic, as well as embassies of the Slovak Republic abroad.
Checks on the national part of the second generation Schengen Information System (N.SIS II)
operated by the Ministry of the Interior of the Slovak Republic and the national part of Visa
information system (N.VIS) operated by the Ministry of Foreign Affairs
and European affairs of the Slovak Republic are included in the control plan on the basis of
recommendation resulting from the resolution of the Government of the Slovak Republic no. 755 of
November 30, 2011, by which the government approved the Schengen Action Plan of the Slovak Republic
as a priority of the Government of the Slovak Republic. In connection with the change of the national access point
Eurodac information system for Eurodac II version (2015) acquired by the operator,
which is the Ministry of the Interior of the Slovak Republic, new competencies and responsibilities;
at the same time, as a result of this fact, the Office was obliged to perform annually
control of the processing of personal data at the Eurodac National Access Point. By acceptance
Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the Agency
European Union for Law Enforcement Cooperation (Europol), which they replace
and repealing Council Decisions 2009/371 / JHA, 2009/934 / JHA, 2009/935 / JHA, 2009/936 / JHA
and 2009/968 / JHA, the Office was obliged to carry out regular inspections of processing
activities of the Europol National Central Office or the Europol National Liaison Officer.
In the national parts (subsystems) of the information systems in question, they are in addition to the usual ones
specific categories of personal data are also processed (eg identification) data, in particular
biometric data, data revealing racial or ethnic origin as well as personal data relating to
guilt for committing a crime or misdemeanor, ie personal data eligible
significantly affect the rights and legally protected interests of the persons concerned. In the evaluated

During this period, a check was made on the processing of the personal data of the data subjects, which included 5 workplaces of the operator Ministry of the Interior of the Slovak Republic, specifically the airport border crossing Bratislava, Vyšné Nemecké border crossing, Computer Center of the Ministry of the Interior of the Slovak Republic (technical support of information systems operated by the Ministry of the Interior of the Slovak Republic including the Schengen systems N.SIS II, N.VIS, NUIP and Eurodac), a for IS AFIS operation - Eurodac (comparison of fingerprints at the international level) and the Europol National Unit (processing of personal data in the field of information exchange within the European Union Agency for Law Enforcement Cooperation (Europol).

Despite the fact that the Ministry of the Interior generally approaches implementation the Schengen acquis with a high degree of responsibility, an error was found during the inspection consisting in the fact that the ministry did not carry out an impact assessment of the planned processing plants operations for the protection of the personal data of the persons concerned, as provided for in the new adjustments to the processing of personal data.

The subject of control at border crossings was the security of personal data processing with emphasis on the adequacy of personnel security measures, personal processing

data under the supervision of the controller, informing the persons concerned, the method of processing properly exercised rights of the persons concerned, as well as to verify the functioning of the technical and the organizational mechanisms in place to fulfill the responsibilities of the competent authority so as to: the lawfulness of the processing of personal data in the national part of the Schengen area has been verified of the second generation information system within the performance of the tasks of the Police Force of the Slovak Republic for the purposes of

Art. Regulation (EU) No 24 of the European Parliament and of the Council 1987/2006, on the basis of which processed data on third - country nationals in connection with refusal of entry, or residence, as well as according to Art. 36 Council Decision 2007/533 / JHA, according to which they are processed data on persons and objects in the N.SIS II for discreet or targeted purposes

control. Based on the outcome of the inspection in the part focusing on the procedures of border guards and the Aliens Police in the processing of personal data of data subjects in the N.SIS II Office stated that the processing of personal data complies with generally binding legal regulations.

The inspection in the Computing Center of the Ministry of the Interior of the Slovak Republic was focused on the security of personal data processing with emphasis on the functionality of technical and organizational mechanisms, processing of personal data under the supervision of the controller and keeping records so-called security measures for information-technical and organizational security of personal data processed in the premises of the data center (storage and communication servers, acquisition procedures and provision of personal data, etc.). Based on the result of the related part of the inspection the Office noted a high level of security of personal data stored and processed on the data center servers, proper log management, as well as overall processing compliance personal data with generally binding legislation.

In accordance with Art. Regulation (EU) No 32 of the European Parliament and of the Council. 603/2013 on the establishment Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) no. 604/2013 laying down the criteria and mechanisms for determining the Member State responsible for examining the application for international protection lodged by the national third country or stateless person in one of the Member States, and Member States' law enforcement authorities and Europol for comparison with the data in the system Eurodac for law enforcement purposes and amending Regulation (EU) No 1077/2011, which a European Agency for the Operational Management of Large-Scale Information Systems is hereby established in the area of freedom, security and justice, an obligation arose on 20 July 2015 carry out an annual review of the processing of personal data for law enforcement purposes and comparing the fingerprint data with the data stored in the central system. Control processing of personal data within the national access point of the information system AFIS-Eurodac was aimed at verifying the lawful processing of personal data within the

national access point, the use of the communication infrastructure in processing
personal data in accordance with the principles of personal data processing, security of processing
personal data, processing of personal data under the supervision of the controller, information
and the manner in which the rights of the persons concerned are properly exercised, as well as the verification
functionality of technical and organizational mechanisms affecting truthfulness, correctness
and the timeliness of personal data. AFIS-Eurodac information system operator
is the Ministry of the Interior of the Slovak Republic, has ensured the fulfillment of related duties
through the national access points established within the Criminalistics Experts Institute of the Presidium of the Police Force,
the Border and Alien Police Office of the Presidium
Police Corps and the Migration Office of the Ministry of the Interior of the Slovak Republic. Control
processing of personal data in the AFIS-Eurodac system was carried out in 2018
in the conditions of the Criminalistics-Expertise Institute of the Presidium of the Police Force. Based on
the result of the control of the procedures of the Ministry of the Interior of the Slovak Republic in the processing of personal
data

data in the automated European fingerprint identification system, the Office noted
compliance of personal data processing with generally binding legal regulations.
In accordance with Art. 40 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016
on the European Union Agency for Law Enforcement Cooperation (Europol), which
Council Decisions 2009/371 / JHA, 2009/934 / JHA, 2009/935 / JHA are hereby replaced and repealed,
2009/936 / JHA and 2009/968 / JHA, the Office is obliged to carry out regular inspections of its activities
Europol National Central Office or the Europol National Liaison Officer in processing
personal data. The inspection at the Europol National Central Office focused on principles and legality
processing of personal data within the national part of the Europol Information System,
on the security of personal data processing with emphasis on the functionality of technical,
organizational and personnel mechanisms, as well as the processing of personal data under

under the supervision of the operator so as to verify the admissibility of the transmission and search
personal data, as well as the communication of such data to Europol and the verification that such
the search or notification does not prejudice the rights of the persons concerned. Based on
the result of the related part of the inspection focused on the procedures of the Ministry of the Interior of Slovakia
Republic in the transmission and retrieval of personal data, as well as in the communication of such data
The Office has noted that Europol has processed personal data with generally binding ones
legislation.

7.2.3 Checks on suspicion of a breach of personal processing obligations
data

Selection of complaints based on suspected breaches of personal processing obligations
The data focuses on the processing activities of both the public and private sectors that they generate
increased risk of unauthorized interference with the rights and legally protected interests of those affected
taking into account the development of technologies used in the processing of personal data
particularly (but not only) in areas where errors have been repeatedly identified in the past
operators or intermediaries in setting personal processing conditions
data and their subsequent compliance.

7.2.3.1 Foreign bank branch

The inspection in question focused on the compliance of the processing of personal data with the principles
processing of personal data, conditions of lawful processing, conditions of expression
consent and fulfillment of the information obligation in the processing of personal data of clients for the purposes
setting up and maintaining their accounts, issuing debit payment cards, as well as marketing
purposes. In relation to the document to which the inspected person was to provide information
during the on-the-spot inspection, it was found that
when obtaining personal data from the data subject, no information is provided to that person,
resp. are provided to the data subject only at his or her request. In line with the principles of transparency
and justice, it is desirable that information on the processing of personal data be given to the data subject

provided before their acquisition, but at the latest at the time of their acquisition. Control

terminated by the inspection protocol, a non-disclosure error was found

information to the data subjects when obtaining personal data (directly) from the data subject;

no deficiencies were found in relation to the other parts of the subject matter.

7.2.3.2 E-shops

Control of the processing activities of two online stores operating in the territory

Of the Slovak Republic was focused on the consistency of the collection of personal data at a distance and their

further processing with the principles of personal data processing, to meet the condition of them

lawful processing, conditions for expressing consent, fulfillment of information obligation

and obligations related to the involvement of the intermediary. Controlled persons in progress

the inspections have not shown that they require the consent of the persons concerned in accordance with the Regulation, whereby

one inspected person has not proved the very existence of the consent of the person concerned, resp.

processing of personal data for the purpose of sending the questionnaire was based on a non-transparent

(confusing, misleading) obtaining “disagreement” of the data subject, and the other person

did not allow the data subjects to freely consent or disagree with the processing

personal data for the purpose of sending information about news, special offers, discounts

and price promotions. The procedures applied by the audited entities conflicted with the principles

legality, justice and transparency. At the same time, it was found that one checked

the person in the position of the operator entrusted the processing of personal data to the intermediary

(law firm), which has a privileged (ex lege) position in the practice of advocacy

operator. Both inspections were completed by an inspection protocol.

7.2.3.3 Fees for personal data protection

The subject of the inspection was the processing activities of the housing cooperative based on the diction of the law

on the ownership of flats and non-residential premises. Inspected person by the representatives of the apartment owners

has announced its intention to charge a reasoned data protection fee
consisting of the increased administrative burden generated by the consistent application of the Regulation
and the law. The inspected person based on negative reactions from apartment owners
and non-residential premises has finally decided to abolish the fee; fee
for the protection of personal data, which the owners of flats and non-residential premises have already paid, he had
be returned in the annual accounts. The inspected person in the position of the operator was according to
Regulations are required to take appropriate technical and organizational measures to ensure compliance
processing of personal data with the requirements of the Regulation. From the related provisions
No operator shall be entitled to reimbursement of the costs associated with the Regulation
with the fulfillment of their own duties, resp. the Regulation itself declares the right of the persons concerned to
protection of their personal data and ensuring the protection of personal data
to the operator as his gratuitous obligation. As a condition of protection
personal data by paying an illegal fee is a flagrant violation of the principles of legality
and justice provided for in the Regulation, the inspection was terminated by the inspection protocol.

7.2.3.4 Hospital

During the period under review, the Office checked the processing of personal data by the provider
health care. The inspection focused on the consistency of the processing of personal data
with the principles of personal data processing, the conditions of lawful processing,
the conditions for expressing consent and the conditions for processing specific categories of personal data
data, fulfillment of information obligations, fulfillment of obligations arising from the relationship between
operators and intermediaries, processing on behalf of the operator
or intermediary and the designation of the responsible person. No inspection was found
shortcomings; the inspection was terminated by the inspection record.

7.2.3.5 Camera systems

Based on suspicion of a breach of obligations established by the Regulation and the law
(anonymous submissions, suggestions from persons other than the persons concerned and media coverage) was

six inspections were carried out. In addition to two natural persons, four include this group of controls

cities and municipalities operating camera systems. Cities and municipalities as operators
camera systems were included among the inspected persons in the context of continuity with the plan
inspections carried out by 24.05.2018. All inspections of camera systems were focused
on the principles of personal data processing, provision of information in the collection of personal data
from the persons concerned, the definition of the legal basis and, in the case of natural persons, etc.
to examine the processing in the light of the material scope of the General Protection Regulation
data.

According to the division of CCTV operators into natural persons and cities (municipalities) was
in the case of two natural persons in the evaluated period, the inspection ended with a record
on control. In both cases, the monitoring of private land was qualified as
processing of personal data in the context of a purely personal or domestic activity which does not fall within
within the scope of the General Data Protection Regulation.

In the case of four towns and villages, it was found in relation to the operation of camera systems
in three cases non-compliance with applicable legislation and inspections were terminated by protocols
on control. The shortcomings concerned in particular the failure to provide accurate information to the persons concerned
(failure to provide information on the legal basis for processing and failure to provide information on site
entry into the monitored area), thereby violating the rights of the persons concerned and consequently
also in breach of certain principles of personal data processing. Preservation was also a problem
camera footage for longer than necessary to achieve the specified purpose
processing of the personal data of the persons concerned by the camera system.

7.3 Conclusions arising from the Office's control activities

In general, the results of the controls carried out during the period under review show an effort
operators to ensure compliance with the provisions of the Regulation and the law, but at the same time they are
Some categories of operators have also been identified, which need to be increased

attention in the coming period.

The control activity of the Office, the basic mission of which is to act preventively

personal data processed by controllers and their intermediaries is therefore desirable

to support other forms of the Office's activities, in particular due to a fundamental change in legislation

processing conditions represented by the Regulation and the law applicable in the territory of Slovakia

Republic shall apply from 25.05.2018.

The basic precondition for achieving compliance with the requirements of the Regulation and the law

is a general identification with the intention that this legislation formalizes.

30

8 PERSONAL DATA PROTECTION PROCEDURE

The purpose of personal data protection proceedings is to determine whether the rights of individuals have been violated

during the processing of their personal data or the provisions of the Regulation have been violated, or

of the law. In the event of deficiencies being identified and, where appropriate and expedient, impose remedial action,

possibly a fine. The provisions of the Administrative Procedure Code apply to personal data protection proceedings

of order.

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 period under review, the Office forwarded a total of 26 submissions to another, competent administrative

authority for action and decision.

Personal data protection legislation allows the Office to file in an exhaustive manner

postponed in certain cases. The most common reason for the postponement was unfounded

submission, when it was already clear from the evidence submitted by the person concerned that the infringement had been

infringed

personal data protection legislation.

Act no. 122/2013 Coll. regulated the institute of deferment of filing in the optional

form.

In accordance with the law, there must be a filing if one of the grounds for postponing the filing occurs

deferred obligatory.

A total of 287 submissions were postponed during the period under review.

The Office, in the framework of supervisory activities, conducts proceedings on the protection of personal data with the aim of

protection

the rights of natural persons against unauthorized interference with their private life during processing

their personal data, while also examining compliance with the obligations laid down

Regulation and law. If it finds a violation of the rights of the person concerned or a breach of obligations

when processing personal data, by decision, if justified and expedient

the operator or intermediary to take measures within

elimination of deficiencies and causes of their occurrence, if any, depending on the severity

imposed a fine. Otherwise, personal data protection proceedings

stops.

The privacy proceedings are under way

 at the proposal of the proposer,

 or on the Office's own initiative.

The Office shall initiate proceedings on its own initiative

 on the basis of an initiative,

 on the basis of the results of an inspection which identified deficiencies, or

 on the basis of the Office's own activity on suspicion of a breach of the law

regulations in the field of personal data protection, such as proceedings initiated without a proposal.

In the monitored period, the Office initiated a total of 126 administrative proceedings, of which

 78 were started at the request of the person concerned,

 25 initiated on the basis of an initiative,

 8 started on the basis of the results of the inspection, which identified deficiencies a

 15 proceedings were conducted by the Office on its own initiative on suspicion of a breach of the law

regulations in the field of personal data protection.

31

In 2018, the Office initiated administrative proceedings

 on the basis of a proposal in 45 cases,

 on the basis of an initiative in 11 cases,

 based on the results of the inspection in 1 case,

 and on its own initiative in 7 cases.

In 2019, the Office initiated administrative proceedings

 on the basis of a proposal in 33 cases,

 on the initiative of 14 cases,

 based on the results of the inspection in 7 cases,

 and on its own initiative in 8 cases.

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

Year

From 25.5.2018 to

12/31/2018

From 1.1.2019 to

5/24/2019

Together

Based on

proposal

Based on

initiative

Based on

inspection results

From my own

initiatives of the Office

45

11

1

7

33

14

7

8

78

25

8

15

Decision of the Office as the administrative body at first instance in personal protection proceedings

data is based on a reliable state of affairs. For this purpose, the Office is in proceedings for protection

personal data is entitled to request the cooperation of anyone, while in the evaluated

period, the Office requested cooperation a total of 601 times. In personal data protection proceedings,

there have been three cases where the entity from which co-operation has been requested

he did not react to it and did not cooperate with the Office even after being called upon to fulfill its obligations

(in the given cases, fine or disciplinary proceedings were initiated against the entities

fine).

In the context of raising public data protection awareness, cases where

resp. the results of the proceedings were often also of interest to the media. The Institute of Legal Representation was

used in a significant number of cases during the period under review, with the exception of cases

when all the parties to the proceedings were represented by lawyers.

The most common subject of personal data protection proceedings was examination or processing

personal data of the data subjects were violated by cameras

regulations in the field of personal data protection.

One of the most common violations was the processing of personal data in conflict

with the principle of legality when personal data were processed without a legal basis,

resp. contrary to the legal basis and processing contrary to the principles of integrity and confidentiality,

which was related to the failure to take appropriate security measures.

In the proceedings on personal data protection, several pieces of evidence were used in the evaluated period

the means by which the true state of affairs can be ascertained and, for that purpose,

in more complicated matters, the inspection was used directly by the operator or

intermediary. Inspection has proven to be an effective means of establishing the true

and complete condition, especially when inspecting the cameras at a location where it has made it possible to reliably

determine the method

and individual aspects of monitoring and, on that basis, to assess the invasion of privacy accordingly

monitored persons. In order to find out the real state of affairs, there is also a relatively high number

requests for co-operation through which they were provided in the file

in particular documentary evidence. The persons concerned submitted mostly precise proposals containing all of them

required requirements, with only a minimal amount to be called upon

rectification of deficiencies in the application (only sporadically the petitioner his application to initiate proceedings after

not completed).

Personal data protection proceedings, as a type of administrative procedure, are characterized by sensitivity

the issue of respect for and protection of fundamental rights and freedoms

in the field of personal data.

The personal data protection procedure is a non-public procedure, which involves several

peculiarities that complement, resp. extend the legal regulation of Act no. 71/1967 Coll., Or there

where necessary, exclude the application of Act no. 71/1967 Coll. These specifics are important

in terms of the correct application of personal data protection, with the Office

at first instance, where appropriate and necessary. Such

a special institute in proceedings on personal data protection is e.g. secrecy of identity

the petitioner in cases where his or her rights and rights could be violated

protected interests (as the person concerned), or negative action by

operator. The secrecy of the petitioner's identity found its justification and the persons concerned

in the interest of their protection, they used it in the evaluated period in the proposals they demanded

protection of their rights and the interests protected by law in the exercise of their profession.

During the period under review, operators often in the course of personal protection proceedings

data before attempting a substantive decision, they tried to dispose of the findings voluntarily

shortcomings in the processing of personal data and to adopt effective safeguards

lawful processing of personal data. Remedial action taken and implemented

As a rule, the participants in the proceedings informed the Office of the identified deficiencies within the imposed deadlines.

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

in the processing of personal data, which is also reflected in the provisions of Art. 1 par. 3 Regulations.

It responds to that Regulation by establishing cooperation and consistency mechanisms in order to:

a consistent and similarly high level of personal data protection was guaranteed in each

Member State, regardless of the place of residence of the person concerned.

9.1 Cooperation mechanism

The Regulation regulates cooperation between supervisory authorities, whether the need for mutual

cooperation arises in the investigation of a specific suspected breach of protection

personal data or in another activity of the supervisory authority (eg dealing with legal issues,

providing consultations). Given that the rules of cooperation are regulated directly

Regulation, no further specific agreements are required between Member States

States for this purpose.

9.1.1 Cross-border processing

Pursuant to Art. 55 Regulations, 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

Art. 4 pt. 23 of the Regulation (a) the processing of personal data which takes place in the Union in context

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

state; or (b) the processing of personal data which takes place in the Union in the context of activities

the only establishment of the operator or intermediary in the Union, but which substantially

affects or is 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

with the mechanism of a single contact point (so-called one-stop-shop) regulated in Art. 56 par. 1

Regulations under which the supervisory body is the principal place of business or sole

the establishment of the operator or intermediary authorized to act as chief supervisor

the authority for cross-border processing carried out by that operator,

resp. intermediary. In accordance with Art. 4 point 22 of the Regulation other supervisory authorities will be

for such 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) concerned

persons residing in the Member State of that supervisory authority are or will be significantly affected

likely to be significantly affected by processing; or (c) the complaint is made against that

supervisory authority.

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

(Internal Market Informational System), under the

which the exchange of information on a specific

processing and specific suspicion of a breach of personal data protection, resp. as long as

the investigation was opened on the basis of a complaint from the person concerned as well as the content of this particular

one

complaints. The exchange of information takes place in English.

34

During the period under review, 1,035 notifications were received by the Office in IMI

designation of the supervisory authority concerned. Office on the basis of a careful assessment

in each case, assessed that it was the supervisory authority concerned in 421 cases;

most often on the grounds that the processing of personal data in question significantly affects or

likely to significantly affect the persons concerned residing in the territory of the Slovak Republic.

The most common were operators such as Facebook (and its platforms Instagram, Youtube),

Google, Paypal, airlines. In some cases, the Office was also affected because

the operator or intermediary is established in the territory of the Slovak Republic, as

e.g. in the case of Amazon or Microsoft, which have in the territory of Slovakia

one or more establishments. If the Office has assessed that it is the supervisory authority concerned

authorities, identified its position in IMI and followed up the case. In accordance with Art. 60

The Office commented on the requests of the head of the supervisory authority, as appropriate,

to its procedure and to the results of the investigation, and also commented on the draft decision. Unless

the Office would be the supervisory authority concerned because it had received a complaint, the Office would

acted as a contact point for the person concerned and notified his decision.

In the monitored period, a total of 19 submissions containing elements were delivered directly to the Office

cross-border processing (of which 15 proposals from data subjects and 4 initiatives). These submissions

were delivered either from foreign persons or were directed towards foreign operators,

among others, for example, to operators established in India or Ukraine. Office

instructed foreign complainants in English on the merits of the proposal

and the obligation to use the Slovak language in personal data protection proceedings. If filed
established a reasonable suspicion of a personal data breach, the Office made the allegations
also checked in cooperation with foreign operators. In one case, the Office
received in IMI and dealt with it in cooperation with the Dutch supervisory authority
authority which was the lead supervisory authority for the processing in question.

9.1.2 Mutual assistance

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 from other supervisory authorities.

During the reporting period, the Authority received 21 requests from other supervisors in IMI
for cooperation within the meaning of Art. 61 Regulations. The highest number of applications (five) was received from the
Hungarian
supervisory authority, four came from the Maltese supervisory authority, three from the Czech supervisory authority
and two applications from the Polish supervisory authority. In the applications in question, the supervisory authorities
asked the Office for its legal opinion, in particular as regards the interpretation of the provisions of the Regulation.
The requests concerned e.g. designation of the responsible person by trade unions, interpretation of Art. 26
and Art. 80 Regulations and implementation of Art. 87 Regulations. The Hungarian supervisory authority was interested in the
practice
the Office in controlling the operation of camera systems (ie how the Office applies the Regulation
for camera dummies, as is the case when cameras capture private land or
neighbor's land, and others). Some supervisory authorities have informed the Authority in this way
on the received notification of a personal data breach and the Polish and Czech supervisory authorities
used this method to consult a specific case before launching the onestop-shop mechanism.

During the reporting period, the Office sent 1 request for cooperation in IMI pursuant to Art. 61
Regulations concerning the independence of the supervisory authority in the processing of data by the supervisory authority

authorities in a state cloud and addressed to the supervisory authorities of all Member States.

However, the Office also used other forms for mutual cooperation with other supervisory authorities

communications such as IMI (email, written and telephone), which he 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 implement joint

supervisory operations, including joint investigations and joint actions in the field

enforcement. During the period under review, the Office did not initiate or accept a request for execution

such joint supervisory operations.

9.2 Consistency mechanism

An important feature of the Regulation is its consistent application in order to achieve this goal,

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 Opinion of the Committee

The purpose of Article 64 of the Regulation is for the Committee to deliver an opinion where it is competent

the supervisory authority plans to take specific measures. To this end, the Authority should have a Committee

notify its draft decision. The regulation regulates the cases in which the supervisory body is obliged

to ask the Committee 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).

The Authority requested the Committee's opinion during the period under review, as it planned to adopt the list

processing operations which are subject to a protection impact assessment requirement

data, so-called blacklist of processing operations. The committee delivered its opinion 21/2018

to the proposed list of the competent supervisory authority of Slovakia in this matter on 25 September

2018. The Office subsequently adopted a blacklist of processing operations

9.2.2 Settlement of disputes by the Committee

Dispute settlement by the Committee allows the Committee to take a binding decision to secure

consistent 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 Committee (Article 64 of the Regulation);

 The Authority did not follow the Committee's opinion (Article 64 of the Regulation).

During the period under review, the Committee did not resolve the dispute with the Office.

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.

These measures may not exceed a period of three months. In this case, he is affected

the supervisory authority is obliged to inform the other supervisory authorities, the Committee and the EC.

If the Authority considers that definitive action is needed urgently, it may

request the Committee for an urgent opinion or a binding decision. Every supervisor

the institution may request an urgent opinion or a binding decision from the Committee in cases

where the competent supervisory authority has not taken appropriate action and there is an urgent need to act.

The Office did not apply this article during the period under review.

10 SANCTATION

Sanctions for violation of Regulation and Act no. 18/2018 Coll. are a fine and a disciplinary fine.

Sanctions are given in the given legal norms optional, ie. that not everyone found

the infringement must automatically end with the imposition of a sanction. The Office imposes fines and penalties

fines depending on the circumstances of each individual case. Office when deciding on the imposition fines and the determination of its amount shall take into account, in particular, the nature, gravity and duration of the infringement, the number of the persons concerned, the extent of the damage, if any, and any breach of personal protection data and the measures taken to mitigate the damage suffered by the persons concerned. Office it also takes into account previous breaches of personal data protection with the Office in rectifying the breach and mitigating the possible adverse consequences of the breach, the category of personal data concerned by the breach and the way in which the Office deals with the breach personal data protection.

10.1 Fine

In the monitored period, the Office for violations of legislation on personal protection data lawfully imposed 38 fines in the total amount of 132,600 euros. In the observed period the Office collected a total of EUR 129,638.89 in fines. The average fine was 3 489, - eur. The Office imposed the lowest fine of EUR 500 on the operator for non-cooperation. The Office legally imposed the highest fine in the amount of EUR 40,000 to the controller for breaching the security of personal data processing.

Overview of fines imposed and collected in the monitored period

Watched period

Count fines

Total height legally fines imposed in Euros

5/25/2018

until

5/24/2019

38

132 600

Average amount of the fine

rounded to the nearest Euro

up

Total selected on

fines in Euros

3 489

129,638.89

The fine, as a type of sanction, served a repressive as well as a preventive function in the period under review.

In imposing it, the Office took into account, inter alia, the status of the entity and its activities as well as the impact

the amount of the fine for its continued existence. In connection with the imposition of fines during the assessment

period for breaches of personal data protection law may be

state that the fines imposed did not have liquidating effects.

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 it does not ensure adequate conditions for its performance. The Office may impose a disciplinary fine

also to a person who is not an operator or intermediary for not providing

required co-operation of the Office in the performance of supervision. In the period under review, the Office imposed four

disciplinary fines in the total amount of EUR 9,500, of which two in the amount of EUR 500 for failure to provide

cooperation and two in the amounts of EUR 3,500 and EUR 5,000 in connection with the obstruction of the inspection.

10.3 Selected cases from the supervisory activities of the Office

10.3.1 Postponements

10.3.1.1 Fulfillment of the information obligation towards the person concerned

In 2018, the Office received a proposal from the person concerned against the company to the person concerned sent a document informing her that, as an operator, she was processing her personal the data for which they process them, the categories of data processed, the recipients, the time retention, the rights of the person concerned, the right to lodge a complaint with the Office. Affected person upon delivery letter, the company suspected that its personal data were being misused because of their personal data the company did not provide or give consent to the processing. The letter showed her personal the data are processed for the purpose of recovery of the claim. The person concerned objected that for a long time has no contractual or non-contractual relationship with any organization against which it would a financial obligation has arisen.

It was apparent from the content of the company's document that, as an operator vis-à-vis the person whose personal data have already been processed in the previous period, by application of the Regulation from 25.05.2018 fulfilled the information obligation to the necessary extent according to Art. 13 and 14 of the Regulation.

The Office further verified that the controller obtained the personal data of the data subject for processing on the basis of a contract on the assignment of claims from the original creditor and for the processing of personal due to the performance of the contract due to late payment of the data subject.

The purpose of processing the personal data of the data subject was to manage the claim, whereby the legal basis for the processing of personal data was the legitimate interest of the controller.

Given that the purpose did not materialize at the time the application was lodged, settlement of the claim against the person concerned, his personal data legitimately the operator processed. The assessment of the case did not reveal any facts that would indicate the procedure operator in breach of the Regulation and therefore the proposal of the person concerned was postponed as manifestly unfounded.

10.3.1.2 Disclosure of personal data in a public decree

In 2018, the Office received a proposal from the person concerned against the operator, which was

village. In the application, the data subject objected to the unauthorized disclosure of his personal data

on the website of the operator and his physical official notice board in the posted appeal,

filed by the person concerned in the construction proceedings. The person concerned stated that the operator

He placed her appeal on the website and on the official board in order to allow other participants

proceedings could comment on the objections. The person concerned considered that the parties could

comment on the content of its submission and not on its person, therefore the operator should ensure protection

her personal data, for example by anonymisation.

The Office documented the evidence from the operator's website and found that the document was

published in the public notice in order to notify the participants of the construction

the appeal procedure and the invitation to submit observations within a specified period. The document in question

should be published for 15 days on the official notice board in accordance with a special regulation.

The Office found in the investigation that the public decree together with the appeal of the person concerned (participant

construction proceedings) was published on the official notice board of the municipality during the legal deadline. The purpose

processing of the personal data of the data subject in such a way that his or her personal data were

appeal published on the official notice board of the municipality, was the service of the document (appeal against

building permit) to other participants in the construction proceedings by a public decree within the meaning of

special regulation for a period of 15 days. At the end of this legal period of posting the document

on the official board of the administrative body or on the website of the administrative body, there was also

to end the purpose of disclosing the personal data of the data subject and it was necessary to terminate

disclosure of personal data in the posted document. The Office has verified that

if, on the expiry of the 15-day period, the public decree and the appeal of the person concerned were

personal data from the online and physical official board of the municipality posted. Delivery to your own

hands as well as service by public decree are equivalent forms of service of documents

in administrative proceedings, where the same applies to documents delivered in administrative proceedings in the form

of the public decree are also delivered to the participants in the administrative proceedings in question, to which this participant shall always have the right to be heard, without the intervention of the administrative authority in these documents, ie. in non-anonymized form. As no reasons were found to initiate personal data protection proceedings against the controller, the proposal was affected postponed as manifestly unfounded.

10.3.1.3 Publication of personal data in the auction notice on the Internet

In 2019, the Office received a joint proposal from the two persons concerned against an entity which: had to improperly publish their personal data on the Internet in the announcement of the auction held in 2016. The persons concerned did not identify the person to whom the proposal is directed. They attached only to the proposal document marked as "Auction notice according to § 17 of Act no. 527/2002 Coll. on voluntary auctions .... as amended ". The persons concerned stated that the disclosure of personal The data in the auction notice causes them problems in their surroundings. Auction notice contained the personal data of the persons concerned as the owners of the subject of the auction to the extent of the name, surname, maiden name, date of birth, place of residence and others related to the subject of the auction.

Whereas the request for initiation of personal data protection proceedings must contain: requisites stipulated by Act no. 18/2018 Coll., The Office invited the persons concerned to supplement missing elements of the proposal submitted by them. As the persons concerned as petitioners they did not complete their proposal within the set time limit, the Office postponed their proposal due to the fact that the petitioners did not provide the necessary cooperation at his request.

The Office follows up on the content of the incomplete proposal and found that by entering data about their persons a link to the page that contained the notification in question was found in a Google search engine on the auction, the case continued to be investigated. The found website mainly offered real estate - reality. The Office called for the cooperation of the operator of the given portal. The Office found that The announcement of the auction was part of the advertisement of the legal entity, taking public display The ad for visitors was canceled in 2016 and based on the fact that the company as

the portal operator is entitled to remove the notification in this particular case

about the auction from its portal, has taken the necessary steps to prevent further interference

to disclose the personal data of the persons concerned in the auction notice.

10.3.1.4 Expert opinion prepared from medical documentation

In 2019, the Office assessed a proposal directed against an operator who, as an expert

based on a court ruling, he prepared an expert report on the petitioner's health and had

in so doing, infringe his right to the protection of personal data by including in an annex to the report

data from the applicant's medical records, to a large extent, including information

which are not necessary as evidence. The Office found that the objected processing was reasonable

legal basis established by Act no. 576/2004 Coll. on health care, services

related to the provision of health care and to amend certain laws

as amended and Act No. 382/2004 Coll. about experts, interpreters

and translators and amending certain laws as amended (hereinafter

only "Act no. 382/2004 Coll. ”). Due to the petitioner's objections to the scope of personal

data in the annex, the Office assessed the expert opinion submitted by the applicant in terms of whether

the operator has complied with the principle of data minimization, ie whether the scope of personal

data in the annex corresponds to the purpose according to § 17 par. 4 letter e) and par. 5 of Act no. 382/2004 Coll.,

with the result that, in the given case, the scope of the processed data corresponds to the established purpose,

which is to ensure the verifiability of the expert opinion. For the above reasons

the Office found that the application was manifestly unfounded and postponed it.

10.3.2 Procedures

10.3.2.1 Exercising the data subject's right of access to personal data

In 2018, the Office received a proposal from the person concerned against the operator with whom

exercised its rights in the processing of personal data. The person concerned requested the operator

for access to their personal data processed through camera recordings

and audio recordings on a given day in connection with the performance of a traffic control. Considering that
the operator did not comply with the request of the person concerned and provided him with only information that the records
camera systems and audio recordings are stored for a period of 15 days and are provided
in particular to law enforcement authorities, the person concerned considered this to be the case
operator for infringing his rights.

According to recital 63 of the Regulation, the data subject should have the right of access to personal data,
obtained and the right to be exercised easily and at reasonable intervals,
so that you are aware of the lawfulness of the processing and can verify it. Pursuant to Art. 23 Regulations
to limit the rights and obligations arising from Art. 12 to 22 Regulations governing rights
concerned, possibly only through a legislative measure in European Union law
or in the law of a Member State. The investigation revealed that the personal data of the data subject were not
processed in the operator's camera system. The processing of the personal data concerned
however, by means of an audio recording made at the time of the transport inspection, which
the operator disposes of it within 15 days. At the time of receipt of the application, the operator had
persons in the matter of the right of access to personal data, the audio recording in question was available and was therefore
obliged to process the application in accordance with the provisions of the Regulation. The Office did not question the
fulfillment
the obligation of the operator to provide or make available the prepared camera or audio
records to bodies active in criminal proceedings, courts, or other eligible entity, however
in this case, it was a question of fulfilling a different obligation, namely the obligations of the operator
in relation to the exercise of the data subject's rights of access to his or her personal data, which
the operator obtained for processing in its information system defined on it
purpose. The Office imposed the operator on the basis of the detected violation of the right of the person concerned
corrective measures as well as a fine.

10.3.2.2 Finding documentation with personal data in the collection yard

In 2018, the Office received an e-mail regarding a suspected breach of processing obligations

personal data, which were found in documents thrown in the premises of the collection yard of the municipality.

For example, the sender of the e-mail also discovered loan agreements with personal documents in the discarded documents data. Given that he took this found documentation from the collection yard and announced it the Office was subsequently secured by the Office to its premises as evidence.

41

The Office initiated proceedings on the protection of personal data on its own initiative against the person responsible to the operator. The discarded documentation included, inter alia, currency loan agreements with surnames, birth numbers, identity card numbers, permanent residence addresses, employers, also contained copies of official documents such as an identity card, birth certificate. The contracts found were from the period of 2006, 2009, 2011. The persons concerned were customers buying goods in installments who applied for a loan.

According to the principle of integrity and confidentiality within the meaning of Art. 5 par. 1 letter f) Regulations must be personal data processed in a way that guarantees adequate security of personal data, including protection against unauthorized or illegal processing and accidental loss, destruction or damage, through appropriate technical or organizational measures. The Authority's investigation found that the operator was responsible for safe disposal personal data in documents, which is one of the processing operations with personal data. Despite the fact that, according to the operator, it was old personal data, it can be stated that it is irrelevant whether any of this personal data was already out of date or untrue, the controller is responsible for the safety of processing throughout the processing cycle (from their acquisition only after liquidation). The information gathered showed that there was no mistake in systematic processing of personal data, but in this individual case it was a one-off error in securing the destruction of personal data. The Office ordered the present case corrective measures and a fine to the operator.

10.3.2.3 Loss of personal documents

In 2018, the Authority adopted a joint proposal of the two persons concerned against the operator,
requested to provide a residential social service. The persons concerned had
provide the operator with his personal data in documentary documents in this connection,
in particular on applications for social services and the necessary documents. Touched
after some time, the persons have found that these documents are not with the operator. They acquired
suspected breach of the protection of their personal data.
According to the principle of integrity and confidentiality within the meaning of Art. 5 par. 1 letter f) Personal data regulations
must
be processed in a way that guarantees adequate security of personal data, including protection
from unauthorized or illegal processing and accidental loss, destruction or
through appropriate technical or organizational measures.
The operator is further obliged to take steps to ensure that each natural person
acting on his behalf who has access to personal data has processed that data
only on the instructions of the operator.
The Office found out through the investigation that the operator processed the personal data of the persons concerned in
paper
form in its information system to the extent and for the purpose established by a special law
governing the provision of social services. Personal data were processed by the operator
through staff whom he has demonstrated to be processed on his basis
instructions and at the same time the controller had received reasonable in the processing of personal data
precautions. The operator performed an internal audit of the matter, investigated the matter and accepted it
corrective measures (including staff in which he terminated his employment)
with the responsible employee). In this case, the Office found a breach of security
processing of personal data and, in the light of the findings, imposed on the controller
measures.

10.3.2.4 Posting a photo on the social network Facebook

In 2018, the Office accepted the proposal of the legal representative of the affected person (child)

against the operator who posted a photo of the child on his official Facebook page

page. By exercising the right of the person concerned, the legal representative requested the operator to delete

photos from the internet, as the operator for such processing of personal data

does not have the consent of the person concerned or any other legal basis. Operator equipped

request the person concerned by informing him of the reasons why the photograph cannot

delete.

The Office found in the investigation that the operator concludes with the legal representatives of the persons concerned

written contracts for the purpose of providing their childcare services, through

from which it obtains personal data. At the same time, the operator fulfills its information obligation towards

concerned. In this particular case, a photo of the child was to be taken

operators during the activities and its publication took place with the consent of the law

the representative provided in this individual case during the communication.

The controller has demonstrated that the consent of the data subjects to the processing of personal data

obtained in writing, via e-mail or chat. However, the Office in this case

found that the operator had failed to fulfill its information obligation under the Regulation

to a sufficient extent.

If the controller has determined a legal basis for the specific processing of personal data, which is

consent of the person concerned, he must take into account that the person concerned may at any time give his consent

call off. If the controller has also determined another purpose of processing, namely proof, application

or defending their legal claims, they must also determine the appropriate means of security

preservation of evidence for the purposes of criminal or civil proceedings for the time necessary,

that the related processing of personal data does not infringe the principles within the meaning of

Regulations. In this particular case, the operator continued to publish the photograph of the child

after revoking the consent of the person concerned on the grounds that he or she is to serve as evidence for the authorities

active in criminal proceedings. The Office therefore found a violation of the principle of legality under Art. 5 par. 1 letter a) Regulations, as the controller revokes the consent to the disclosure of personal data and by applying for its deletion, he continued to publish the photograph with the portrait, while being entitled the operator's interest in its further publication on the Internet did not outweigh the right of the person concerned (child) over the protection of his personal data. The Authority did not impose a corrective action on the operator measure, as the operator ensured the deletion of the photograph from the Internet and its during the proceedings processing solely for the purpose of proving, applying or defending its legal claims. However, the Office imposed a corrective measure on the operator in relation to the fulfillment of the information obligations towards the persons concerned.

10.3.2.5 Indication of the date of birth on the delivered envelope

In 2018, the Office initiated proceedings on the protection of personal data on the basis of the proposal suspicion of unauthorized processing by the Bailiff the date of birth on the envelope received.

One of the legal bases for the processing of personal data is the legitimate interest of the controller or a third party. On the basis of the documents and evidence gathered during the proceedings, the Office found that that the Bailiff's Office delivered the petitioner a document in an envelope stating, in addition to the name, surname and address as well as her date of birth. In this case, the Office evaluated the proceedings operator in accordance with Art. 6 par. 1 letter f) Regulations, as the proportionality assessment

between making the date of birth available and ensuring security of processing (secure delivery of the consignment to the addressee and not to another person) the Office found that the envelopes before third parties prevail over disclosure of date of birth as personal data, which is not a special category. As the Office did not find an infringement of the appellant's rights in the proceedings (the person concerned) or a breach of the Regulation, he stopped the proceedings.

10.3.2.6 Unauthorized processing of a telephone number

In 2018, the Office initiated proceedings on the protection of personal data on the basis of which

city police beyond the scope established by Act no. 564/1991 Coll. on the General Police as amended later regulations (hereinafter referred to as the "Municipal Police Act") obtained and used a telephone number the notifier's wife in connection with the disputed motor vehicle parking.

The whistleblower said that his wife was called by an unknown man who urged her to she immediately parked her vehicle. Office in order to ascertain the complete and actual state of affairs asked the city police for a statement stating that the city police operations officer at the request of a city police patrol sent to the scene, he found out in the records motor vehicle data of the person concerned in relation to the parked vehicle, giving him the mobile phone number of the registered owner of the motor vehicle was also announced. Office stated that in accordance with § 24 par. 3 of the Municipal Police Act, the telephone number does not belong among data that the city police is authorized in connection with the parking of a motor vehicle from the registration of motor vehicles. By processing a phone number beyond the range specified a special law violated Art. 6 par. 1 of the Regulation, as the personal data was processed without a legal basis. Subsequently, the Office imposed on the operator ensure that the telephone number is deleted from the file kept by the city police in the matter.

10.3.2.7 Unauthorized disclosure of data on the website

In 2018, the Office initiated proceedings on personal data protection on the basis of a proposal in which the petitioner stated that the city had unlawfully published his personal data on its website data in the range of surname, address and information on recurring info requests addressed city in the order and personal data in the range of name, surname and recurring information requests, complaints and suggestions in an addendum to the contract for the provision of legal services.

In the proceedings, it was found that the city disclosed the petitioner's personal data as part of its performance published obligation stipulated by Act no. 211/2000 Coll. on free access on Information and on Amendments to Certain Acts (Freedom of Information Act) (hereinafter only "info law"). The city could disclose personal information only if it did the info law

with the prior written consent of the person concerned. Office

After examining the complete file, he found that the city in question was personal

published the data of the petitioner in violation of the info law, resp. without the consent of the petitioner

contrary to the principle of legality. On the basis of the detected violation, the Office imposed

corrective action to the operator as well as a fine.

REMEDIES AND DECISION-MAKING

Against the decision of the Office in the matter of personal data protection proceedings, against the decision

on the imposition of a fine as well as against a decision not to disclose information resp. decision

an appeal may be lodged on the non-disclosure of the information - an appeal, whereby

the provisions on remedies set out in the Administrative Procedure Code shall apply in the alternative

of order. The President of the Office shall decide on the appeals lodged on the basis of

recommendations of the Appeals Commission, which may be extended or supplemented by the appellant

for another motion or for additional points within the time limit set for filing an appeal.

The President of the Office, as the appellate body, decided on a total of 30

filed appeals, of which

 13 appeals were lodged against the decision imposing a fine, or there were

both the measure and the fine imposed; of which 7 first instance decisions in terms of amount

the fines confirmed by the others as regards the amount of the fine were changed;

 of all the filed appeals, the first-instance decision was confirmed

in 16 cases.

During the period under review, the President of the Office reviewed one decision imposing measures on

elimination of identified deficiencies and causes of their occurrence outside the appellate procedure of its own

initiatives and the review has shown that there are no grounds for exceptional action

appeal.

Decision-making in the second instance also affects the decision-making activity of the Office as a liable person

according to law no. 211/2000 Coll., In which the Office either makes the required information available or issue a decision not to disclose information resp. decision not to disclose the information partly. In the period under review, the President of the Office received 1 such an appeal. Decision annulled and referred the case back to the first-instance body for a new hearing and decision.

A party to the administrative proceedings may file an appeal against a valid decision of the President of the Office an action for review of the legality of the decision. Within the material and local jurisdiction, these authorities hears at the Regional Court in Bratislava.

45

12 EUROPEAN AND INTERNATIONAL PROTECTION OF PERSONAL DATA LEGISLATIVE PACKAGE

12.1 European level

Following the adoption of Regulation and Directive 2016/680, the EC submitted a draft regulation on 10 January 2017 on respect for privacy and the protection of personal data in electronic communications and repealing Directive 2002/58 / EC (Directive on privacy and electronic communications) to ensure consistency with a uniform approach to personal data protection across the EU.

The draft e-privacy regulation will be a lex specialis in relation to the Regulation.

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 market participants. Electronic communications data means their content, such as Contents private messages, but also metadata, which includes e.g. dialed numbers, visited internet site, geographical location, call or message timing.

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 governments in the Council of the EU, which did not adopt a joint agreement

text agreement. The Bulgarian Presidency of the Council of the EU presented at the end of its term in May 2019 progress report. This report points out, inter alia, the problematic - open provisions of the draft e-privacy regulation. This is, for example, determining the scope of the proposal e-privacy regulations and regulations so that this interconnection is technology neutral and at the same time legally clear; boundaries between the reasons for electronic processing communication data and the right to privacy, including the confidentiality of communications; determination the supervisory authority responsible for monitoring compliance with the e-privacy regulation. Proposal 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.

12.1.1 European Data Protection Board

The European Data Protection Board is an independent EU body with legal personality, which contributes to the consistent application of data protection rules throughout the EEA and promotes cooperation between EEA data protection authorities. It was established pursuant to Art. 68 of the Regulation and is the successor to WP29.

The committee is represented by its chairman, who is currently the chair of the Austrian Supervisory Authority Andrea Jelinek. It consists of the head of one supervisory body of each EEA Member State and the Supervisor. The EC has the right to participate in the activities and non-voting committee meetings.

The committee shall act in accordance with its rules of procedure. The activities of the Committee are divided between 12 expert subgroups, which are divided thematically. E.g. Technology Expert Group fines, 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 11 expert subgroups by personal participation, sending written comments, participation video and body conferences, and related workshops.

The documents on which the expert subgroups are working are approved in plenary Committee. During the period under review, 10 meetings were held and the Office participated in all of them.

The greatest benefit to the public is the issuance of the Committee's guidelines on various issues.

During the period under review, the Committee issued 6 guidelines, but 2 of them are not yet final, as they are have undergone a public consultation and are in the process of being finalized. The guidelines (and other documents) are published on the Committee's website. The Office also publishes on its website these guidelines in Slovak and English.

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

12.1.2 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 measures acts. The Committee provided for in Article 93 of the Regulation shall meet on an ad hoc basis as necessary. In the evaluated The Committee met several times during the period and considered in particular the draft decision on adequacy for Japan.

12.1.3 European Data Protection Supervisor

On 11 December, Regulation 2018/1725 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on movement of such data, repealing Regulation (EC) No 45/2001 and decision no. 1247/2002 / EC.

The Data Protection Supervisor is the EU's independent supervisory authority responsible for ensuring respect for the fundamental rights and freedoms of natural persons, and in particular their right to data protection by the Union institutions and bodies. The Supervisor is responsible for monitoring and ensuring the application of the provisions of Regulation 2018/1725 and any other Union acts concerning the protection of the fundamental rights and freedoms of natural persons with regard to for the processing of personal data by the Union institution or body and for advising the institutions and the institutions of the Union and the persons concerned in all matters relating to the processing of personal data data.

The EU has created a number of European large-scale IS, the supervision of which is shared between national ones

data protection authorities and supervisors. 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 following IT systems are currently subject to this oversight model:

• Eurodac,

• Visa Information System (VIS),

• Schengen Information System (SIS),

• Customs Information System (CIS),

• Internal Market Information System (IMI).

The exercise of supervision over the protection of personal data processed in these IS is carried out in close

cooperation, either joint supervisory bodies set up by the EC and its bodies or groups for

supervisory coordination set up by the supervisor.

A representative of the Office represented the Slovak Republic in the joint supervisory bodies

and the Schengen Coordination Coordination Groups for the Schengen Information System II (SCG SIS II),

Visa Information System (SCG VIS), Customs Information System (SCG CIS), Europol (JSB

Europol) and Eurodac (SCG Eurodac). At the same time a representative of the Office during the reporting period

participated as a member of the evaluation teams in charge of the Schengen on-the-spot checks

personal data protection assessments in Estonia, Ireland and the Czech Republic.

Although there are small differences between the legal bases for these systems, in general

provide that national supervisory authorities and the supervisory officer shall cooperate to ensure that

coordinated supervision. To this end, representatives of national data protection authorities

and the Supervisor meet regularly - usually twice a year - to discuss

on common supervisory issues. Activities include, inter alia, joint

inspections and investigations and work on a common methodology. The Office during the period under review

did not attend these meetings.

12.1.3.1 Europol Cooperation Council

Europol was established by Council Decision No 2009/371 / JHA in order to provide assistance and support the competent authorities of the Member States and facilitate their cooperation in prevention of organized crime, terrorism and other forms of serious crime activities involving two or more Member States and in combating such forms crime. Council Decision No 2009/371 / JHA replaced the Convention establishing the European police authority established on the basis of Article 3 of the Treaty on European Union. From May 1 2017, the new Europol Regulation no. 2016/794.

In order to ensure the supervision of the processing of personal data by Europol, Article 45 of the Europol Regulation 2016/794 established by the Cooperation Council, which has following tasks:

- discusses the general policy and strategy regarding data protection supervision Europol and the admissibility of the transmission, retrieval and any communication of personal data Europol by the Member States,
- examines difficulties related to the interpretation or application of the Europol Regulation,
- studies general problems associated with the exercise of independent oversight; or exercising the rights of the persons concerned,
- negotiates harmonized proposals for joint solutions if serious irregularities are identified between Member States' practices or possible illegal transfers through Europol’s information exchange channels or in relation to issues raised one or more national supervisory authorities concerning enforcement interpretation of the Europol Regulation and make such proposals
- discusses cases submitted by the European Data Protection Supervisor and which relate to data originating from one or more Member States,
- discusses cases submitted by any national supervisory authority, and
- promotes awareness of data protection rights.

During the period under review, the Office attended one meeting of the Cooperation Council at which issues concerning Europol were discussed. The following topics were covered during this meeting:

- Europol data protection functionality,
- the supervisory activities of the European Supervisor,
- the consequences of Brexit ("the withdrawal of the United Kingdom from the European Union") on activities Europol,
- the supervisory activities of the national supervisory authorities over Europol,
- the Council's future activities and the Council's work program,
- adoption of a new version of the Europol National Units handbook,

tools used by the Council for communication.

12.1.3.2 Joint Supervisory Body for the Customs Information System

The Office also oversees the CIS. The legal basis for the CIS, laid down in particular in Council Regulation (EC) no. 515/1997 was amended in 2015 by Regulation (EU) of the European Parliament and of the Council 2015/1525. Relevant changes include data retention periods (maximum period data retention 5 years plus 2 years if necessary and cancellation of the annual obligation data review) and the introduction of the possibility to limit the visibility of new cases to authorities of selected Member States.

The Office is part of the Joint Supervisory Body CIS ("JSA Customs"), which was established on the basis of Art. 18 of the Convention on the use of information technology for customs purposes as an institution authorized to supervise the processing of personal data in the CIS. The role of JSA Customs is in particular the monitoring and application of the provisions of personal data protection legislation, examining problems which may arise in the operation of the CIS, drawing up proposals for joint problem-solving as well as opinions on the adequacy of personal data protection measures data.

The Supervisory Coordination Group is also active in the area of CIS protection
over the Customs Information System (SCG CIS). It is made up of representatives of JSA Customs
and the Supervisor. In order to promote good cooperation with JSA Customs for Customs
its chairman is usually elected chairman of the CIS oversight coordination group.
Working meetings of both subgroups are usually coordinated and follow each other.
In 2019, one SCG CIS meeting was held, which was focused on discussion
future work program of the CIS SCG group, draft handbook for access to the CIS, agreement
on a common format for conducting CIS inspections, updating the CIS SCG website
and other topics.

12.1.3.3 SCG Working Group on the Coordination of SIS II Supervision

Schengen Information System II, established by Council Decision 2007/533 / JHA
allows members of the designated security forces of the Member States to access
to data on searches for persons and objects that have entered the Schengen Information System
imposed by any Member State and, in specific cases, adequately
records respond.
Schengen Information System Supervisory Coordination Working Group II (SCG
SIS II) belongs to a group of working groups set up by the Supervisor. Intention
is subject to the supervision of the protection of personal data processed by the European institutions
responsible authority, ie the supervisory officer.
The SCG SIS II was established in accordance with Article 46 of the Regulation of the European Parliament and of the Council
1987/2006 of 20 December 2006 on the establishment, operation and use of the Schengen acquis
second generation information system (SIS II) and Article 62 of Council Decision 2007/533 / JHA
of 12 June 2007 on the establishment, operation and use of the second Schengen Information System
generation (SIS II). SSG SIS II met twice during the period under review. The subject of the meeting
were mainly national criteria for issuing alerts, questionnaires, a handbook on the right to

access, modification of the SIS SCG website as well as a proposal for a Regulation establishing the

access of other EU information systems for the purposes of ETIAS.

12.1.3.4 Working Party for the Coordination of Visa Information System Supervision

SCG VIS is another working group that belongs to the group of working groups set up

supervisory officer. The Visa Information System (VIS) primarily serves visa authorities

for the purpose of examining visa applications, for the purpose of consulting other Member States

States, as well as the authorities responsible for carrying out border checks or controls carried out

in the territory of the Member States for the purpose of verifying the visa holder or the authenticity of the visas themselves.

Supervision

the national part of the information system is carried out by the national supervisory authorities,

t. j. in the conditions of the Slovak Republic, this supervision is performed by the Office, with the Supervisory Officer

checks that the managing authority carries out personal data processing activities in accordance with

with Regulation 767/2008 and whether it also carries out regular audits of personal data processing activities.

The role of this group is to coordinate the supervision of the processing of personal data

in the VIS at national level. The SCG VIS was set up in accordance with Article 43 of the Regulation

Of the European Parliament and of the Council 767/2008 of 9 July 2008 on the Visa Information System

system (VIS) and the exchange of data between Member States on short stay-visas (Regulation

or VIS). During the period under review, a representative of the Office participated in one SCG VIS meeting.

The SCG VIS meeting took place at the end of 2018 and focused on topics such as the amendment

the VIS Regulation, the preparation of personal data protection training for authorized staff

to enter the VIS and other VIS SCG activities for the years 2019-2021.

12.1.3.5 Working group for the coordination of Eurodac supervision

Eurodac was originally established by Council Regulation (EC) No 2725/2000, which was

aimed at comparing fingerprints for the effective application of the Dublin Convention,

however, in 2013, this regulation was repealed and a European regulation was adopted

Parliament and of the Council (EU) 603/2013 on the establishment of Eurodac for the comparison of fingerprints

fingers. This new regulation entered into force on 20 July 2015. According to Regulation 603/2013

The purpose of the system, which has been in operation since January 2003, is to assist EU Member States in

determining which Member State should be responsible for examining a particular application for asylum.

He is in charge of the meetings of the working group for the coordination of Eurodac supervision

a supervisory officer who also performs under Regulation 603/2013 and Regulation 2018/1725

supervises the central part of the system and coordinates the activities of the national supervisory authorities.

During the period under review, the Authority attended one SCG Eurodac meeting at which they were present

the following topics were discussed: finalization and adoption of the report on the activities of the SCG Eurodac for the years

2016-2017, preparation and draft of the next work program of the SCG Eurodac and the rights of the stakeholders

persons in Eurodac.

12.2 International level

12.2.1 Convention Consultative Committee 108

The Consultative Committee established by the Council of Europe on Convention 108 consists of representatives

Contracting 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 improving the implementation of Convention 108 and for drawing up reports, guidelines

and guidelines in areas such as contractual provisions governing protection

data in the transfer of personal data to third parties which did not guarantee an adequate level

data protection or data protection with regard to biometrics, profiling and automatic

decision-making or data protection in the field of health. The mentioned areas are only an example

the remit of the committee. They attend regular meetings of the Advisory Committee

representatives of the Office, whether in plenary or in committee meetings.

13 INTERNATIONAL MEETINGS WITH PARTNER BODIES

SUPERVISION

13.1 One Stop Meeting Program V4

In June 2018, the Office organized a two-day meeting of the supervisory authorities of the V4 countries in Šamorín. The meeting was attended by delegations from the Polish and Hungarian supervisory authorities. President she welcomed the guests with an speech in which she emphasized that we in Europe care about the protection of individuals data and therefore cooperation between supervisory authorities is necessary to ensure effective Privacy. Representatives of the Slovak office had prepared discussion papers, which concerned in particular the innovations introduced by the Regulation. An impact assessment was discussed, on fines, certifications, prior consultation, etc. The representatives exchanged their findings in this area and also how they prepared for the new legislation not only legislatively but also organizational.

13.2 INFORM workshop

A representative of the Office attended the INFORM in October 2018 and in December 2018 in Leiden workshop. It is a project funded by EU funds. The aim of the project is to provide comprehensive and a multidisciplinary understanding of Regulation and Directive 2016/680 through preparation high quality training materials, trainers prepared in this field for all members landscape and e-learning program. The analytical activities within the INFORM project are being investigated balance between the protection of personal data and other fundamental rights of interest deepening professional expertise, especially for judges and lawyers

13.3 Debating Ethics: Respect and Dignity in Data Driven Life 40th International Conference of Data Protection and Privacy Commissioners

The 40th ICDPPC meeting was held in Brussels on 22-26 October 2018. ICDPPC was organized under the auspices of the Supervisor. The meeting focused on the use of artificial intelligence and the application of ethical standards in their use (if any). The program was divided into closed sections, to which only ICDPPC members had access, and open sections, which were conducted in the form of presentations and panel discussions. Guests from different areas performed there - from supervisors, social platforms (eg Facebook), technical giants (eg Apple),

journalists, European Commissioner Věra Jourová, etc.

13.4 TRUSTECH 2018

In November, the President of the Office attended a conference called TRUSTECH 2018, which took place in Cannes. The uniqueness of the conference lies in its narrow focus on security and technologies in the field of biometrics, data protection, cyber security and also in the field data protection in the business and payment world. More than 300 people presented themselves this year companies, 250 international speakers and more than 50 start-ups. About 11 thousand visited her visitors. A significant part of the keynote lectures was also devoted to the first experiences with new legislation of the Regulation and its application in practice in the implementation of the so-called privacy-bydesign solutions therefore the specification of customized data protection in the internet environment.

13.5 Workshop between the Consumer Protection Cooperation (CPC) network and the members of the European Data Protection Board

A representative of the Office attended a meeting organized by the EC in Brussels in November selected experts from EU Member States in the field of personal data protection and protection consumers. The meeting took the form of a workshop during which each Member State could present a specific case with a focus on consumer protection (such as concerned), which he met in the course of his supervisory activities.

13.6 Data Protection Case Handling Workshop

A representative of the Office took part in a workshop in Hungary in November, which focused on case management. The workshop was attended by more than 50 participants, representing 14 EU supervisors and 7 non-EU supervisors. The workshop focused on topics such as use of cameras, processing of personal data obtained from public registers, transmission personal data, etc.

13.7 Change of chairman of the German supervisory authority in Bonn

The President of the Office together with the Director of the Office of the Office attended in January 2019

the inauguration of the new chairman of one of the supervisory authorities in Germany. This

The meeting was enriched with lectures on the Regulation and the protection of children and young people

and seniors. The benefit of the meeting was the exchange of experiences of the presidents regarding implementation

Regulations and functioning of offices in the light of new powers and tasks.

13.8 Electronic communication and privacy seminar in the new E-privacy regulation

Representatives of the Office at a seminar in February 2019 on the forthcoming regulation E-privacy

organized by the Chamber of Deputies of the Czech Republic, with the participation of selected experts

from the Czech Republic. The meeting took the form of lectures during which each expert

presented his chosen topic. In addition to the draft e-privacy regulation, the lectures were also given

principles of personal data processing, the true basis, the relationship between the Regulation and the proposal

e-privacy regulations, cookies, etc.

13.9 Europe Votes 2019: how to unmask and fight online manipulation

In February 2019, a representative of the Office attended a conference under the auspices of the EDPS on

fight against online manipulation in elections. The meeting focused on supervisory authorities in the area

personal data protection, electoral regulators, audiovisual regulators, media

and platforms that fight online election manipulation. The conference was held

in the form of panel discussions on topics such as fair and free elections

in the context of online manipulation, the co - operation of regulators in different areas that

to ensure free and fair elections, strengthen protection of personal data, etc.

13.10 IT Security Workshop 2019

In March 2019, representatives of the Office took part in a workshop in Prague, which focused on

the use of artificial intelligence (AI) as a future in IT security with a focus on detection

threats, to its use in practice, to cyber security in critical infrastructures

companies, a comprehensive system of security against cyber threats, management

security of privileged access, as well as the pitfalls of critical cyber security

infrastructure and the risks of cloud computing from a lawyer's point of view and how to avoid them

and, last but not least, to present companies that are effective tools in the fight

with cybercriminals in the IT environment.

13.11 APP Data Protection Intensive: UK 2019

In March 2019, the President of the Office in London took part in a specialized workshop

and a conference on data leakage and data protection in practice after application

Orders since May 2018. The entire conference was marked by the impending departure

Of the United Kingdom from the EU and raised the issue of relations and the future application of the Regulation

in practice with the United Kingdom as a third country. An important element that was

visible in the discussions, was the focus of UK trade attention

to the USA. Setting up privacy and data protection relationships is an obvious priority at

islands, relations with the EU seem to remain secondary.

The simulation of mass data breaches was extremely interesting. The participants were divided into

groups and deal with the task from the position of operator, intermediary, supervisory body,

concerned, the media and the public. It was interesting to see how they deal with it

especially those who represent operators and intermediaries in real life. From our

from the point of view of the regulator, it was surprising how insufficient they took into account compliance

deadlines for reporting data breaches, as they escaped the basic obligations arising from the Regulation.

From this point of view, it can be stated that there is a lack of preparedness for the consequences

from an infringement of the Regulation.

The conference participants rated the time spent together as extremely useful, also in terms of appearance

to international representation. In addition to the United Kingdom and the United States, there were teams at the conference

from Denmark, Germany, Latvia, Spain.

13.12 Integrating Ireland´s Data Protection Law into Everyday Business

In May, the Director of the Office of the Office and a representative of the Office attended a conference organized by

PRIVACY LAWS and BUSINESS in Dublin with the participation of experts from

EU Member States in terms of personal data protection as well as the professional public. The meeting was small
a form of workshop during which the individual speakers presented their topics. The topics were
for example, carrying out inspections at individual supervisory authorities and the inspection procedure
information obligations of operators. Another interesting topic was the institute of infringement
data breach. Included were practical cases of what is considered or
does not consider it a breach of personal data protection within the meaning of Art. 33 Regulations. The biggest
The attraction for the participants was a lecture by Helen Dixon, Chair of the Irish Supervisory Authority
authority. Her presentation aimed to provide information on how Ireland had dealt with
with the implementation of the Regulation. She pointed out the application problems in connection with the implementation
new legislation.

14 ASSESSMENT OF THE PERSONAL DATA PROTECTION STATUS IN THE MONITORING PERIOD

In the monitored period, interest in personal data protection and personal data as a result
application of the new legislation has grown enormously, not only the interest of journalists but also
the public and the controllers who are to apply the data protection rules
in practice.

Awareness and awareness of personal data about personal data has increased significantly; people
are interested in their personal data, protect it and ask operators much more than
and why they process their personal data. This trend is also confirmed by the operators. People are you
they are much more aware of their rights and are not afraid to demand their fulfillment in practice.

Personal data is becoming an important business item, therefore a necessity today
digital reality are strict data protection rules. They are and will be the focus of many
companies, but also the state, the more it is necessary to pay attention to their consistent protection, legal
processing and the correct setting of the legislation governing their processing. In particular
Recently, the Office has learned from its activities that it is a trend to prioritize

economic interests against the protection of the individual and his personal data, when unfortunately necessary to state that the economy still wins over the legal side and the fact that legislation only catches up with research and application practice and not the other way around. This trend needs to be reversed what the office strives for in the work of its employees to the extent that it is personal and economic possible to cover by him; it is therefore very important that the priority of the state becomes sufficient staff and material security of the Office and that the right to protection is sufficiently ensured personal data as a fundamental human right. Any underestimation of the protection situation the rights of the individual can have very negative consequences in the future. Necessary significant increase the Office 's budget, has a real foundation and support at European level as well (Communication Commission to the European Parliament and the Council, see point 3.3). It is also necessary, within public sector, to ensure equal and fair cooperation between stakeholders so that their interaction resulted in legal norms that met the criteria for protection personal data in accordance with the Regulation, which will not be prepared quickly and whose quality review the time of their effectiveness and little or no need for their frequent amendment.