ČPT 330

PERSONAL DATA PROTECTION STATUS REPORT

FOR THE PERIOD

25. MAY 2019 to DECEMBER 31, 2019

Office for Personal Data Protection of the Slovak Republic

November, 2020

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

All rights reserved.

Reproduction for educational purposes

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

REPORT ON THE STATUS OF PERSONAL DATA PROTECTION PERIOD

25. MAY 2019 to DECEMBER 31, 2019

The Office for Personal Data Protection of the Slovak Republic in accordance with the provisions of § 81 par. 2 letter k) Act no. 18/2018 Coll. on the protection of personal data and on the amendment of certain laws submits to the National Council of the Slovak Republic the Report on the Status of Personal Data Protection for period 25 May 2019 to 31 December 2019. The present report provides an overview of activities Office in a period in which both the Regulation and the law were already established in the minds of the operators and their intermediaries as well as the persons concerned.

In particular, for reasons of consistency with other European Supervisory Authorities, the Authority has decided

adopt a model of reports on the status of personal data focused on comprehensive calendar years.

Although the reporting period covered by this report is relatively short, it covers

extensive activities of the Office at the domestic as well as international level.

Based on the above provision, I am submitting a Report on the state of personal data protection

for the period from 25 May 2019 to 31 December 2019, which will be discussed in the National Council

Of the Slovak Republic in accordance with the law published on the website of the Office

(www.dataprotection.gov.sk) for the general public, provided to the media and submitted to the European

Data Protection Board and the Commission.

Anna Vitteková

Vice-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 laws

as amended by Act No. 84/2014 Coll.

Directive 95/46

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

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

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

Directive 2016/680

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

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

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

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

MPK

Interdepartmental comment procedure

Portal

Legislation Portal Slov - Lex

e-privacy directive

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

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

(Directive on privacy and electronic communications)

proposal for an e-privacy regulation

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

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

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

5

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 the free

repealing Regulation (EC) No 45/2001 and decision

no. 1247/2002 / EC

Act no. 211/2000 Coll.

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

laws (Freedom of Information Act)

EDPS

European Data Protection Supervisor

EU

European Union

EK

European Commission

EEA

European Economic Area

EDPB

The European Data Protection Board established by

Art. 68 Regulations

CONTENTS

8

1

INTRODUCTION

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

Pursuant to the provisions of § 81 par. 2 letter k) of the Act, the Office of the National Council of the Slovak Republic submits the Report on the state of protection

personal data for the period from 25 May 2019 to 31 December 2019. This is a summary of activity information

Office and its findings for the period under review. The aim of the report is to map the activities of the office

and highlight the most important changes and developments in the field of personal data protection.

The presented report is the thirteenth in the history of the independent Slovak Republic and the eleventh in history

existence of a separate office.

9

2

STATUS, PERSONNEL SECURITY AND BUDGET

OFFICE

2.1 The position of the Office

The protection of personal data in the Slovak Republic is entrusted to the

powers of the Office. The Office is a state administration body with nationwide competence performing

supervising the protection of personal data and participating in the protection of fundamental rights and freedoms

natural persons in the processing of their personal data. In exercising its powers, the Office shall proceed

independently and in the performance of its tasks, it is governed by the constitution, constitutional laws, laws, others

generally binding legal regulations and international treaties, which is Slovenská

Republic bound. The Office is a budgetary organization according to the provisions of § 21 par. 5

letter a) of Act no. 523/2004 Coll. on budgetary rules of public administration and on amendment

certain laws as amended.

2.2 Staffing of the Office

2.2.1 Public functions of the Office

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

proposal of the Government of the Slovak Republic.

The term of office of the President of the Office shall be five years. The position of the President of the Office in the monitored

period

held by Soňa 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 with effect from

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

on December 2, 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 activities

and obligations under generally binding legislation. It requires their provision

the required number of qualified staff qualified to carry out professional activities at

expert level. In the conditions of the Office, in terms of staff structure, with the exception of one

an employee who performs work in the public interest, the others are employees

in civil service. Selection of employees and filling of vacancies

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

competitions.

As of May 25, 2019, the office had 49 seats, of which

• 48 employees in the civil service relationship,

• 1 employee performing work in the public interest.

As of 31 December 2019, the Office had 50 seats, of which

• 49 employees in the civil service relationship,

• 1 employee performing work in the public interest.

Average age of employees

• as of May 25, 2019 was 40.2 years, while

 was 42.1 years for men;

 in women 39.4 years;

• as of 31.12.2019 was 40.2 years, while

 was 41.6 years for men;

 in women 39.6 years.

Overview of the number of employees of the Office

Year

to 25.5.2019

to 31.12.2019

Actual staffing of the Office

Civil service

Performance of work in public

ratio

interests

48

1

49

1

Together

49

50

The protection of personal data has been carried out since 25 May 2018 in accordance with the Regulation and the law, which directly determine to the Office all its rights, obligations and competences. Despite the undisputed the importance of the Office 's work, which depends on the importance and value of personal data, such as sources of information on natural persons, the number of staff of the Office does not change significantly.

The current number of staff of the Office is not sufficient in the context of the agenda set by the Office which has an ever-increasing trend in terms of the volume of work that falls on one employee. For the proper functioning of the office and also with regard to human possibilities and effort For high quality staffing, it is essential that the number of employees be significant increased. This will ensure a redistribution of work and the possibility of higher specialization of individuals employees, as many now perform cumulative activities, each of which they requires full concentration and attention.

The Office currently has a limit of 51 employees, and notifies the need each year increase in their number, ie increase the said limit of the maximum number of employees

at least 25. The Office's agenda is also disproportionate in the context of the obligations arising from the Regulation
has risen and is still rising. On average, there are about 110 files (cases) per employee
equipment. The current situation is unsustainable in the long run and there is a shortage of skilled people
employees is necessarily reflected in the quality of work, or sometimes it results in
impossibility of meeting procedural deadlines. To fulfill the strategic direction of the Office 's activities
it is essential that the number of staff be increased so that they complete and participate on an ongoing basis
necessary educational activities, they expanded their knowledge and were thus able in addition to professional
growth should also reflect the requirement to digitize public and state administration.
The Office also needs to be strengthened by information technology experts, as more and more
processing activities takes place in electronic form and it is necessary that, as part of the
as well as inspections, the Office was able to comment at expert level on the findings
on the information technologies used by operators and intermediaries.
The Office also feels the lack of staff dedicated to legislation, both in its area
as well as its comments, as this is often a lengthy process of examining the proposal
legislation that requires high attention and concentration and is essential to have
employee enough time and knowledge for such work, not only theoretical but also
practical. The undersized personnel side of the Office is also reflected in the fact that the Office does
time cannot think at all of setting up detached workplaces, which would be closer to
to the persons concerned, operators and intermediaries across. Undersizing the number

employees also has the effect that it is not possible to develop the necessary specialization by creating
new unions, which would take over from existing ones and subsequently develop some agendas to
expert level. The very limited possibility of educating the current ones also seems to be problematic
employees and the inability to obtain and maintain long-term pay conditions
specialists, as a result of which the Office is not in an equal position vis-à-vis
operators and their capabilities, which is ultimately always to the detriment of the person concerned

persons. The application practice of the Office implies an acute need for at least two detached persons workplaces, one in central and one in eastern Slovakia. The reason for the need of these workplaces is that the employees of the office are closer to the persons concerned also in these areas Slovakia and also the fact that this would make the performance of controls more efficient and significantly reduced the Office's staff travel costs from Bratislava and the Office would also contribute to the increase employment in these regions, where there are still a sufficient number of qualified people to work they cannot or do not want to move to the west of Slovakia or directly to Bratislava.

2.3 The Office 's budget

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

The budget for 2019 was originally approved for the Office in the amount of EUR 1,442,263.00, which was increased by valorisation in May 2019 to the amount of EUR 1,561,419.00 and in September 2019 was increased budget of the Office to the amount of 1,731,419 Eur.

The drawing of the Office's budget as at 31 December 2019 amounted to EUR 1,728,356.94, which represents 99.82% of the Office's total adjusted budget for 2019.

Overview of the Office's budget for the period 1.6.2019 to 31.12.2019 in Euros

Pointer	Approved budget to 01/01/2019	Modified budget to 1.6.2019	Modified

budget

to 31.12.2019

Pumping

budget from

6/1/2019

to 31.12.2019

Pumping

budget from

1.1.2019 to

12/31/2019

Wages, salaries,

service income

and OOV (610)

879,575.00

967,723.00

967,723.00

665 422.53

966,806.90

Wage premiums

(620)

309 654.00

344 562.00

356 522.00

245 370.37

356,505.91

Goods and services

(630)

237,034.00

233 134.00

361 204.00

225,498.24

359 101.34

Current transfers

(640)

5,000.00

5,000.00

11,870.00

8,369.61

11,869.06

EKW02 (630)

current expenses

11,000.00

11,000.00

34,100.00

30,351.42

34,071.73

0

0

0

0

0

EKW02

capital

expenses

Current expenses

together (600)

Capital

expenses (700)

1,442,263.00 1,561,419.00 1,731,419.00 1,175,012.17

0

0

0

0

1,728,354.94

0

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

and responsibilities

office,

is an

necessary

take into account

increase

agenda

a

needs

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

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

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

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

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

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 personal data protection and involved in the protection of fundamental human rights and freedoms with regard to the processing of personal data natural persons. The Office fulfills its role in supervising the processing of personal data, etc. by supervising and commenting on the texts of draft laws and other generally binding ones legislation (legislative materials) as well as non-legislative texts (vision, strategies, etc.). It formulates its comments on the proposals through the Portal within the MPK. The purpose of the Office's comments is, in particular, to ensure the quality of the legislation as far as it is concerned on the regulation of personal data processing was high, so that the subsequently adopted legal regulation was accurate, unambiguous, both in relation to the operator and in relation to the person concerned, whose personal data will in practice be subject to processing.

During the period under review, the Office submitted comments on 19 of the submitted materials. Together
He submitted 78 comments, 51 of which were substantial.
With his comments, he asked, for example, to modify the list or the scope of processing
personal data in relation to the purpose of processing, the Office has also often fundamentally requested
draft responsibilities for processing have been clarified and clarified in the draft legislation
personal data in the processing of the entities involved. Specific wording applied
The Office's comments can be found on the Portal using the filter institutions that comment
and using a comment filter (whether it is an organization comment marked as essential,
or ordinary).

3.2 Methodological guidelines

The Office methodically guides operators and intermediaries in the processing of personal data
data, raises public awareness of the risks and rights associated with the processing of personal data
data and also raises the awareness of controllers and intermediaries about their obligations.
Proven form of operator and intermediary guidance and information
based on the practice of the Office, the methodological guidelines of the Office have become public, especially of the persons
concerned
and short ad hoc methodologies published on the Office's website. The Office published within it
The methodology addresses issues and issues that are of the greatest interest at the time
public.
Of course, the Office also monitors developments in the field of personal data protection in the case of judgments, whether or
not
European Court of Human Rights or the Court of Justice of the European Union, when all relevant
publishes decisions affecting the protection and processing of personal data on its website
Legislation and case law and informs about important decisions in a short form
news directly in the news on its website. It was significant in the observed period
Judgment on the storage of cookies by Internet users.

The subject of publication and indirectly also the subject of education of interested subjects is also the publication of information and guidelines issued by the EDPS and the EDPB on the Office 's website, which attention must also be paid.

14

Significant in the period under review were, for example:

• EDPB guidelines on the right to be forgotten in search engines;

• EDPB guidance on specifically designed and standard data protection;

• EDPB guidelines on the processing of personal data pursuant to Art. 6 par. 1 letter (b) of the Regulation in the provision of online services.

The Office has focused much of its methodological work on assisting the persons concerned, with: primarily focused its activities in the period under review on the exercise of the rights of the persons concerned in the Schengen Information System, where he prepared forms for the exercise of the rights of data subjects persons also in Hungarian, French and Romani.

15

4

COMMUNICATION OF THE OFFICE WITH THE PUBLIC

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

The issue of personal data protection does not only concern operators or intermediaries, who have an obligation to apply personal data protection legislation in practice. It also affects people, persons affected, having issues arising from everyday life situations related to them personal data and their processing.

The Office's operators and intermediaries most often address questions of a professional nature related to their obligations arising from the Regulation and the law, or special laws governing processing operations.

Compared to the last Report on the state of personal data protection, there is a relatively sharp decline in issues by law firms; We attribute this decline to the time it has been

The regulation and the law apply and also the relatively vigorous but necessary approach of the Office when

after negative experiences, he made it clear that it was not possible to expect him to work out the whole

case studies for the processing of personal data provided by many law firms

they sent. The Office welcomes this changed position of law firms and is, of course, ready for them

to comment, but on specific issues, not on the case as a whole.

In the monitored period of 2019, the Office was already consulting the telephone by the allotted time

did not provide, as this activity was very burdensome and within the activities carried out

in the context of the Regulation, the number of other activities that needed to be covered has increased. Despite of

Due to the great popularity of telephone consultations with the public, these were not possible during the period under review

renewed despite considerable efforts, as these consultations relieved the Office of otherwise sent

questions to the public in writing or electronically. In the event of an increase in the number of employees

it is possible that the office would restore this very popular form of communication, at the present time

However, this is not feasible.

Regarding written and e-mailed questions to the public during the period under review

the staff of the office handled up to 800 questions.

4.2 Communication of the Office with the media

Over the period under review, media interest in privacy has decreased slightly, as has been the case

There was no longer a regulation or a law introducing new rules in the area of personal data protection

completely new and gradually used by both operators and intermediaries.

In the period under review, the Office provided a total of 50 statements for the media (print, radio and television)

together). The issues raised by the media were specific issues and "cases" in which there were

subject to the processing or protection of personal data, or questions from journalists

aimed at specifying the rights of the persons concerned, how to exercise them correctly and all that

possible as a person concerned to claim from the operator. Especially in late May and early June

media interest focused on summarizing the first year of application of the Regulation and the law in practice

and the Office’s experience this year.

4.3 Office website and its traffic

The Office's website meets the conditions and technical criteria in accordance with the Decree of the Ministry of Finance SR on standards for public administration information systems, reflects on the new legislation in the field of personal data protection, and is gradually supplemented by new functionalities and up-to-date forms, methodologies and guidelines. The Office also bases its appearance on and the division of its website

and tries to make the website more transparent as user-friendly as possible. In the rest During the period under review, the Office sought in particular to improve the English version so that the persons concerned were aware obtain information even if they do not speak Slovak and also in the context of the Office and the Slovak Republic have been the subject of a Schengen evaluation in terms of personal data protection when The evaluators were also interested in accessing and providing information in English.

The Office 's website was searched 416 903 times during the period under review, namely most often through websites and browsers google.sk, google.com, bing.com, facebook.com.

4.4 The Office's website and reporting privacy breaches through a designated form (reporting data breach)

The Office's website is a key source of information related to personal data protection. At the same time, it is also a basic service according to Act no. 69/2018 Coll. on cyber security and amending certain laws. Operators and intermediaries must ensure the continued credibility, integrity, availability and resilience of processing systems and services and to assess at regular intervals the effectiveness of the technical and organizational arrangements in place measures. Nevertheless, it may occur (whether due to intentional action, negligence, error or natural disaster) to a personal data breach which, as a result, may mean accidental or unlawful destruction, loss, alteration, unauthorized disclosure or disclosure of personal data transmitted, stored or otherwise processed. Operator

has an obligation under Art. 33 Regulations or, pursuant to Section 40 of the Act, to report a breach of protection
personal data breaches of the Office. He can do so in several ways, one
one of them is possible to use the designated form to fulfill this obligation.
During the period under review, 70 personal data breaches were reported to the Office. Reporting
is an obligation for the operators, not for the persons concerned. In cases where the violation
data protection authorities have been reported by the data subjects, who have also often reported that they have reported a
breach
because the operator stated that he would not report it because there was no incident
evaluated as such, which must be reported to the Office. We would also like to appeal this way
operators to fulfill their obligations themselves, as if the Office finds that they have occurred
to a personal data breach that has not been reported to the Office and should have been, it may be
considered by the Office to be an aggravating circumstance in any personal data protection proceedings.
The most frequent breach of personal data protection in the period under review was erroneous
service of a document on a person other than the one who was supposed to be (sometimes a single case, sometimes
several at once), loss of documentation containing personal data, cyber attack on
operator and theft of materials containing personal data. The most statistically most common
personal data breaches are reported by bank operators
and insurance, health services, energy industry, tourism follow
state institutions, cities, schools and school facilities.

5

RESPONSIBLE PERSON

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 and is obliged to do so

report to the office.

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

Resposible people

Total number of reported responsible persons

Period

5/25/2019 to 12/31/2019

Count

1881

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 persons. The result of the processing of the application by the Office, as the operator, was the sending answers that he does not process any personal data about her.

18

6

APPROVAL AND CONSULTATION ACTIVITIES OF THE OFFICE

6.1 Prior consultation

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

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

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

According to Art. 35 par. 4 of the Regulation “The Authority shall draw up and publish a list of those

processing operations that are subject to a data protection impact assessment requirement

pursuant to paragraph 1. The supervisory authority shall forward these lists to the Committee referred to in Article 68. "; list

processing operations, which are always subject to the impact assessment of the Slovak Republic in terms of

of the said article (the so-called black list), is available on the website of the Office "List

processing operations subject to a personal data protection impact assessment

Slovak Republic". This list of processing operations serves, among other things, for clarification

Art. 35 par. 1 The regulations and operators who intend to carry out such processing are

in the event that their intended processing would lead to a high risk to rights and freedoms

the persons concerned should the operator fail to take measures to mitigate that risk,

shall be required to consult the Authority in advance.

One request for prior consultation was received by the Office during the period under review.

6.2 Transfer of personal data

The free movement of personal data is guaranteed within the EEA. However, when transferred to countries outside the EEA

or international organizations, additional protection requirements need to be complied with

personal data referred to in Regulation and Directive 2016/680. Although some transfer tools

personal data under both laws are the same, it is always necessary to examine the factual

the scope of the instrument used. A novelty compared to the previous legislation is that it is being amended

transmission to international organizations.

Transfers can be divided into two groups:

• transfer to third countries (international organizations) guaranteeing an adequate level

protection,

• transfer to third countries (international organizations) that do not guarantee an adequate level

protection.

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

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

third country guaranteeing or not guaranteeing an adequate level of personal data protection. Status

country, which guarantees an adequate level of personal data protection, the EC determines

decision. It is necessary for the third country to ensure, by reason of its national law or

international agreements it has signed, the level of protection of fundamental rights, which is

equivalent to the level of protection guaranteed by EU law.

19

The EC issues a decision on adequacy separately for the material scope of the Regulation and separately for the material

the scope of Directive 2016/680. Decisions on adequacy issued by the EC during its term of office

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

by a decision taken pursuant to the Regulation. These decisions apply only to the transfer

personal data within the material scope of the Regulation, not Directive 2016/680. The Office shall publish

adequacy decisions on its website.

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

Directive 2016/680.

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

Even when transferred to a country or international organization that does not guarantee an adequate level

protection, it is necessary to distinguish between the instruments offered by the Regulation and those

offered by Directive 2016/680.

6.2.2.1 Transmission according to the Regulation

If the EC has not issued a decision on adequacy, or annulled the decision on adequacy,

the operator or intermediary may also use the following institutes for the transfer:

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

public bodies

No such instrument was adopted during the period under review.

(b) binding internal rules

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

Regulations.

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

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

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

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

Regulations.

(e) an approved code of conduct

No codes were approved during the period under review.

(f) an approved certification mechanism

No certification mechanisms were approved during the period under review.

(g) contractual clauses

No contractual clauses were approved during the period under review.

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

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

No administrative arrangements were approved during the period under review.

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

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

20

6.2.2.2 Transmission according to Directive 2016/680

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

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

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

(b) the controller has assessed all the circumstances of the transfer of personal data and concluded that

there are adequate guarantees for the protection of personal data,

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

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

21

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 its authorized to carry out control of personal data processing, control of compliance code of conduct approved by the Office pursuant to Section 85, control of compliance of personal data processing with the issued certificate according to § 86 and control of compliance with the issued grant certificate accreditation according to § 87 and § 88 of the Act. They were in the territory of the Slovak Republic in the evaluated period only checks on the processing of personal data are carried out.

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

7.1 Checks started before 25.05.2019

From the period before 25.05.2019 to the evaluated period (from 25.05.2019 to 31.12.2019) transferred 30 controls of personal data processing, of which the Office completed 20 during this period.

The auditees in ten cases were commercial companies (including one non-state health establishment), in three cases state authorities and in three cases municipalities; the remaining controls were focused on the processing activities of the public institution, health care provider (state hospital), civic association and contributory organization established by the city (House of Culture).

No breach was found in relation to the two companies and the civic association Regulations, as a result of which these inspections were terminated by an inspection record. Performance

The remaining 17 inspections revealed inconsistencies with the requirements of the Regulation, resulting in these

inspections completed by the inspection protocol.

Summary of the structure of inspected persons and the results of 20 completed inspections:

Controlled persons

state authorities

public institution

village

trading companies

state medical facility

civic association

House of Culture

Deficiencies found

(inspection report)

3

1

3

8

1

0

1

No shortcomings found

(inspection record)

0

0

0

2

0

1

0

7.1.1 Health insurance company

The subject of the inspection was a suspicion of unauthorized processing of the personal data of the data subject person (at the time of the inspection already a former employee of the inspected person), including data concerning health, for a purpose for which the inspected person was not authorized. The person inspected was an operator who processes personal data of natural persons in its information systems persons for the purposes of public health insurance. As part of the inspection in question, the inspection body

22

focused on the specific case of unauthorized verification of professional medical examination data employee to his superiors for employment purposes and following the current situation directly as well as indirectly related technical and organizational measures taken by the operator. Checking the validity of the approaches of the operator's employees assigned to the purchasing department health data to the data on the health of the persons concerned (public health policyholders) insurance), it was found that the operator had given access to healthcare data provided to a particular policyholder, even in cases where it was not necessary, by which processed personal health data against the risk of their unauthorized use processing. When covering risks with safety measures, the operator is in sufficient nor did it address a specific group of affected persons who are its employees and at the same time by its policyholders (for example, in the form of a specific policy targeted at this group persons concerned). Detected breach of the controller's obligations in the processing of personal data was reflected in the inspection report.

7.1.2 Public transport provider

The subject of the inspection was the procedure of the inspected person in the processing of passengers' personal data as well as the fulfillment of obligations in the processing of personal data by means of cameras systems in vehicles and public transport stops. During the inspection

it was found that the inspected person draws up the auditors when checking the tickets
audio recording, while checking the tickets of the persons concerned in obtaining them
does not provide personal data at all or provides insufficient information
required by Article 13 of the Regulation. At the same time, it was found that the inspected person did not accept
appropriate technical security measures for the protection of recorded audio recordings (principle
integrity and confidentiality) and does not respect the retention period set by it (principle
minimization of storage). In connection with the processing of personal data collected
cameras in the stop areas were also found to be in conflict with the principle of data minimization,
whereas the size of the monitored area significantly exceeded the area of stops, which was the case
unjustified interference with the rights and legally protected interests of the persons concerned without
regardless of whether they were passengers. In relation to video surveillance, the persons concerned were not at
information required by Article 13 of the Regulation
and in relation to the camera recordings, the specified time was found to be exceeded
storage. A breach of the controller's obligations in the processing of personal data was found
reflected in the inspection report.

7.1.3 Non-bank institution

The inspection in question focused on the compliance of personal data processing with the requirements
Regulations, specifically with the principles of personal data processing, with legal conditions
processing and the conditions of the consent and the rights of the data subject in relation to
with the provision and administration of credit. During the inspection, it was found that the individual documents
by which the controlled entity provides its clients with information concerning the legal basis
processing of personal data are incomprehensible, non-transparent and, in some parts,
contradictory. In relation to clients' consent to the processing of their personal data
the requirement to provide it freely has not been met. At the same time, personal information was found
clients are kept for longer than is necessary to achieve the intended purpose
processing. Furthermore, the inspected person did not prove the lawfulness of the processing of personal data

about the husband (wife), about the partner (companion) and about another contact person. Mistakes controlled persons were also identified during the fulfillment of the information obligation, both towards clients and towards guarantors, liaison officers and other persons concerned. Found breach of operator 's obligations during the processing of personal data was reflected in the inspection report.

23

7.1.4 Non - state medical facility

The inspection in question focused on the compliance of personal data processing with the requirements general data protection regulation, in particular with the principles of personal data processing, conditions of lawful processing, conditions of consent and conditions processing of specific categories of personal data as well as the provision of information to data subjects persons, to the intermediary, to the processing of personal data by delegation operator or intermediary and to designate the responsible person. During the inspection it was found that the processing of personal data, which was based on the consent of the data subject, it was not transparent as no clear information was provided to the data subject on the legal basis of the processing according to the purpose of the processing and information on the rights of the data subject including the right to withdraw consent to the processing of personal data. At the same time, it was found to be affected the person did not have the opportunity to decide whether or not to consent to the execution and subsequent using photo documentation. The inspected person also for the purpose of processing orders and did not proceed transparently for marketing purposes by not providing the person concerned information on the retention period of personal data and the rights of data subjects, resp. Information, which the controlled person is obliged to provide to the data subject when obtaining his / her personal data. In relation to the intermediaries of the inspected person, it was found that one of the contracts did not contain all the elements required by the Regulation. The inspected person's mistakes were also found in connection with the designation of the responsible person. Detected breach of duty the controller during the processing of personal data was reflected in the control report.

7.1.5 State authority

Inspection by a state authority initiated by a suspicion of a breach of personal processing obligations
data was focused on the compliance of personal data processing with the principles of personal data processing
data and the conditions for their lawful processing, transparency and fairness of provision
information to the persons concerned, as well as the procedure for designating the responsible person. Controlled
the person in his capacity as a public authority processed the personal data of the designated contact persons, such as
also the personal data of other data subjects, without proving that in the processing of these personal data
data has met one of the conditions of lawful processing according to Art. 6 par. 1 of the Regulation
(lawfulness of processing), as a result of which it did not comply with the principle of lawfulness,
justice and transparency. The document by which the inspected person provided his
employees (data subjects) information related to the processing of their personal data,
did not contain the correct identification data of the operator and at the same time was not stated in it
information on the right to withdraw consent to the processing of personal data, as a result
the procedures of the inspected person did not comply with the wording of Art. 13 Regulations (information provided by
concerned in obtaining their personal data), ergo principle of transparency. Detected
breach of the controller's obligations in the processing of personal data was reflected
to the inspection report.

7.1.6 Public health facility

The inspection initiated by the suspicion of a breach of personal data processing obligations was
focused in particular on the compliance of personal data processing with the principles of personal data processing,
conditions of lawful processing, conditions of consent and conditions
processing of specific categories of personal data. The review found a violation of the policy
data minimization by the fact that the inspected person also processed in the employee's personal file
personal data which were not necessary to achieve the purpose of the processing, as well as by
attendance records processed a special category of personal data (biometric data)
data in the form of fingerprints). A breach of the principle of integrity was also found during the inspection

and confidentiality in that the inspected person in relation to certain processing purposes

24

did not take appropriate technical and organizational measures and other errors were found

related to the processing of personal data for the purpose of protection of hospital property and protection of persons

and property of persons lawfully staying in the hospital for the purpose of processing information

on the doses of ionizing radiation to which the persons concerned have been exposed, as well as errors in

ordering and paying for meals for employees. Mistakes were also found in the relationship

to process personal data for the purpose of recording visits upon their one-time entry

to selected objects of the inspected person, as the inspected person did not prove to him

the legitimate interests outweigh the interests or fundamental rights and freedoms of the data subject

persons. A breach of the controller's obligations in the processing of personal data was found

reflected in the inspection report.

7.1.7 Camera systems

Out of a total of 20 inspections started before 25.05.2019 and completed in the monitored period, 8 inspections were

performed

focused on camera systems. In terms of the inspection initiative, 5 inspections were performed

in the framework of personal data protection proceedings and 3 inspections on suspicion of an infringement

obligations in the processing of personal data laid down by Regulation or law. Subject

inspections was aimed at determining the real state of personal data processing with emphasis

compliance of processing activities with the requirements of the Regulation and the law. In relationship

no mistake was found to the civic association (check completed by record

on control). The shortcoming identified by the control of the central state body was the failure to prove

compliance with the law in fulfilling the operator's obligation to provide information to the data subject

in obtaining her personal data. In the other two cases (city and municipality), the deficiencies concerned

in particular the failure to provide information to the persons concerned, the disproportionate scope monitored

storage as well as video storage for longer than necessary

to achieve the intended purpose of the processing, which also violated the related principles
processing of personal data. Failure to designate a responsible person was also found
to fulfill the tasks arising from the Regulation. In the framework of four inspections focused on
for the processing activities of three legal entities and one contributory organization set up
shortcomings were identified by the city (House of Culture), mainly related to non-compliance
conditions for the lawfulness of the processing of personal data, the provision of information to data subjects
to an insufficient or incorrect extent, a disproportionate scope of monitoring
cameras and video retention periods. Shortcomings were also found in the relationship
the obligation to take appropriate technical and organizational security measures and in relation to
to the obligation to draw up records of processing activities. Identified shortcomings logically
also conflicted with related personal data processing principles. Identified breaches of duty
operators in the processing of personal data have been reflected in the control protocols.

7.2 Inspections started in the evaluated period (25.05.2019 - 31.12.2019)

Controls of personal data processing started after 25.05.2019 were in the evaluated period
carried out in the framework of personal data protection proceedings, on the basis of a control plan, as well as
on suspicion of a breach of personal data processing obligations
By regulation or law. The focus of the inspections was on the real state of personal processing
data with an emphasis on the compliance of processing activities with the requirements of legal regulation
represented in particular by the Regulation and the law. When creating a control plan, as well as when selecting controls
initiated by the Office on an ongoing basis on suspicion of a breach of processing obligations
personal data, the Office drew mainly from its own experience gained in the performance of its tasks
in the field of supervision.

By delivering the notification of the inspection to the inspected person, the Office started in the evaluated period
32 inspections, of which 12 on the basis of a plan of inspections, 12 on the basis of a suspected breach of obligations
in the processing of personal data and 8 in the framework of personal data protection proceedings. Controlled

the person was in all cases other than a natural person in the capacity of operator (including

two cities and one municipality).

Out of a total of 32 inspections started in the evaluated period, 8 inspections were completed by 31 December 2019,

of which 2 inspections by inspection protocol and the remaining 6 inspections by inspection record. From the point of view

At the time of the inspection, 4 inspections were carried out on the basis of the inspection plan, 1 inspection on the basis of

suspected breaches of personal data processing obligations and 3 controls within the proceedings

on the protection of personal data.

Of the total of 32 inspections initiated in the period under review, it was up to the forthcoming period

24 controls transferred.

Stage and results of 32 inspections started after 24.05.2019

30

20

24

10

2

6

0

checks completed by the protocol

checks completed by the record

unfinished checks

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

Controlled persons

state authorities

towns and villages

natural persons

Deficiencies found

(inspection report)

0

0

2

No shortcomings found

(inspection record)

4

1

1

In the evaluated period, the so-called "Schengen

evaluation ”aimed at fulfilling the tasks that the Slovak Republic derives from the Schengen

acquis. The evaluation in question, with a periodicity of once every seven years, applied directly to the Office

(evaluation of the Office 's performance in this area) and indirectly (co - operation provided by the Office at

evaluation of the two ministries).

7.2.1 Control plan - 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 and European Affairs

matters of the Slovak Republic are included in the inspection plan on the basis of a recommendation

resulting from the resolution of the Government of the Slovak Republic no. 755 of 30 November 2011

26

The government approved the Schengen Action Plan of the Slovak Republic as a priority of the Slovak government

of the Republic. In connection with the change of the national access point of the Eurodac information system

for the Eurodac II version (2015) was acquired by the operator, which is the Ministry of the Interior of Slovakia republics, new competencies and responsibilities; following that fact, it arose at the same time the Office is obliged to carry out an annual inspection of the processing of personal data in the national Eurodac access point. Adoption of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), replacing and repealing Council Decisions 2009/371 / JHA, 2009/934 / JHA, 2009/935 / JHA, 2009/936 / JHA and 2009/968 / JHA, the Office has the obligation to regularly control of the processing activities of the Europol National Unit or the National Liaison Officer Europol.

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 guilty of a criminal offense or misdemeanor, ie personal data capable of being significantly affected interfere with the rights and legally protected interests of the persons concerned.

In the evaluated period, 8 inspections of personal data processing of the data subjects were performed, which were focused on 4 workplaces of the operator of the Ministry of the Interior of the Slovak Republic, 3 workplaces of the Ministry of Foreign Affairs and European Affairs of the Slovak Republic and one office of the Criminal Office of Financial Administration.

7.2.1.1 Ministry of Foreign Affairs and European Affairs of the Slovak Republic

The subject of the inspection of the National Part of the Visa Information System were processing activities Consular Section of the International Law, Consular and Crisis Management Section Ministry of Foreign Affairs and European Affairs of the Slovak Republic related to the issuance of Schengen visas, respect for the principles of personal data processing, with emphasis on the rights of data subjects and the security of personal data, as well as the processing activities of the two consular posts selected embassies of the Slovak Republic related to the issuance of Schengen visas and respect for the principles of personal data processing, with emphasis on the rights of data subjects

and security of personal data. None of the three were completed during the period under review
control.

7.2.1.2 Ministry of the Interior of the Slovak Republic

The subject of the control of the national part of the Schengen Information System were processing
activities of the National SIRENE Bureau within the fulfillment of the tasks of the Police Force of the Slovak Republic for the
purposes of
Regulation (EC) No 1049/2001 of the European Parliament and of the Council 1987/2006 of 20 December 2006
operation and use of the second generation Schengen Information System, on the basis of
whose data on third-country nationals are processed in connection with a refusal of entry
or residence, as well as Council Decision 2007/533 / JHA of 12 June 2007 establishing,
operation and use of the second generation Schengen Information System, according to which they are
processed data on persons and objects in N.SIS II for the purpose of discreet surveillance; or
targeted controls. The inspection was completed by the inspection record.

Subject to control by the automated European fingerprint identification system
(EURODAC), the processing activities of the EURODAC National Access Point were carried out
pursuant to Regulation of the European Parliament and of the Council no. 603/2013 of 26 June 2013 on the establishment of
the system
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 an application for international protection lodged by a third-country national
country or stateless person in one of the Member States, and at the request of the authorities
Member States for law enforcement and Europol for comparison with Eurodac data
for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing
European Agency for the Operational Management of Large Area Information Systems
Freedom, Security and Justice (recast) as well as under the European

Parliament and of the Council 604/2013 of 26 June 2013 laying down the criteria and mechanisms for
designation of the Member State responsible for examining the application for international protection lodged
a third-country national or a stateless person in one of the Member States
States (recast). The inspection was completed by the inspection record.
The subject of the inspection of the liaison office of the Slovak Republic (Europol) in The Hague were processing plants
activities under 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), establishing
replace and repeal Council Decisions 2009/371 / JHA, 2009/934 / JHA, 2009/935 / JHA,
2009/936 / JHA and 2009/968 / JHA, as well as the consistency of the processing of personal data of data subjects
with the principles of personal data processing and the conditions of lawful processing with emphasis on
the rights of data subjects and the security of personal data. The check was completed by recording
on control.
The processing of the National Passenger Information Center (NUIP) was the subject of an inspection
the activities of the National Passenger Information Center set up as part of the transposition of the Directive
Regulation (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of records data
on Passengers (PNR) for the prevention, detection, investigation and prosecution of terrorist
crime and serious crime. The inspection was completed by the inspection record.
7.2.1.3 Criminal Financial Administration Office
The inspection in question focused on the processing activities of the Criminal Finance Office
reports under Council Regulation (EC) No 515/97 of 13 May 1997 on mutual assistance between
administrations of the Member States and on cooperation between the administrations of the Member States
and the Commission in ensuring the proper application of customs and agricultural rules
matters as amended and Council Decision 2009/917 / JHA of 30 November
On the use of information technology for customs purposes as well as on the consistency of the processing of personal data
data subjects with the principles of personal data processing and legal conditions
with an emphasis on the rights of data subjects and the security of personal data. Listed

the inspection was not completed within the evaluated period.

7.2.2 Inspection on suspicion of a breach of personal processing obligations

data

The inspection focused on the consistency of the processing of personal data of the persons concerned by attendance

system of the controlled person (city) with the principles of personal data processing, conditions

lawful processing and the restrictions applicable to the processing of specific categories

personal data, as well as the exercise of the rights of data subjects, the security of personal data

and the existence and content of related operator instructions addressed to the intermediary.

The inspection revealed that the attendance system works on the principle of assigned codes

and continuous photography (i.e. not based on biometric data); regarding

no processing deficiencies were found with the processing activity in question

personal data of the persons concerned. The inspection was completed by the inspection record.

28

7.2.3 Checks in the framework of personal data protection proceedings

In the evaluated period, all 3 inspections were within the framework of personal data protection proceedings

focused on camera systems operated by individuals. In one case, they were not

No non-compliance with the requirements of the Regulation was found, as a result of which this inspection was terminated

inspection record. The performance of another 2 inspections revealed shortcomings, which consisted mainly

in not providing any, inaccurate or incomplete information to the persons concerned

and failure to prove compliance with the conditions of lawfulness of the processing of personal data. Doubts

At the same time, the persons inspected were identified in relation to the retention of videos for a period of

longer than is necessary to achieve the intended purpose of the processing, as well as in the relationship

to the disproportionate size of the monitored area, thus violating the related principles

processing of personal data (in particular the principle of data minimization and the principle of minimization

storage). Identified violations of the obligations of controllers in the processing of personal data

were reflected in the inspection reports.

7.3. CONCLUSIONS ON 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
long-term identified categories of operators that need to be given increased
attention for objective reasons (large scale of personal data processing, sensitivity
personal data processed, and the like) as well as subjective ones (especially intentional or
negligent prioritization of one's own interests over the rules of personal processing
data).

The supervisory activity of the office, whose basic mission is undoubtedly also preventive action
for the protection of personal data processed by controllers and their intermediaries, is already
long-term desirable to support other forms of activities of the Office, which are directly proportional to its financial,
material and personnel situation, which currently does not allow for implementation and permanent application
sophisticated (especially in the field of information technology) or otherwise demanding
the Office's procedures aimed at protecting the personal data of the persons concerned, ie all of us.

However, the basic precondition for achieving compliance with the requirements of the Regulation and the law is also
general identification with the intention formalized by this legislation.

8

PERSONAL DATA PROTECTION PROCEDURE

The purpose of personal data protection proceedings is to determine whether the rights of natural persons have been violated
during
processing of their personal data or the provisions of the Regulation or the law have been violated.

In the event of deficiencies being identified, if justified and expedient, impose remedial action, if any
fine. The provisions of the Administrative Procedure Code apply to personal data protection proceedings.

If the competence of the Office to act and the decision in the case is not given, the Office is obliged to file it
forward to the competent administrative authority.

In the period under review, the Office forwarded a total of 14 submissions to another, competent administrative authority for action and decision.

Personal data protection legislation requires the Office to make the submission exhaustive postponed in certain cases. The most common reason for the postponement was the unfounded submission, when it was already clear from the evidence submitted by the person concerned that the law had been infringed regulations in the field of personal data protection.

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

In the monitored period, a total of 138 submissions were postponed, of which

• 94 were postponed because the proposal was manifestly unfounded,

• 6 because the case to which the application related was heard by a court or a criminal body proceedings,

• 33 because the petitioner did not provide the Office with the necessary cooperation at his request,

• 5 due to the fact that more than three have elapsed since the event to which the proposal relates on the day of its delivery years.

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

Otherwise, it will stop the personal data protection proceedings.

The privacy proceedings are under way

• at the request of the applicant,

• 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 finding of a suspected infringement

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

30

In the monitored period, the Office initiated a total of 71 administrative proceedings, of which

• 43 were launched at the request of the data subject,

• 13 started on the initiative,

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

• 7 proceedings were conducted by the Office on its own initiative on the basis of a suspected breach of the law

regulations in the field of personal data protection.

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

Year

Based on

proposal

From 25.5.2019 to

12/31/2019

43

Based on

initiative

13

Based on

inspection results

From my own

initiatives of the Office

8

7

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

it is based on a reliably ascertained state of affairs. For this purpose, the Office is in proceedings for the protection of personal

data

authorized to request the co-operation of anyone, and the Office requested it during the period under review

for cooperation a total of 381 times. In personal data protection proceedings, there have been two cases where

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

comply

did not cooperate (in these cases proceedings were initiated against the entities

on a fine or a disciplinary fine).

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

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

used in a significant number of cases, with the exception of cases where all

the parties were represented by lawyers.

The most common subject of personal data protection proceedings was 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 breach of the principle of non-discrimination

legality when personal data was processed without a legal basis, resp.

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

related to the failure to take appropriate security measures.

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 materials in particular documentary evidence. The persons concerned submitted mostly precise proposals containing all of them required, with only a minimal need to call for removal
deficiencies in administration.

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.

31

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 where it is necessary to exclude the application of Act no. 71/1967 Coll. These specifics are important in terms of correct application of personal data protection, the Office in the first instance proceedings take them into account where appropriate and necessary. Such a special institute in the proceedings on personal data protection is e.g. secrecy of the identity of the petitioner in cases where his rights and legally protected interests (as a person concerned) may have been violated, or negative action by the operator. The secrecy of the petitioner's identity has found its way justification and the persons concerned used it in the period under review in the interest of their protection in proposals seeking the protection of their rights and the interests protected by law with 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.

32

9

COOPERATION AND CONSISTENCY MECHANISM

The functioning of the internal market requires that the free movement of personal data within the Union is not impeded

restricted or prohibited, not even for reasons related to the protection of individuals during processing

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

responds by establishing cooperation and consistency mechanisms to ensure consistency

and a similarly high level of personal data protection in each Member State, regardless of

place of residence of the person concerned.

9.1 Cooperation mechanism

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

cooperation will arise in the framework of the investigation of a specific breach of personal data protection

data or other activities of the supervisory authority (eg addressing legal issues,

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

Regulation, no further specific agreements are required between Member States

for this purpose.

9.1.1 Cross-border processing

Pursuant to Art. 55 of the Regulation, each supervisory authority performs the tasks and exercises the powers published

By regulation in the territory of its State. However, the regulation also specifically regulates the procedure and jurisdiction

in proceedings for the cross-border processing of personal data. Cross-border processing makes sense

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 a single activity
the establishment of an operator or intermediary in the Union but which significantly affects it
or likely to significantly affect the persons concerned in more than one Member State.
The regulation governs cooperation between supervisory authorities, in particular in relation to
with the mechanism of a single contact point (so-called one-stop-shop) regulated in Art. 56 par. 1
Regulations under which the supervisory authority is the main establishment or the sole establishment
operator or intermediary authorized to act as lead supervisory authority for
cross-border processing carried out by that operator or intermediary.
According to Art. 56 par. 2 of the Regulation, each supervisory authority is competent to deal with it
complaint or possible infringement of the Regulation, if the facts concern only
establishment in its Member State or significantly affects the persons concerned only in its own Member State
Member State. In accordance with Art. 4 point 22 of the Regulation other supervisory authorities will be for this
processing in the positions of the supervisory authorities concerned, if (a) the controller; or
the intermediary is established in the territory of the Member State of that supervisory authority; (b) the persons concerned
resident in the Member State of that supervisory authority are significantly affected or will be significantly affected
likely to be significantly affected by processing; or (c) the complaint has been lodged with that supervisory authority
authority.
The designation of the lead supervisor and the authorities concerned is done in IMI
(Internal Market Informational System), within which
the exchange of information on specific processing takes place between the different supervisory authorities
and a specific suspicion of a breach of personal data protection, resp. if the investigation
started on the basis of a complaint from the person concerned as well as the content of that particular complaint. Exchange
information is in English.
33
During the period under review, 450 identification notifications were received by the Office in IMI
the head and the supervisory authority concerned. The Office shall, on the basis of a careful assessment of each one

assessed that it was the supervisory authority concerned in 94 cases; most often for reasons that
the processing of personal data in question significantly affects or is likely to significantly affect
will affect the affected persons residing in the territory of the Slovak Republic. It went most often
on social network operators, operators providing accommodation services, air
companies, various e-shops and online gaming rooms. In some cases, the Office was also affected because
that the operator or intermediary is established in the territory of the Slovak Republic, ie. on the
the territory of the Slovak Republic has one or more establishments. If the Office has assessed that it is
the supervisory authority concerned, identified this in IMI and followed up the case. In accordance
with Art. 60 of the Regulation, the Office had the opportunity to comment on the requests of the head, if necessary
the supervisory authority, its procedure and the results of the investigation, as well as to comment on the proposal
decisions. If the Office were the supervisory authority concerned because it was delivered to it
complaint, the Office would act as a contact point for the person concerned and would inform him or her
decision of the head of the supervisory authority.

A total of 21 submissions containing elements were received by the Office during the period under review
cross-border processing (of which 9 proposals from data subjects, 8 complaints and 4 notifications
on breaches of personal data protection, the so-called data breach). These submissions were received either from
foreign persons or directed at foreign operators, such as
also to operators established in the USA, the Netherlands or Ireland. Office within each
first examined (so-called preliminary examination of the complaint) whether the subject of the submission
meets the conditions for cross-border processing according to Art. 4 point 23 of the Regulation, resp. whether it has been met
definition according to Art. 56 par. 2 Regulations. If the subject of the application gave rise to a reasonable suspicion
from a breach of personal data protection, the Office also verified the allegations in cooperation
with the supervisory authority of the Member State in whose territory the operator had its principal or
single establishment. In two cases, the Office entered the received submissions into IMI and beyond
addressed in cooperation with the supervisory authorities, who were the chief supervisor for the given processing
authorities. These were the supervisory authorities of Ireland and the Czech Republic. The Office was designated in the period

under review

the Slovenian supervisory authority as the lead supervisory authority, based on the place of its head office

operator, as the complaint from a Slovenian citizen was directed against the operator

established in the Slovak Republic.

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

other supervisory authorities.

During the reporting period, the Office received 18 requests for cooperation from other supervisory authorities in IMI

within the meaning of Art. 61 Regulations. Three requests were received identically from the Polish and Italian supervisory

authorities,

Luxembourg and Ireland submitted two requests for cooperation, Cyprus, the Czech Republic, Estonia, Hungary,

Latvia, Lithuania, Malta and Norway submitted one application to the Authority during the period under review.

In the requests in question, the supervisory authorities sought the Office's legal opinion in particular

interpretation of the provisions of the Regulation. The requests concerned e.g. automated decision-making

including profiling in connection with the evaluation of the absence of employees in the workplace,

use of biometric signature, retention period of personal data on the basis of the authorized

interest, credit registers, legal opinion on the interpretation of Art. 77 Regulations, tasks and responsibilities

responsible person, the coherence of the Regulation and national protection rules

personal data, a representative of a controller not established in the European Union, position

responsible person for consultations during the preparation of the draft legislative measure, interpretation

Art. 55 par. 3 Regulations. In this way, some supervisory authorities informed the Office of the receipt

notification of a personal data breach or use this method for consultation

case before launching the one-stop-shop mechanism.

During the period under review, the Office sent 4 requests for cooperation in IMI pursuant to Art. 61
Regulations. The requests concerned information on specific cross-border cases, consultations
individual cases or the legal opinion of other supervisory authorities on interpretation
Regulations. For example, the Office asked other supervisory authorities whether they considered net processing
record from the criminal record for processing according to Art. 10 Regulations when there are records
from the criminal record necessary for the purpose of recruitment. The Office also requested other supervisory authorities
authorities on cooperation in relation to the issue of compensation between the operator
and a responsible person who has not fulfilled his tasks under the Regulation. Office on mutual
in cooperation with other supervisory authorities, it also used other forms of communication such as IMI
written and telephone communication) in which he used contacts acquired during his
activities, including contacts gained through membership of the Committee's expert groups.

9.1.3 Joint supervisory operations

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

9.2 Consistency mechanism

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

9.2.1 EDPB opinion

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

Regulation)

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

9.2.2 EDPB Dispute Resolution

Dispute resolution The EDPB allows for binding decisions to ensure consistency

application of the Regulation in the following cases:

• The relevant reasoned objection was raised by the supervisory authority concerned or

rejected by the lead supervisory authority (Article 60 of the Regulation);

• Disagreement with the appointment of the head of the supervisory body (Article 56 of the Regulation);

• Absence of consultation of the EDPB (Article 64 of the Regulation);

• The Authority did not follow the opinion of the EDPB (Article 64 of the Regulation).

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

35

9.2.3 Emergency procedure

Article 66 of the Regulation provides for an urgency procedure. In exceptional

in cases where the supervisory authority concerned considers it urgent to protect rights and freedoms

concerned, it may take interim measures having legal effect in its territory. Validity

these measures may not exceed three months. In this case, the supervisory authority concerned is concerned

obliged to inform the other supervisory authorities, the EDPB and the EC.

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

EDPB for an urgent opinion or an urgent binding decision. Each supervisory authority may

request an urgent opinion or a binding decision from the EDPB in cases where the competent authority

the supervisory authority has not taken appropriate action and there is an urgent need for action. In the evaluated

period, the Office did not apply this article.

36

10 SANCTATION

Sanctions for violations of the Regulation and the law are fines and disciplinary fines. Sanctions are in place

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

10.1 Fine

In the monitored period, the Office for violations of legal regulations in the field of personal data protection
imposed nine fines in the aggregate amount of EUR 75,300. In the monitored period, he selected the office
on fines in total EUR 94,238. The average fine was EUR 8,367. The lowest fine
in the amount of EUR 500, the Office ordered the operator for failure to cooperate. The highest fine
the Office legally imposed an amount of EUR 50,000 on the operator for breach of security
processing of personal data.

Overview of fines imposed and collected in the monitored period

Watched
period

Count
fines

5/25/2019
until
12/31/2019

Total height

Average height

Total selected on

legally

fines rounded to the nearest euro

fines imposed in Euros

whole Euro up

75 300

8 367

94 238

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

period1 for breaches of personal data protection legislation can be stated,

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

does not provide adequate conditions for its performance. The Office may also impose a disciplinary fine

to a person who is not an operator or intermediary for failing to provide the requested

cooperation 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 4,000, of which one in the amount of EUR 500 for non-cooperation and the other

in the amount of EUR 3,500 in connection with the obstruction of the inspection.

The Ministry of Finance of the Slovak Republic set the Office a binding indicator for the collection of fines for 2019 in the amount of EUR 81,778, while for the whole of 2019 the Office collected a total of EUR 119,114 in fines, ie it met the set indicator beyond.

1

37

10.3 Selected cases from the supervisory activity of the Office

10.3.1 Postponements

10.3.1.1 Ambiguity of the data subject's request

The Office assessed the petitioner's proposal that the operator had infringed his right of access to personal data according to Art. 15 of the Regulation by notifying him at his request did not provide the information on the processing of the personal data he requested. The Office examined the application the petitioner and the notification from the operator to whom he handled it, on the basis of which he stated that the request was so vague that if the information provided did not fully meet the intention the petitioner with whom he turned to the operator, it cannot be fairly concluded that the operator has thereby infringed certain rights of the data subject provided for in Art. 15 Regulations. Office for the above reasons, the proposal was postponed according to § 100 par. 5 letter a) instructed the law and the petitioner, as he has rights under Art. 15 Apply the regulations properly.

10.3.1.2 Processing a telephone number in order to contact the data subject

The Office received submissions from natural persons requesting, for example, telephone checks numbers from which they have been contacted in order to offer or request various goods and services check the progress of an unidentified company that contacted them by telephone without having to knowledge of where such a company obtained their telephone number.

The Office does not have a database of telephone numbers in which the telephone user can be identified numbers. The Office may initiate proceedings against the operator or intermediary on the basis of duly filed application by the person concerned who i. it must also indicate the person against whom the proposal is directed; name and surname, registered office or permanent residence and identification number, if

has been allocated. In such submissions, the Office invited the person concerned to file a petition
to initiate proceedings on personal data protection in a lawful manner with the prescribed law
essentials. The person concerned if he suspects his phone number of any company
obtained without her knowledge and uses it further, she has the right to access her personal data when
it may also request any available information upon request to the operator
about the source of obtaining his personal data and may also exercise other rights of the data subject
processing of personal data.

10.3.1.3 Disclosure of arrest data in the United States

During the period under review, the Office received a submission from the applicant stating that
a US-based operator repeatedly publishes its personal data on its website
data on his arrest in the US in 2011 along with his photograph. The applicant further stated that
in the past, he asked the operator to delete the said data, while he was also responsible for this
to pay, but information about his arrest should have been made public again.

In order to ensure that individuals are not denied the protection to which they are entitled under
Regulation claim, the Regulation should apply to the processing of personal data concerned
persons located in the Union by an operator or intermediary who:
is not established in the Union if the processing activities involve the supply of goods or services thereby
concerned, whether or not it is linked to a payment. In order to determine whether such
the operator or intermediary offers the goods or services to the persons concerned
located in the Union, it should be ascertained whether it is clear that the operator or intermediary
plans to offer services to the persons concerned in one or more Member States of the Union.
While the mere availability of the website of the operator, intermediary or

information society service provider in the Union, email address or other contact details
data or the use of a language generally used in the third country where the controller is located
established are not sufficient to confirm such an intention, based on factors such as use

language or currency commonly used in one or more Member States

with the possibility of ordering goods and services in a given second language or mentioning customers

or users located in the Union, it may be apparent that the operator intends

to offer goods or services to the persons concerned in the Union.

The content and nature of the operator's website showed that the data on the arrested

persons were generated from publicly available databases within the United States, by neither intention nor intent

the operator of the site in question did not offer goods or services (whether free of charge or for

money) to the persons concerned within the European Union. Office after reviewing the filing and Internet

The site operator stated that the very availability of the website in the European Union

neither the use of the language commonly used in the United States (English) was sufficient to determine

the intention to offer services to the persons concerned in the European Union, and thus the activity itself

the operator of the website, which was the collection and subsequent publication of data from the public

available US databases was not sufficient to determine the territorial scope of the Regulation.

The Office subsequently informed the applicant that in accordance with Art. 3 of the Regulation on the subject of his

submission does not apply. The Office also informed the applicant that this did not affect his right

contact the appropriate U.S. privacy authorities.

10.3.1.4 Sending harassing leaflets to the homeowners' association

During the period under review, the Office dealt with the filing of the President of the Association of Homeowners against

companies established in another Member State. The subject of her complaint was her complaint against

unsolicited letter mail from the company that sent the quotations via leaflets

for cleaning services in the mailboxes of homeowners' associations and administrators. According to the submission,

that the company contacted by e-mail not to send unsolicited to the homeowners' association

mail, while the company should have received a response to ignore their offers.

The evidence annexed to the submission showed that the company had confirmed that the tenders had been sent

to the addresses of the associations of apartment owners and housing cooperatives and subsequently the chairwoman

assured the community of owners that it would indicate in the system that the omission of its address would be next

delivery of offers and if he is not interested in their offer, he can ignore it.

The controller 's conduct showed signs of cross - border processing of personal data according to

Art. 4 pt. 23 of the Regulation, since in the present case it was an operator established in another

Member State of the European Union. The Office first examined the application (so - called preliminary examination

complaint) whether the subject of the application meets the conditions for cross-border processing according to Art. 4 pt. 23

Regulations, resp. whether the definition according to Art. 56 par. 2 of the Regulation under which it is

any supervisory authority competent to deal with a complaint or breach lodged with it

Regulations if the facts concern only an establishment in its Member State or substantially

affects the persons concerned only in its Member State. The Office shall bear the cost of the preliminary assessment

subsequently determined whether there is a reason for cross-border cooperation in the present case.

In this case, the president of the community of owners represented the community of owners

housing - a legal person, while the processing of personal data concerning legal persons,

in particular companies set up as legal persons, including name, form and contact details

legal person does not fall within the material scope of the Regulation.

39

In its preliminary assessment of the case, the Office found that there was no material scope in the present case

authority or the powers of the supervisory authority of another Member State, since the Regulation

Art. 1 par. 2 of the Regulation applies to the protection of the rights of natural persons, not to the protection of legal rights

persons - in this case the community of apartment owners, therefore the Office evaluated the complaint as obvious

unfounded, which does not constitute a ground for initiating proceedings and a complaint in accordance

with § 100 par. 5 letter a) of the Act postponed.

10.3.2 Procedures

10.3.2.1 Determining the prognosis of incapacity for work

The Office conducted personal data protection proceedings on the basis of a proposal according to which the controller

unjustifiably processed the applicant 's personal health data in that regard as his

the employer asked the attending physician for a prognosis when he expects to end the petitioner's

incapacity for work. The operator objected that it did not intend to obtain data
about the petitioner's health, but only information about his return to work due to the organization
work process. The Office stated that objectively the operator requested a professional forecast
development of the patient's state of health, which is a health claim that falls into a special category
personal data according to Art. 9 par. 1 Considered the regulations and the operator's procedure as processing
the applicant 's health data which does not meet any of the conditions for lawful processing under
Art. 6 par. 1 of the Regulation and does not fall under any exception to the prohibition on processing special categories
personal data according to Art. 9 par. 2 of the Regulation, whereby the operator violated the principle of legality
according to Art. 5 par. 1 letter (a) Regulations and prohibitions on the processing of specific categories of personal data
according to Art. 9 par. 1 of the Regulation. The Office given the circumstances of the specific case of the operator
according to Art. 58 par. 2 letter (b) of the Regulation reprimanded that the said operation of obtaining personal
infringed the provisions of Art. 5 par. 1 letter a) and Art. 9 par. 1 of the Regulation.

10.3.2.2 Publication of portraits of proposers

The Office conducted proceedings on the protection of personal data on the basis of a proposal, the subject of which was
unlawful disclosure of portraits of claimants by an operator on
for business purposes, it published on its website photographs of the interior in which
pictorial images of the petitioners were exhibited. The operator objected when taking pictures
The interior was also attended by one of the designers who did not take any action to make them
the images were not part of the photograph taken; office with reference to Art. 5 par. 2 and Art. 24 par. 1
The regulations stated that it is the operator's responsibility to ensure that processing
personal data in accordance with the Regulation and may not transfer its responsibility to
draftsmen. The operator also objected to the nature of the published portraits as personal
data due to their reduced quality, for which, according to the claimants, the
published photo identifiable. After examining the published portraits, the Office stated that
that these are photographs of faces that show distinct anatomical elements specific to physical identity
the individual person on the basis of which the petitioners are identifiable and their images as they were

published by the operator meet the defining characteristics of personal data according to Art. 4 par. 1
Regulations. The Office assessed the given publication of the portraits of the petitioners as a personal processing
data which does not meet any of the conditions of lawful processing under Art. 6 par. 1 of the Regulation,
whereby the operator violated the principle of legality under Art. 5 par. 1 letter a) Regulations, for which
imposed a fine on the operator due to the circumstances of the particular case.

40

10.3.2.3 Violation of personal data protection by sending a phishing e-mail

The Office received a complaint by which the controller reported a personal data breach
cyber attack via phishing e-mail, as a result of which the account of one employee
sent e-mails to many internal and external recipients. Circle of those affected
persons should also be employees of the operator.

The operator learned about the incident not from an external source, but from a warning
its established security team. The attacker should also have given names, surnames,
business phone numbers and email addresses. In the present case, the Office initiated proceedings against
to the operator and investigated the matter in writing. During the proceedings, the Office
demonstrated that the operator had received safety instructions prior to the occurrence of the security incident
measures which it considered appropriate, but which nevertheless infringed
personal data in its environment. The operator demonstrated that after detecting the incident promptly
took the necessary measures, evaluated the incident as a breach of personal data, began his
investigation and notified the Authority as the supervisory authority. The office had found that the employee was on time
incident was also trained in the processing of personal data and was not a mistake
caused by his conduct. He is also responsible for compliance with the principle of confidentiality of personal data
operator. In the present proceedings, the Office found a breach of the principle of confidentiality of personal data
data of the operator 's employees as a result of the cyber attack via
phishing email unauthorized to a third party. The Office did not impose on the operator
corrective action, as the deficiencies were remedied and the imposition of measures was in place

ineffective and unreasonable in each case. The Office imposed a fine on the operator.

10.3.2.4 Unauthorized disclosure of personal data in the photo gallery of the advertised offer

The Office accepted the initiative to initiate proceedings on personal data protection regarding the publication of part of the proposal

for deposit in the cadastre with specific names of the persons concerned and their other personal data such as

date of birth, birth number and address within the real estate agency offered real estate on

sale. Part of the proposal for a deposit with personal data of natural persons was in the published

photo galleries for real estate.

Due to suspicion of unauthorized disclosure of personal data, in particular birth numbers, which

as a universally applicable identifier of a natural person, it is prohibited to publish unless

that it is published by the person concerned himself, the Office has started against the real estate agency as the operator,

administrative proceedings. In the present case, the Office collected the documents for issuing the decision

in the form of written cooperation. During the proceedings, it was found that he was responsible for disclosure

personal data was a real estate agent who was a real estate agent. Office therefore

also conducted proceedings against the intermediary. Personal data can be processed by the operator himself

or processing on his behalf may be carried out by an intermediary. Processing

the intermediary is governed by a contract or other legal act which it binds

intermediary vis-à-vis the operator and setting out the subject matter and duration of the processing,

the nature and purpose of the processing, the type of personal data and the categories of persons concerned and the obligations and rights

operator. The real estate agency of the office has proved that the broker, as an intermediary, processes

personal data on the basis of a concluded mediation contract and in this case processed

personal data of the persons concerned to the extent and under the conditions agreed in the given contract.

Among other things, the mediator undertook in the contract to take such measures to prevent this from happening

unauthorized or accidental access to, exchange, destruction, loss of personal data,

unauthorized transmission, their other unauthorized processing as well as other misuse

personal data.

41

The Office had proved that the intermediary also published personal data when uploading the advertisement

affected persons, including birth numbers in the part of the application for deposit in the photo gallery sold

properties, with their publication being made in error for approximately twenty minutes.

The disclosure of personal data violated security, this personal data was accessible

internet users. By decision, the Office found an infringement on the part of the mediator

principles of confidentiality of personal data by unauthorized disclosure on the Internet and breach of the prohibition

disclosure of the birth number of the persons concerned. Due to the implementation of the immediate remedy

errors on the intermediary's own initiative, the Office did not impose a corrective measure

to ensure that the identified deficiencies are remedied. The Office in the proceedings ordered for the given error

to the intermediary.

10.3.2.5 Publication of the purchase contract

During the period under review, the Office conducted proceedings on the protection of personal data on the basis of the

proposal

suspicions of unauthorized processing of personal data, which should have occurred through disclosure

a donation agreement containing the personal data of the data subject.

The operator referred to Act no. 211/2000 Coll. As the operator published personal

data above the extent allowed by the special law in question, the Office found a violation

principles of legality within the meaning of Art. 5 par. 1 letter (a) Regulations.

42

REMEDIES AND DECISION-MAKING

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

fines, as well as against the decision not to disclose information or non-disclosure decision

the information may be partially remedied - dismissed in the alternative

the provisions on remedies laid down in the Administrative Procedure Code. About filed corrective actions

the President of the Office shall decide on the basis of the recommendations of the Appeals Committee, whereby the petitioner may extend or supplement this by another proposal or by other points within the time limit intended for the application of decomposition.

In the period under review, the President of the Office received 36 appeals.

During the period under review, it ruled in 17 cases as an appellate body.

Of the total number of appeals lodged, 27 were lodged against the decision imposing a fine, or they imposed both a measure and a fine; of which in the period under review was a decision 13 of them and as regards the amount of the fine in 4 decisions, the amount of the fine was confirmed, in 7 the decision of the first instance body was annulled and the case was returned to a new proceeding and in 2 cases the first-instance decision has changed as regards the amount of the fine.

Of the total number of appeals lodged, 5 were against the decision to stay the proceedings, of which in the monitored period, a decision was made in 3 cases, while twice the decision was made at first instance confirmed and canceled once.

Out of the total number of submitted appeals, 1 appeal was filed against the decision not to file measures and fines, which was also dealt with during the period under review; President of the Office confirmed at first instance.

Out of the total number of submitted appeals, 1 appeal was filed against the decision on imposition measures, 1 appeal was lodged late and was subsequently considered as a subject for review decisions imposing measures to remedy the identified deficiencies and their causes outside appeal proceedings and 1 appeal was directed against the decision imposing measures and non-imposition fines. In all three appeals, the President of the Office decided only in 2020.

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 will either make the required information available or issue it decision not to make information available resp. decision not to disclose the information in part.

During the period under review, the President of the Office did not receive any such dissolution.

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.

12 EUROPEAN AND INTERNATIONAL PROTECTION OF PERSONAL DATA LEGISLATIVE PACKAGE

12.1 Legislative process at EU 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) in order to ensure consistency with a common approach to personal data protection across the EU. Proposal for a regulation e-privacy will be a lex specialis in relation to the Regulation. For this reason, the Office is a co-manager in the legislative process for the adoption of the draft e-privacy regulation at European level.

The aim of the draft e-privacy regulation is to ensure strict privacy rules for users of electronic communications services and a level playing field 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 Finnish Presidency of the Council of the EU presented at the end of its term in December 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

the e-privacy regulation and the regulation so that this interconnection is technologically neutral and at the same time clear from a legal point of view; boundaries between the reasons for processing electronic communications data and privacy rights, including the confidentiality of communications; inclusion of specific provisions on the protection of children from abuse are included in the draft e-privacy or adoption regulation another legal act. The draft e-privacy regulation remains the subject of ongoing negotiations on EU agreement with a view to reaching an agreement on its text as soon as possible.

12.2 European Data Protection Board

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

The EDPB is represented by its chairman, 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 EDPS. The EC has the right to participate in the activities and meetings of the Committee without voting rights.

The EDPB operates in accordance with the Rules of Procedure, which have been amended three times during the period under review.

The activities of the EDPB are divided into 12 expert subgroups, which are divided thematically. E.g. expert group for technology, fines, cooperation, and others. These expert subgroups are working on documents which help to ensure the consistent application of the Regulation. The office participates in the work of 11 expert subgroups by personal participation, by sending written comments, by participating in video and teleconferencing, possibly related workshops.

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

During the evaluated period, 6 meetings were held and the Office participated in all of them.

The greatest benefit to the public is the issuance of EDPB guidelines on various issues.

During the period under review, the Committee issued 5 guidelines, 2 following a public consultation and 3 following a public consultation

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

it also publishes these guidelines in Slovak and English on its website.

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

12.3 Committee set up under Article 93 of the Regulation

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

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

did not sit down.

12.4 Cross - border data exchange

The EU has set up a number of European large-scale information systems and agencies, which it oversees

is shared between the national data protection authorities and the EDPS. In order to ensure high

and a consistent level of protection, national data protection authorities and supervisors shall cooperate

official in the coordination of supervision.

The Data Protection EDPS is the EU's independent supervisory body responsible for security

respect for the fundamental rights and freedoms of natural persons, and in particular their right to data protection from

by the institutions and bodies of the Union. The EDPS is responsible for monitoring and security

application of the provisions of Regulation 2018/1725 and any other acts of the Union relating to

protection of the fundamental rights and freedoms of individuals with regard to the processing of personal data

institution or body of the Union and for advising the institutions and bodies of the Union and the persons

all matters relating to the processing of personal data.

The national supervisory authorities and the supervisor shall cooperate to ensure a coordinated approach

supervision. To this end, representatives of national data protection authorities and the Supervisor

they meet regularly - usually twice a year - to discuss common issues

relating to supervision. Activities include, but are not limited to, joint inspections and investigations and work

on a common methodology.

These are specifically the following groups:

• Europol Cooperation Council,

• Joint Supervisory Body for the Customs Information System,

• SCG Working Group on the Coordination of Schengen Information Surveillance

system II,

• Working Group for the Coordination of Supervision of the Visa Information System,

• Working group for the coordination of Eurodac supervision.

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

for the coordination of the Schengen Information System II (SCG SIS II), the Visa Information System

system (SCG VIS), Eurodac (SCG Eurodac) and the Coordinated Supervisory Committee (CSC).

45

12.4.1 Coordinated Supervision Committee (CSC)

The CSC had its first meeting in December 2019. In Article 62 of Regulation 2018/1725 and others

legislative acts of Union law provide for the coordinated supervision of national supervisors

authorities and the European Data Protection Supervisor takes place within the EDPB. On this

a coordinated supervisory committee is set up for this purpose.

The CSC strives to achieve the objectives of its participating bodies, each of which acts to an extent

their respective competencies and within the scope of their responsibilities, in order to exchange relevant

information, assist each other in carrying out audits and controls, investigate any problems

associated with the interpretation or application of Regulation 2018/1725 and other applicable acts

Union to address problems with the exercise of independent oversight or the exercise of the rights of the persons concerned

people, in order to find harmonized solutions to all problems and increases

awareness of personal data protection rights.

The scope of the CSC currently covers the Internal Market Information System (IMI), Eurojust

and the forthcoming European Public Prosecutor's Office, expected in December 2020.

12.5 Schengen evaluation

In October 2019, the Schengen evaluation of the Slovak Republic in the field of protection took place
personal data. A team of European experts led by the President - a representative of the EC assessed the situation
protection of personal data of the Schengen acquis in the Slovak Republic. During the evaluation experts
personally visited the Office, the Office of International Police Cooperation, the National SIRENE Bureau,
but also the M. R Štefánik International Airport in Bratislava. He was an expert during the presentations
presented approach to personal data protection within the scope of individual auditors
authorities, while experts had the opportunity to ask additional questions on the topics presented.
During the personal visits to the institution, the experts had the opportunity to see their functioning in practice
and to evaluate in more detail the conditions for the protection of personal data within the framework of the Schengen acquis at
Slovakia. The processing of the results of the Schengen Evaluation of the Slovak Republic 2019 is still in the process of proper
adopted and approved conclusions, the Slovak Republic will be informed through a report
with the results of the evaluation.

12.6 Convention Consultative Committee 108

The Consultative Committee established by the Council of Europe on Convention 108 shall consist of representatives of the
Contracting Parties
Parties to the Convention supplemented by observers from other States (members or non-members)
and international organizations. The committee is responsible for interpreting the provisions and for improvement
implementation of Convention 108 and for drawing up reports, guidelines and guidelines in such
areas such as contractual provisions governing data protection in the transfer of personal data
to third parties who did not guarantee an adequate level of data protection or data protection
with regard to biometrics, profiling and automatic decision-making or data protection in the field
health. These areas are only an exemplary part of the work of the committee. Meeting
The Advisory Committee shall be regularly attended by representatives of the Office, whether in plenary
meetings or narrower meetings of the Committee.
On 17 December 2019, the Slovak Republic acceded to Protocol no. 223 to the Council of Europe Convention no. 108

on the protection of individuals with regard to automatic processing of personal data (Convention 108).

Slovakia thus became the 38th country to sign this Additional Protocol. The protocol aims

modernize the original document in accordance with the latest knowledge in the field of technical development,

artificial intelligence and the IT sector in general.

46

13 MEETINGS WITH PARTNER SUPERVISORY AUTHORITIES AND OTHER ENTITIES

13.1 Erasmus for public administration

In July, a representative of the Office participated in the two-week Erasmus for Public program

administration, which took place in Brussels and Luxembourg. The program was aimed at acquaintance

with the roles and work of all EU institutions as well as advisory bodies. The lecture was beneficial

focused on the EU decision - making process, which is important for a better understanding of the Office 's role

contributes not only to the drafting of EU legislation but also to its application. The program included

also a visit to the Court of Justice of the EU together with a lecture by Advocate General Sharpston,

which guided the participants from the application to the Court of Justice of the EU until the adoption

final decision. She also explained the importance of the Advocate General 's opinions and the role they played

have in court. The representative also took part in a simulated decision - making in the European

Parliament as Members of the European Parliament through a visit

The parliamentarians in which the information presented on the decision-making process was applied. He plays

was aimed at adopting two directives - the EU - wide common pipeline directive and the

on chipping. After the game, participants received certificates. The most important part of the program was “job

shadowing ”, which the representative attended at the EDPS, where she became acquainted with the tasks of the EDPS and

was involved

to their work.

13.2 EDPB BCR workshop

A representative of the Office took part in an approval workshop in Oslo in June

binding internal rules in which the EEA supervisory authorities participated. Subject

The workshop was a great opportunity to gain contacts with supervisory staff

other Member States who deal with the issue of binding internal rules on a regular basis

they work and have extensive years of experience in approving them. The workshop also served to

that Member States exchange lessons learned and the Member States they have

less experience with the process of approving binding internal rules; or

so far none, they provided at least basic information and tips "how to do it" and what to do with it

process attention.

13.3 Data protection and competitiveness in the digital age

Under the auspices of the EDPS and the BfDI (Federal Office for Data Protection and

Informationsfreiheit) a lecture on personal data protection and digital competition took place

attended by a representative of the Office in July 2019. The lecture was focused on German

decision on Facebook and abuse of market power. In the panel

The discussion was addressed with contributions from the President of the CNIL, ICO, Chairman of the Federal NEM SA,

EDPS

and the Secretary-General of the EC. The discussion focused on the relationship between competition law and the right to

protection

personal data. In the discussion, the speakers emphasized that this relationship is deepening, especially because

since the adoption of the Regulation, people have become more interested in the protection of personal data and therefore are

able to see links with other areas as well.

13.4 EU Software and Cloud Suppliers Customer Council

In August 2019, a representative of the Office attended the first meeting of this new platform, which is

organized under the auspices of the EDPS and the Dutch Ministry of Justice. The aim of the meeting is

to develop joint European cooperation in the conclusion of contracts and licenses between public authorities

(including EU institutions) and large technical giants. Representatives from the Netherlands presented in

in general, contractual changes in the part of personal data protection that they have managed to negotiate at concluding a contract for the use of Microsoft services for the Dutch state authorities. Based on these information and knowledge, it is possible to proceed with the conclusion of similar agreements in other states EU.

13.5 MyData2019 Conference

In September, a representative of the Office attended a conference in Helsinki called MyData2019. The main topics of the conference were data management and portability, privacy-enhancing technologies and trust, online identification, collective intelligence - from citizenship science to open innovation a blockchain. The conference was held in several panels and brought many interesting ones insights into state-of-the-art personal data processing solutions as well has opened many topics related to the legal side of the use of modern technology at processing of personal data.

13.6 European Privacy Law Scholars Conference (PLSC Europe)

The President of the Office, together with a representative of the Office, attended the PLSC Europe conference in October in Amsterdam. During two intense days, Tilburg University took turns several important speakers from both the public and private sectors. 43 workshops, at which discussed 130 registered participants were focused on legislative amendments to the Regulation and e-privacy directives, social media regulation in the light of data protection, freedom of expression and media laws to European democracy and free elections in the age of artificial intelligence.

13.7 Cybersec CEE - Securing the world's digital data

Representatives of the office attended the Cybersec conference in October 2019 in Katowice. Through this conference, the participants got acquainted with the development of the latest technological trends and their impact on personal data protection. Lecturers from all over presented the latest findings, and the conference program was divided into several panels by topic. The representatives also gained some important contacts with colleagues who they work in a similar sector and who are interested in personal data protection and cyber

security. The conference also included the Expo - an exhibition of specific projects by the authors
presented their functions and thus approximated their functioning in practice. This invaluable knowledge
have a wide range of uses in the functioning of the Office, as these technical solutions are gradually being developed
get into practice.

13.8 Workshop on ISO / IEC 27701 and GDPR certification

A representative of the Office attended a Workshop on ISO / IEC 27701 and GDPR in Brussels in November 2019
certification, which was organized under the auspices of Microsoft. The main topics focused on
basic explanation of ISO / IEC 27701: 2019 (PIMS) and its relation to global regulation
privacy. In the second block, there was a discussion on the application of the rules for certification and accreditation
criteria under the Regulation and the impact on businesses. The discussion was conducted by Chatham House rules
(a set of rules for debates and discussion panels on controversial issues so that the discussion
could be open, without the risk that the discussants will be penalized for what they said in the discussion.
Due to the short time and breadth of the topic, the conclusions were not summarized. The participants of the workshop were
both from the private sector (majority) and from national regulators.

13.9 Cyberspace 2019

A representative of the Office attended an international conference in November 2019 entitled
Cyberspace, which took place in Brno. The conference focused on topics such as cookies and online
surveillance, freedom of expression and journalism, the Open Data Directive and more. It's a possibility
direct exchanges of views between perceptions of personal data protection in academia,
representatives of the private sector as well as the Office and other public authorities. There were several presentations
focused on research in the field of personal data, such as ownership of personal data or
problematic aspects of the Open Data Directive. Thanks to the fact that this conference
acting on academia is its benefit of the free exchange of views and arguments of the participants.

13.10 European case handling workshop

A representative of the Office participated in the European case handling workshop, which was organized after

31 times in Brussels under the auspices of the EDPS and the EDPB in November 2019. The workshop was attended by 50 participants. The workshop consisted of 6 presentations and group discussions. The lecturers prepared questions or cases for the presentation that were discussed after the presentation. The participants were divided into 6 groups in which they exchanged their views and solved cases. Then yours the participants presented the conclusions to the other groups.

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

However, the period for which this Privacy Report is presented is relatively short, it was very rich in the activities of the Office in all directions, so in the number of proceedings, controls and also in the work of specific staff of the Office who participated in the preparation of methodologies The EDPB and the active participation and representation of the Authority were directly involved in their text. These methodologies - guidelines are very important for the correct application of the Regulation and its sometimes they translate relatively brief text into concrete recommendations and examples as needed look at specific articles and their practical application in practice. With regard to the guidelines issued and in preparation by the EDPB, the Office slightly weakened its own methodological activity as it did not it is expedient for a certain area of processing to be methodically adjusted by the Committee and the Office at the same time, which could lead to their incompatibility.

Again, in the period under review, the Office's legislative activities admit that many the submitted legislative materials within the MPK do not have the necessary quality in terms of on the provision of the processing of personal data are vague and the wording needs to be clarified in particular as regards personal data processing operations. Despite that in the monitored period, the Office submitted comments on 19 materials, as well as the number of submitted fundamental comments

shows that when drafting legal standards in the context of personal data protection and their
the role of the Office is irreplaceable and the submitters of legislative materials still have
shortcomings in this area. However, it should be noted that year after year, the situation is gradually improving
and the Office is sometimes approached by the submitters of legislative materials to be with it
some issues and nuances of the future draft legislative material were discussed. Within
In the legislative activity of the Office, it is necessary to conclude that this is the quality of the submitted material
very important, but many times the explanatory memorandum to the material is very important, as
clarifies the intention of the submitter, which is not always obvious from the material itself.
The protection of personal data is one of the fundamental human rights and freedoms and is guaranteed by the Constitution
Of the Slovak Republic, this is not an area that should be on the fringes of the interest of both
as well as the state that is to guarantee it. There is personal data for both the private and public sectors
gradually valuable and sometimes the only source of detection and research on the basis of which
They "set the processes" of the economic and social direction of the state, but also of concrete ones
operators. Personal data is thus not only what identifies people as persons, but they are
source of forecasts for the future, it is therefore necessary that their processing and understanding is not
degraded only to the level of the source "for setting economic goals for the future", but they were
still understood as unique identifiers associated with a particular person, which is not possible without
the rules laid down for the activities for which they are needed. Their processing
and in some ways exploitation must have its own rules, it must respect their individuality
and must not slip into the "source" plane, because they are not primarily. This role in all directions
is becoming more and more noticeable to the Office, as it is also due to the increasing use of smart
technologies, personal data are only becoming part of them and their uniqueness is gradually disappearing, this one
the wrong trend needs to be stopped, as with the right cooperation of all involved
It is possible for technologies to advance and personal data be protected within them
and processed in accordance with the Regulation and the law. However, this symbiosis arises gradually, and only after
cooperation of all parties involved.