

CPT 939

ABOUT THE STATUS OF PERSONAL DATA PROTECTION

A MESSAGE

FOR THE YEAR 2021

Personal Data Protection Office of the Slovak Republic

March, 2022

Personal Data Protection Office of the Slovak Republic

Hraničná 12

820 07 Bratislava 27

Slovak republic

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

Electronic version of the report accessible at

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

ID: 36064220

VAT number: 2021685985

All rights reserved.

Reproduction for educational purposes

and non-commercial purposes only permitted with attribution

REPORT ON THE STATUS OF PERSONAL DATA PROTECTION FOR THE YEAR 2021

Office for the Protection of Personal Data of the Slovak Republic pursuant to § 81 par. 2 letters k)

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

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

of personal data protection for the year 2021. The submitted report is an overview of the office's activities

in the monitored period.

According to Art. 59 of the Regulations "Each supervisory authority prepares an annual report on its activities,

which may include a list of the types of violations reported and the types of compliance actions taken

with Article 58 par. 2. Said reports shall be submitted to the national parliament, government and others by the authority determined by the law of the member state. The reports shall be made available to the public, the Commission and the Committee."

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

"The office submits a report on the status of personal data protection to the National Council of the Slovak Republic at least once a year; the report on the status of personal data protection is published by the office on its website based and provides it to the European Data Protection Board and the Commission.", based on which I submit this report to the National Council of the Slovak Republic on behalf of the office. After discussing it in the National Council of the Slovak Republic will be published on the website of the Office for Broad public and available to the media and also submitted to the European Data Protection Board and the Commission.

JUDr. Anna Vitteková

vice president of the office

LIST OF USED ABBREVIATIONS

office

Personal Data Protection Office of the Slovak Republic

SR SR

National Council of the Slovak Republic

a message

2021 State of Personal Data Protection Report

the law

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

as amended by Act no. 221/2019 Coll.

Regulation

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

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

repeals 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 physical persons in the processing of personal data by the competent authorities for the purpose of preventing criminal offences acts, their investigation, detection or prosecution or for the purpose of enforcing criminal sanctions and on the free movement of such data and on the repeal of Council Framework Decision 2008/977/JHA

MPK

Interdepartmental comment procedure

Portal

Portal of legal regulations Words – Lex

e-privacy directive

Directive of the European

concerning

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

(directive on privacy and electronic communications)

draft e-privacy regulation

Draft REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on respect of private life and protection of personal data in electronic communications and on cancellation directive 2002/58/EC (directive on privacy and electronic communications)

Convention 108

Council of Europe Convention No. 108 on the protection of individuals during automated processing personal data

of July 12, 2002,

2002/58/EC

parliament

and Councils

5

Regulation 2018/1725

Regulation of the European Parliament and the Council (EC) no. 2018/1725 on the protection of natural persons at processing of personal data by institutions, bodies, offices and agencies of the Union and on free movement such data which

decision

no. 1247/2002/EC

Act No. 211/2000 Coll.

Act No. 211/2000 Coll. on free access to information and on changes and additions to some of laws (the Freedom of Information Act)
the regulation is repealed

(EC) No. 45/2001 a

EDPS

European Data Protection Supervisor/ European Data Protection Supervisor

EU

European Union

EK

European Commission

EEA

European Economic Area

EDPB

The European Data Protection Board established by

Art. 68 Regulations

6

CONTENTS

3

2

2.3

1.1

4.1

4.2

2.1

2.2

LIST OF USED ABBREVIATIONS5

CONTENTS7

1. INTRODUCTION9

Purpose of the report 9

STATUS, PERSONNEL SECURITY AND BUDGET OF THE OFFICE11

Position of the office 11

Personnel security of the office 11

2.2.1 Public functions of the office 11

Personnel area of office employees 11

2.2.2

Budget of the office 13

LEGISLATIVE ADJUSTMENT OF THE PROTECTION OF PERSONAL DATA16

3.1 Interdepartmental comment procedures 16

3.2 Methodological guidelines and information 17

4 COMMUNICATION OF THE AUTHORITY WITH THE PUBLIC20

Statements of the office on issues of natural persons and legal entities 20

Provision of information based on requests for disclosure of information according to law

no. 211/2000 Coll. 20

Communication of the office with the media	21
4.3	
4.4 The website of the office and its traffic	21
4.5 Website of the office and reporting of violations of personal data protection	21
4.6	
Project - 311071Z328 Electronicization of the services of the Personal Data Protection Office of the Slovak Republic	23
RESPONSIBLE PERSON	24
APPROVAL AND CONSULTING ACTIVITY OF THE AUTHORITY	25
Previous consultation.....	25
Transfer of personal data	25
Transfer to a country guaranteeing an adequate level of personal data protection	25
Transfer to a country that does not guarantee an adequate level of personal data protection	26
7 CONTROLS	28
Inspections registered in 2021	28
Checks completed in 2021	28
Selection from inspections completed in 2021	32
6.2.1	
6.2.2	
7.1	
7.2	
7.3	
6.1	
6.2	
5	
6	
7.3.1 Controls of personal data processing in information systems, with the help of which	

7.4

ensures the practical implementation of the Schengen "acquis" 32

Processing of personal data by the pharmacy 32

7.3.2

Processing of personal data by the technical control station 32

7.3.3

Processing of personal data by a medical facility 33

7.3.4

Processing of personal data by the city's camera system 34

7.3.5

7.3.6

Processing of personal data for the purpose of issuing resident parking cards 34

7.3.7 Monitoring tables in a fast food establishment 34

7.3.8 Monitoring of publicly accessible spaces by a state institution 35

Conclusions 35

8 PERSONAL DATA PROTECTION PROCEDURE36

9 COOPERATION AND CONSISTENCY MECHANISM38

9.1 Cooperation mechanism 38

9.1.1 Cross-border processing 38

9.1.2 Mutual assistance 39

9.1.3

Joint operations of supervisory authorities 40

9.2 Consistency Mechanism 40

9.2.1

Opinion of the EDPB 40

9.2.2 EDPB dispute resolution 41

9.2.3

Procedure for urgent cases 41

10 SANCTIONING42

A fine 42

10.1

10.2

Disciplinary fine 43

10.3 Selected cases from the office's supervisory activities 43

10.3.1 Postponements 43

10.3.2 Proceedings 44

11 REMEDIES AND DECISION ON THEM48

12 COMPLAINTS ACCORDING TO THE COMPLAINTS ACT49

13 EUROPEAN AND INTERNATIONAL LEGISLATIVE PROTECTION PACKAGE

PERSONAL DATA50

13.1

Legislative process at EU level 50

13.2

European Data Protection Board 51

13.3 Extensive information systems and bodies, offices and agencies of the Union 51

13.4

Schengen evaluation 52

13.5 Consultative Committee on Convention 108 52

14 MEETINGS WITH PARTNER SUPERVISORY BODIES, CONFERENCES

AND WORKSHOPS54

14.1 Challenges of international data transfer from the perspective of the Convention 108+ and

GDPR	54
14.2	
PL&B 34th Annual International Conference	54
14.3 Qubit Conference Prague 2021	54
14.4	
Privacy Conference 2021	54
14.5 GDPR Conference 2021	54
14.6 Global Privacy Assembly Conference 2021	55
14.7	
Privacy in video games: the darkest of patterns	55
14.8 GDPR and the Personal Data Protection Act 2021	55
15 ASSESSMENT OF THE STATUS OF PROTECTION OF PERSONAL DATA IN THE MONITORED PERIOD	57

8

1. INTRODUCTION

1.1 Purpose of the report

The aim of this report is to provide statistical indicators of the office's activities, but above all to provide comprehensive picture of the state of personal data protection within the Slovak Republic and also point to the office's activities on an international and European scale. The description is no less important of the actual state of the office with regard to its personnel, material and financial security, what was in the monitored period and what is necessary and appropriate to change based on the indicated indicators. By regulation, the European Union defined the supervisory authorities of individual member countries unified scope of their scope, which was justified by the need for effective protection of the rights of individuals when processing their personal data, as a result of which it expects from individual supervisory authorities, that they will systematically fulfill this goal, with the necessary support of the state. The mentioned unfortunately, neither the personnel potential nor the financial coverage of the activities correspond to the facts

office. In situations where the effort to consistently fulfill the tasks of the office runs into the absence of conditions that would allow him to do so, it is impossible to achieve the level of supervision over the protection of personal data, to which the Slovak Republic is obliged. Significant for the significantly unfavorable situation of the office is the fact that the office does not yet have its own within the state budget also has an impact on the budget chapter, as a result of which there is a blatant contradiction with every request for removal between the scope and difficulty of the assigned tasks, confronted with the amount of imposed fines, which they are just a side effect of his mission.

The lack of employees affects the staff of the office in the form of an enormous workload, which was not removed even by the cumulation of the functions of organizational units or the cumulation of the functions of some employees. The mentioned facts in connection with already standard problems in security, inadequate financial evaluation and sometimes even when securing the wages themselves are manifested as disillusionment, burnout, or departure of office employees to the commercial sphere or acceptance of a lucrative offer from other state administration bodies. Here it is important to point out that fluctuation of employees is devastating for the office, as familiarization with the issue of protection of personal data, regardless of the education of the new employee, is a process that does not take several weeks or months. Therefore, the current state and functionality of the office cannot (without using euphemisms) be described in other ways than the words "before the collapse".

In November 2019, the Schengen evaluation of the Slovak Republic took place, which included an assessment of the Slovak Republic in the area of personal data protection was also part of it. According to the conclusions of the evaluation, the European Union recommends that we increase personnel and budget security of the office.

I am again pointing out the conclusions of the latest evaluation, according to which the European Union, among other things, recommended increasing the staffing and budgeting of the office. Slovak Republic should the Personal Data Protection Office of the Slovak Republic:

-

-

-

ensure that in order to increase the efficiency and effectiveness of the protection authority
personal data further increased its budget and number of employees,
to ensure that the part of the total state budget that is intended only for the authority for
personal data protection, clearly visible to guarantee that the authority for personal data protection
data has a separate public budget,
ensure that the National Council becomes familiar with the budget process

the opinion of the authority for the protection of personal data regarding its budgetary needs,

9

as well as the budget negotiations conducted by the Personal Data Protection Authority
with the Ministry of Finance,

- take measures to ensure that the Ministry of Finance cannot give to

mutual connection budget and amount of fines that the authority for personal data protection has
to choose because it could affect the nature and prioritization of the protection authority
personal data and thus affect his independence. It should be guaranteed that the budget of the body
for the protection of personal data will not be possible to reduce during the calendar year if the authority for
personal data protection will not collect the estimated amount of fines in full.

Since the fulfillment of the above recommendations is the basic premise of the entire process

Schengen assessment, I consider it necessary to meet these requirements repeatedly even today

draw attention. I believe that delaying the solution can have consequences for the Slovak Republic and

the functioning of the office itself, unfortunate consequences in the form of proceedings conducted against Slovenská

to the Republic by the European Commission, which would significantly negatively affect the perception

functioning of the rule of law in our country. At the same time, we are in a situation where if there are no quick and effective
measures

step by step, we are waiting for the breakdown of the structures of the office so that the provision of protection to the persons

concerned, as well as

the fulfillment of other tasks will remain uncovered for a long time.

In direct contrast to the aforementioned Ministry of Finance of the Slovak Republic

requested that the office deal with the request to reduce staff levels across the state

administration, namely 10% in accordance with Government Resolution no. 649 of October 14, 2020. In the conditions

the office was represented by five employees. At this time, the office was significantly understaffed

undersized, while the current state of the number of employees, after the necessary reduction of staff

of employees is alarmingly insufficient for the proper performance of the tasks of the office and its national ones

competencies. The situation at the office is currently critical, as the employees of the office must

hold more than one position cumulatively, due to the insufficient number of employees.

Today, the office is confronted with the departure of experts who are leaving not only for better conditions

to the private sector, but also to other places in the state administration, where they can offer them significantly better

conditions.

Beyond the scope of the above, the current situation is aggravated by the unresolved insufficient financial

the budget of the office, which we are trying to deal with in the long term. In addition to the fact that our numbers have

decreased

employees, in contrast to the evaluation conclusions mentioned above, are also employees

office insufficiently motivated for their expertise and managing a wide range of agenda on

national or international level already by default beyond the scope of their working hours. Nowadays

in a young team, going on maternity leave is often one of the reasons why female employees leave

and then on parental leave.

Considering the above and the fact that there was a reduction in the number of employees of the office, it means

non-fulfilment, or a serious collision with the conclusions of the expert team of the Schengen evaluation

of the Slovak Republic 2019 in the field of personal data protection, which we have not fulfilled so far

not in any of the above points.

In conclusion, I would like to state that in the event of non-fulfillment of the obligation arising from the law of the European

Union, there is a risk

to the member state proceedings for breach of obligations initiated by the European Commission pursuant to Article 258 and so on Treaties on the functioning of the European Union. In the case of proving that the state will not fulfill its obligations the obligation imposed by EU law, the member state is threatened with possible monetary sanctions imposition of a flat-rate fine until the time when the situation in the member state corresponds to the situation required by EU law.

10

2 BUILDING, STAFFING AND BUDGET

AUTHORITY

2.1 Position of the office

The protection of personal data in the Slovak Republic is, on the basis of the law and Regulation, entrusted to powers of the office. The Office is a state administration body with nationwide scope of execution supervision of personal data protection and participating in the protection of fundamental rights and freedoms natural persons when processing their personal data. The office is progressing in the performance of its mandate independently and in fulfilling its tasks, it is governed by the constitution, constitutional laws, laws, others generally binding legal regulations and international treaties, which is Slovak republic bound. The office is a budgetary organization according to the provisions of § 21 paragraph 1 and paragraph 5 letter a) of Act no. 523/2004 Coll. on budgetary rules of public administration and on amendments some laws as amended.

2.2 Staffing of the office

2.2.1 Public functions of the office

The office is headed by a chairman, who is elected and recalled by the National People's Congress of the Slovak Republic at the proposal of the Government of the Slovak Republic.

The term of office of the head of the office is five years. Soňa held the position of chairperson of the office Pötheová, who was elected to the post by the NR SR on May 14, 2015 based on the voting results of members of the NR SR (Resolution of the National Council of the Slovak Republic No. 1736/2015). Based on

of the government's proposal to remove her from her position, which was delivered to the NR SR on April 27, 2020 (item 74) was on 29/04/2020 based on the result of the vote of the members of the NR SR on the proposal for her recall dismissed from her position (Resolution of the National Council of the Slovak Republic No. CRD-852/2020 of April 29, 2020).

Management of the office

subsequently, in accordance with the law, the vice-president of the office took over.

The office's vice-president is held by Anna Vitteková, who was with effect from

On January 2, 2016, to the position appointed by the Government of the Slovak Republic by resolution no. 658/2015 from on December 2, 2015. In connection with the dismissal of the head of the office for the entire year 2021, the office led vice president of the office.

2.2.2 Personnel area of office employees

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

activities and obligations according to generally binding legal regulations. Securing them

requires the necessary number of qualified employees capable of performing professional activities

at the expert level, while it is also necessary to take into account the necessary degree of substitutability.

In terms of the office, from the point of view of the structure of the employees, in 2021 there were all employees

by employees in the state employee relationship. Selection of employees and filling of vacancies

of civil servant positions is implemented according to the conditions set by law for

individual functions exclusively on the basis of selection procedures, which the office publishes on the central office public service portals.

As of December 31, 2021, the office had 45 positions filled, of which

☐ 45 employees in the state employee ratio.

Average age of employees

☐ as of 01/01/2021, he was 41.67 years old, while

11

☐ for men it was 42.54 years;

- 41.30 years for women;
- as of 31/12/2021, he was 41.29 years old, while
- for men it was 41.79 years;
- 41.04 years for women.

Overview of the number of employees of the office

Year

Civil servant

Performance of work in public

The actual state of the office's employees

as of 01.01.2021

as of 31.12.2021

ratio

45

45

interest

0

0

Together

45

45

From May 25, 2018, the protection of personal data is carried out in accordance with the Regulation and the law, which they directly establish all of the authority's rights, obligations and competences. Despite the indisputable the importance of the office's activity, which depends on the importance of the meaning and value of personal data, such as source of information on natural persons, the office's employee limit for 2021 was reduced to 461 compared to the office's employee limit from 2020, which was 51 employees.

The established limit of employees in 2021 was not sufficient in the context of the agenda, which the office

provides and which has an ever-increasing tendency in terms of the amount of work per person employee. For the proper operation of the office and also with regard to human possibilities and efforts for high-quality work of employees, it is necessary that the number of employees is significant increased by at least 30 employees. This will ensure the redistribution of work and the possibility of a higher salary the specialization of individual employees, as many now carry out cumulative activities, each of which requires full concentration and attention.

The office's agenda, even in the context of the obligations arising from the Regulation, has grown disproportionately and has constantly

growing trend. The current situation is unsustainable in the long term and there is a lack of qualified personnel of employees is inevitably reflected in the quality of work, or even results in impossibility compliance with procedural deadlines. In order to fulfill the strategic direction of the office's activities, it is necessary, to increase the number of employees, so that they graduate and continuously participate in the necessary educational activities, they expanded their knowledge and were thus able to grow professionally also reflect the demand for digitization of public and state administration.

It is necessary to strengthen the office with experts in information technology, as more and more processing activities takes place electronically and it is necessary that within the proceedings, as well as controls, the office was able to comment on the findings at an expert level

it goes

about information technologies used by operators and intermediaries.

The Office also feels a lack of employees dedicated to legislation, in its field creation, as well as its comments, as it is a lengthy process of examining the submitted proposal legal regulation or non-legislative proposal that requires high attention and concentration and it is essential that the employee has enough time and knowledge for such work, and not only that theoretical, but also practical. The undersized personnel side of the office is also reflected in this

1 The reduction of the limit of the number of employees of the office occurred on the basis of the discussion and approval of the material "Budget draft

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

of the Government of the Slovak Republic no. 649/2020 of 14/10/2020. Mandatory consideration of the reduction in the number of employees in the conditions of the office meant a loss of 5 employees.

12

regarding the fact that the office of that time cannot even think about establishing detached workplaces, which would be also closer to the affected persons, operators and intermediaries.

The undersizing of the number of employees also has the effect that it is not possible to develop the necessary specialization by creating new branches that would take over from the existing ones and then develop them some agendas to expert level. We consider it particularly necessary that it be an employee the necessary training provided to the office, which will have a positive impact on the performance of their activities, so when it comes to speed, but especially expertise.

The impossibility of obtaining adequate salary conditions in the long term appears to be problematic to maintain erudite specialists, as a result of which the office is not in an equal position to operators and their options, which is ultimately always to the disadvantage of the affected party persons. From the application practice of the office, there is an acute need for the creation of at least two secondees workplaces, one in central and one in eastern Slovakia. The reason for the need for creation of these workplaces is so that the employees of the office are closer to the affected persons from these areas as well of Slovakia and also the fact that in this way the performance of controls would be made more efficient and they would be significantly reduced office costs for employees' travel from Bratislava; the office would also contribute to the increase employment in these regions, where there are still enough qualified people looking for work they can't or don't want to move.

2.3 Office budget

The office is a budgetary organization, which is linked to the state by its income and expenses

budget through the General Treasury Department, which is managed by the Ministry
of the Slovak Republic's finances.

For the year 2021, a budget of EUR 1,727,539.00 was initially approved for the office. During
of the year, the budget of the office was increased to the amount of EUR 1,738,043.75.

The utilization of the office's budget as of 31.12.2021 was in the amount of EUR 1,737,952.97, which represents 99.99%
from the total adjusted budget of the office for 2021.

13

Overview of the budget of the office for the period 01.01.2021 – 31.12.2021 in Euros

Pointer

Approved

budget

as of 1/1/2021

Adjusted

budget

Budgeting

from 1/1/2021 to

as of 31.12.2021

31.12.2021

Wages, salaries, service income

and OOV (610)

966,701.00

1,027,244.00

1,027,241.52

Insurance premiums from wages (620)

352,088.00

381,559.70

381,559.70

Goods and services (630)

374,750.00

298,316.52

298,230.38

Regular transfers (640)

8,500.00

5,423.53

0

0EK0W02 (630) current expenses

25,500.00

25,500.00

25,497.84

Current expenses total (600)

1,727,539.00

1,738,043.75

1,737,952.97

Capital expenditure (700)

0EK0W02 capital expenditure

(710)

0

0

0

0

0

0

Expenses in total

1,727,539.00

1,738,043.75

1,737,952.97

a

is a

increase

office,

agendas

necessary

take into account

Similarly, as it is necessary to increase the number of employees in the context of increasing activity

and responsibilities

needs

material and technical retrofitting in the budget of the office. The increase was recorded by the office in the European and

international agenda, where the employees of the office are directly involved and must regularly

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

the subject is important guidelines and documents affecting the office's activities on behalf of Slovenská

of the Republic.

The Office carries out activities resulting not only from the Regulation and the law, but also from other special ones

regulations, for example according to the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (EU,

Euratom) 2019/493 of March 25, 2019, amending Regulation (EU, Euratom) no. 1141/2014,

regarding the procedure for verifying violations of the rules on the protection of personal data in context

elections to the European Parliament (see Article 10a, paragraph 2 of the aforementioned regulation). If the office decides

in proceedings on the protection of personal data, that a natural or legal person has violated the relevant rules

on the protection of personal data, and if it follows from the given decision or if there are other reasons

reasons to believe that the infringement is related to the political activities of a European political party or a European political foundation in the context of elections to the European Parliament, so the decision will notify the Office for European Political Parties and Foundations.

framework

3 LEGISLATIVE REGULATION OF PERSONAL DATA PROTECTION

3.1 Interdepartmental comment procedures

The office is a state administration body with nationwide scope, exercising supervision over protection personal data and participating in the protection of basic human rights and freedoms during processing personal data of natural persons. The Office fulfills its role in the field of processing supervision personal data also by overseeing and commenting on the texts of draft laws and others generally binding legal regulations (materials of a legislative nature) and also to texts non-legislative materials (visions, strategies, etc.). He formulates his comments on proposals through the Portal within the MPK. The purpose of the comments applied by the office is, so that, in particular, the quality of legislation regarding the regulation of personal data processing is high, so that the subsequently adopted legislation is precise and unambiguous, and so in relation to the operator, as well as in relation to the person concerned, whose personal data will be used in practice subject of processing.

IN

of the monitored period, the office made comments on 89 materials from of all submitted to the MPK (regardless of whether it was legislative or non-legislative material nature). In total, the office made 439 comments, 337 of which were fundamental.

The office always tries to improve the quality of the legal regulation with the comments it makes, as the case may be about the need to protect and respect the legislation regarding the processing of personal data data, if the subject of comment is non-legislative material, for example, a concept that has

in the future to be the basis for the creation of legal regulations or the fulfillment of set goals.

Smaller deficiencies in legislation can be corrected with simple comments that

in principle, they specify the correct wording of the provision, or adjust it to a form that, as far as

about processing, is correct.

The essence of the office's reminder activity consists of fundamental reminders that point to

more or less fundamental shortcomings of legal standards that need to be supplemented or revised.

In the observed period, many fundamental comments of the office were directed to the respondents

determining and clarifying the purpose for which personal data are to be processed, as many purposes as there were

formulated very generally, or they were completely absent from the legal point of view

certainties

and enforceability of the legal norm in practice would certainly cause problems and be at a disadvantage

of the person concerned. The comments also related to the scope of personal data to be processed,

as often the submitter did not provide specific data, and often could not even define them

during the adversarial proceedings, which conflicted with the principle of data minimization. Another often

a recurring fundamental reminder was the reminder requesting the deletion of certain

of the proposed provisions, as the processing proposed by them in the context of the purpose went beyond the scope

necessity and necessity. In the case of such comments, it often happened that the office from the gestor

even in the adversarial proceedings, he did not receive a satisfactory answer as to why extensive processing is necessary,

possibly what it results from and what it is supposed to achieve. In several cases there was a discrepancy

deleted by explanation and wording adjusted together. Others, more and more frequently recurring

the deficiency commented on by the office is the insufficient content of the explanatory report,

especially its special part, when especially in the provisions related to the processing of personal data

the reasons and causes of the proposed amendment, explanations from the drafter of the law are absent.

The justifications in the explanatory report are often general, given in one sentence, of which there is none

it is clear why the processing is requested and why it is necessary to the extent indicated. Very often

with a recurring reminder is the absence of internal references to other special laws which

specify and supplement the very purpose of processing personal data in terms of the legal agenda, which

16

may relate to the processing, or refer to the provision of another law, where it is established

scope or list of processed personal data for the established purpose. Last but not least,

the office also encountered an insufficient modification of the restriction within the commented materials

rights of the persons concerned for the purposes resulting from the specific submitted proposal.

In the monitored period, it also continued to influence the creation of legislation and the method of its adoption

the pandemic of the disease COVID-19, which, from the point of view of the legislation and in the opinion of the office, reflected

on

its quality rather negatively, as many legislative standards were adopted in abbreviated form

legislative proceedings, without comment. The office does not dispute that the protection of human life is

primary, but in its legislative setting in terms of preventing the spread of the disease COVID-19 would

fundamental legislative amendments should have been adopted so that they were consistent with the regulating legislation

other basic human rights, so that situations do not arise in practice where legal standards conflict with each other

they compete or collide.

Other deficiencies encountered by the office as part of its commenting activity were

the fact that the adversarial procedure was omitted several times to the fundamental comments which

the office applied and about the acceptance as well as the final form (whether comments were accepted or not)

learned only from the wording of the regulation published in the Collection of Laws.

The specific wording of the office's comments can be searched on the Portal using a filter

institutions and using the comment filter (whether it is an organization comment marked as essential,

or ordinary).

3.2 Methodological guidelines and information

The Office methodically guides operators and intermediaries in the processing of personal data

data, increases public awareness in the area of risks and rights related to the processing of personal data

data and also increases the awareness of operators and intermediaries about their obligations.

A proven form of guidance for operators and intermediaries and information

the public, especially the affected persons, based on the office's practice, became the office's methodological guidelines and short ad hoc methodologies published on the office's website, dedicated to questions and issues that are the subject of public interest at the given time or that are necessary to inform.

Among other things, the office uses a website to inform about current events related to protection of personal data. In the monitored period, the office published information regarding, for example:

□ Slovak translation of the Handbook on European legal texts in the field of personal protection

link

data

[https://dataprotection.gov.sk/uouu/sk/content/slovensky-preklad-prirucky-o-europskych-legal-regulations-in-the-area-of-data-protection\]](https://dataprotection.gov.sk/uouu/sk/content/slovensky-preklad-prirucky-o-europskych-legal-regulations-in-the-area-of-data-protection)

24/06/2021,

[published

available

(2018)

this one

on the

□ Declaration of the T-PD group of the Council of Europe on vaccinations, documents and personal protection

link

data

[https://dataprotection.gov.sk/uouu/sk/content/vyhlasenie-skupiny-t-pd-rady-europy-k-vaccination-documents-protection-of-personal-data\]](https://dataprotection.gov.sk/uouu/sk/content/vyhlasenie-skupiny-t-pd-rady-europy-k-vaccination-documents-protection-of-personal-data)

12/05/2021,

[published

available

this one

on the

□ The Committee of Ministers of the Council of Europe adopted Recommendations on the protection of individuals in connection with

with automated processing of personal data in the context of profiling [published 10/11/2021,

link

<https://dataprotection.gov.sk/uouu/sk/content/opportucania-o-ochrane-jednotlivcov-v-context-with-automated-processing-of-personal>]

available

this one

on the

□ The European Commission adopted 04.06.2021

standard

contractual clauses between

17

operators according to Art. 28 par. 7 of the General Data Protection Regulation

[published

link

<https://dataprotection.gov.sk/uouu/sk/content/standardne-zmluvne-dolozky-medzi-operators-intermediaries-brokerage>]

07.06.2021,

available

this one

on the

□ The European Commission adopted on 04.06.2021 modernized standard contractual clauses for

transfer of personal data to third countries according to Art. 46 par. 2 letters c) general regulations on the protection of personal data [published 07.06.2021, available at this link <https://dataprotection.gov.sk/uouu/sk/content/standardne-zmluvne-dolozky-pre-prenos-personal-data-to-three-countries>]

□ On 28/06/2021, the European Commission adopted two decisions on adequacy for the United States link

kingdom

<https://dataprotection.gov.sk/uouu/sk/content/rozhodnutia-o-primeranosti-pre-spojene-kingdom-for-the-purposes-of-personal-data-transfer>

11/10/2021,

[published

available

this one

on the

□ Competition – design of icons for fulfilling the information obligation of the operator

Of course, the Office monitors developments in the field of personal data protection and judgments of the European Court of Human Rights or the Court of Justice of the European Union. All relevant publishes decisions affecting the protection and processing of personal data on its website located in the Legislation and Jurisprudence section. It also informs about important decisions in the form of a short one news directly in the news on your website.

In the monitored period, the office published information regarding the decision of the European Court of Justice Union:

□ Decision of the SC of the EU in the case of Facebook Ireland and i. [published 16/06/2021, available at this link <https://dataprotection.gov.sk/uouu/sk/content/rozhodnutie-sd-eu-vo-veci-facebook-ireland-i>]

□ Decision of the SC of the EU in the case of M.I.C.M [published on 17.06.2021, available at this link

<https://dataprotection.gov.sk/uouu/sk/content/rozhodnutie-sd-eu-vo-veci-micm>]

☐ Decision of the SC of the EU in the case of Latvijas Republikas Saeima (Penal points) [published
link

25/06/2021,

<https://dataprotection.gov.sk/uouu/sk/content/rozhodnutie-sd-eu-vo-veci-latvijas-republikas-saeima-penalty-points>]

available

this one

on the

The subject of publication and indirectly

so the operators,

intermediaries as well as the persons concerned is the publication of information and guidelines issued

EDPS and EDPB on the office's website.

In the monitored period, the following guidelines and others were published on the office's website

EDPB documents about which the Office informed:

in the form of education,

☐ EDPB guidelines on the processing of personal data in connected vehicles [published
link

15.03.2021,

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-o-spracuvani-osobnych-data-in-connected-vehicles>]

available

this one

on the

☐ EDPB guidelines on a relevant and justified objection [published on 16.03.2021,

available at this link <https://dataprotection.gov.sk/uouu/sk/content/usmernenia-k->

relevant-reasoned-objection]

□ EDPB guidelines on targeting social media users [published 22/04/2021,
available at this link <https://dataprotection.gov.sk/uouu/sk/content/usmernenia-o-targeting-social-media-users>]

□ EDPB guidelines on the concepts of controller and intermediary [published on 14.07.2021,
18

available at this link <https://dataprotection.gov.sk/uouu/sk/content/usmernenia-k-by-the-term-operator-intermediary>]

□ EDPB guidelines on virtual voice assistants [published 14.07.2021, available
on this link <https://dataprotection.gov.sk/uouu/sk/content/usmernenia-k-virtualnym-by-voice-assistant>]

□ EDPB guidelines on restrictions under Art. 23 of the General Data Protection Regulation
link

[published
<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-o-obmedzeniach-podla-cl-23-of-the-general-regulation-on-data-protection>]

20/10/2021,

available

this one

on the

□ EDPB guidelines on examples of personal data breach notifications [published
link

04/01/2021,

<https://dataprotection.gov.sk/uouu/sk/content/usmernenia-o-prikladoch-oznameni-personal-data-protection-violations>]

available

this one

on the

☐ Recommendations on the legal basis for storing credit card data exclusively on

for the purpose of facilitating further online transactions

19

4 COMMUNICATION OF THE AUTHORITY WITH THE PUBLIC

4.1 Statements of the office on issues of natural persons and legal entities

The issue of personal data protection does not only concern operators or intermediaries, who have the obligation to apply personal data protection legislation in practice, but also to people, specific natural persons - affected persons, who have questions arising from ordinary situations life, related to their personal data and their processing. In the monitored period, with regard to the pandemic was still dominated by questions regarding the processing of personal health data, measurements temperatures, processing of data on children's health in schools and kindergartens, identification of employees in employment. In connection with this topic, we referred part of the questions to the National Center health information. Again, a relatively large part of the questions consisted of questions related to processing personal data in apartment buildings and installing cameras in apartment buildings. On the the office was approached by many operators about what obligations they have in connection with it with the operation of their website. Subsequently, the rights of those affected are among the frequent questions persons, deletion of data from the bank register, or from the non-bank register, also related questions with the term "Responsible Person". During the monitored period, the office recorded high demand law firms with questions in the field of personal data protection that they cannot answer to their clients.

Operators and mediators of the office most often address questions of a professional nature related to their obligations arising from the Regulation and the law, or special laws regulating processing operations. Since municipalities and cities are also operators, several of them contacted the office either in connection with testing, or addressed questions to the office in particular

regarding their position in the testing process, or the fulfillment of the information obligation towards the affected parties persons or the possibility or impossibility of using municipal or city-operated cameras on purposes of monitoring the density of people in front of the test site.

The employees of the office handled 685 questions in the monitored period, while it is necessary to take into account that the records are kept on the document, not the number of questions asked in it, so it really was answered several times more questions from the public.

4.2 Provision of information based on requests for disclosure of information according to the law no. 211/2000 Coll.

One of the possibilities for public access to information is the possibility to submit a request in terms of Act No. 211/2000 Coll. The Office, as an obliged person, evaluates these requests and in accordance with the law no. 211/2000 Coll. equips.

In 2021, the office received 228 requests to make information available. Of this total number, in 50 cases the office processed the request by making the required information available, in 44 cases issued a decision not to make the information available in part and at the same time made the information available, that could have been made available, in 40 cases the office issued a decision not to make the information available, in 30 cases, he postponed the submitted applications, as they were not within the deadline specified in the request for supplementation

supplemented. In 48 cases, the office of the office forwarded the request as the relevant department to another relevant department of the office for processing, since their content indicated that they were not a request to make information available, but for example a question from the public, or some advanced to equipment to another obliged person, to whose competences they belonged based on the assessment of their content.

20

Communication of the office with the media

4.3

The subject of questions from the media were specific problems and "cases" in which it was the subject processing or protection of personal data, or journalists' questions were directed to

specification of the rights of the persons concerned, how to apply them correctly and what is possible the affected person to claim from the operator. Processing issues persisted for the second year and personal data protection in connection with the pandemic, and subsequent measures and obligations, which were related to the processing of personal data of natural persons, especially if they were the subject processing data related to health. The repeated security measures also aroused great interest in the media incidents involving the National Center for Health Information. Subsequently, the media became interested about the case connected with the pre-election survey of the OLANO movement.

During the monitored period, the Office reminded citizens of the following days:

□ Personal Data Protection Day 2021 [published on 28.01.2021, available at this link

<https://dataprotection.gov.sk/uouu/sk/content/den-ochrany-osobnych-udajov-28-januar-2021>]

□ The second Tuesday of February is International Safer Internet Day [published

link

02/02/2021,

<https://dataprotection.gov.sk/uouu/sk/content/druhy-februarovy-utorok-je-international-safer-internet-day>]

available

this one

on the

□ 3rd anniversary of the application of the General Data Protection Regulation (GDPR) and the Act

no. 18/2018 Coll. on personal data protection in practice (25/05/2018 to 25/05/2021)

4.4 Website of the office and its traffic

The website of the office meets the conditions and technical criteria in accordance with the Revenue 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 with new and up-to-date functionalities forms, methodologies and guidelines. The Office is also based on practice in the appearance and division of the website

and tries to make the website transparent so that it is as user-friendly as possible. In the other during the monitored period, the office tried to improve and supplement the English version in particular, so that the affected persons were able to obtain information even if they do not speak the Slovak language and also in the context of the fact that the office

and the Slovak Republic were the subject of the Schengen evaluation regarding personal protection data, when access and provision of information was also the subject of interest of the evaluators in English, or in another foreign language or the language of a national minority.

The website of the office was searched a total of 698,926 times during the monitored period.

4.5 Website of the office and reporting of violations of personal data protection

The website of the office is a key source of information related to the protection of personal data.

At the same time, it is also a basic service according to Act no. 69/2018 Coll. on cyber security and on the amendment of some laws. Operators and intermediaries must ensure continuous reliability, integrity, availability and resilience of processing systems and services and at regular intervals assess the effectiveness of established technical and organizational measures. Nevertheless, it may occur (either due to deliberate action, negligence, mistake or natural event) to the violation of personal data security, which as a result may mean accidental or unlawful destruction, loss, alteration, unauthorized disclosure or making available, transmitted, stored or otherwise processed personal data.

21

The operator has an obligation under Art. 33 of the Regulation or to report a violation according to § 40 of the Act protection of personal data (so-called "data breach") of the office. He can do so in relation to the office in several ways, while one of them, recommended, is the possibility to use to fulfill this obligations for this form, published on the website of the office, which was the beginning of the observed period specified so that the office based on its details and answers therein mentioned learned all the necessary information to know the reported breach of protection personal data as best as possible.

In the monitored period, 165 violations of personal data protection were formally reported to the office (by all means specified). After research and evaluation from the mentioned number it was possible as violation of personal data protection actually flag 137 reports. The remaining 28 reports it mostly represented another agenda of the office, such as a proposal to initiate proceedings, which was unfounded a complaint filed without relevant data or another document that did not meet the requirements violation of personal data protection in accordance with Art. 33 Regulations. In graphic and statistical representation was included in the stimulus group.

Line labels

Unauthorized provision/disclosure

Cyber attack

INITIATIVE

Unauthorized processing

Loss of documentation

Theft, burglary

technical error/errors in configurations/non-observance of change management

IMI

total sum

Number of Species

incident

77

38

28

8

6

3

3

2

165

DB overview for 2021 by type of incident

3 3 2

6

8

28

38

Unauthorized provision/disclosure

Cyber attack

INITIATIVE

77

Unauthorized processing

Loss of documentation

Theft, burglary

technical error/errors in

configurations/non-compliance with change management

IMI

22

4.6 Project - 311071Z328 Electronicization of the services of the Slovak Personal Data Protection Office

In 2021, the Office started activities within the Office Project 311071Z328 Electronicization of Services

Office for the Protection of Personal Data of the Slovak Republic.

The goal of the project is to build a comprehensive information system that will be effective

electronically support office processes. The project introduces and optimizes process automation,

which will make the implementation of the agenda by office employees more efficient in their activities and facilitate

communication

external

state authorities,

operators and others.

with an office, a citizen, an entrepreneur,

subjects

to others

23

5 RESPONSIBLE PERSON

For supervising the protection of personal data processed according to the Regulation and the law

the operator is responsible. The operator and intermediary can, or must

in specified cases (Art. 37 para. 1 letter a) to c) of the Regulation, or § 44 par. 1 letter a) up to

c) of the Act) by exercising supervision over the protection of personal data to determine the responsible person while it is

obliged to report it to the office.

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

Responsible people

Total number of reported responsible persons

Period

01.01.2021 to 31.12.2021

Count

1244

The number of requests that the affected persons addressed to the office, as the operator

In the monitored period of the office, the office received 4 requests from affected persons. In all of them

cases, the persons concerned have exercised the right to access their personal data. In three cases

information was sent to the affected persons according to Art. 15 Regulations together with the required

photocopies of their personal data. In one case, the person concerned applied the request of the person concerned

person to access their personal data by email. The email contained only the last name of the person concerned

(i.e. it did not contain any verification element). Moreover, it was not obvious from him to what extent you affected person right according to Art. 15 Regulations applied. The concerned person was, in accordance with Art. 12 para. 6 Regulations by email requested to complete her correspondence address and signature as of the verification element (or guaranteed electronic signature in the case of sending in electronic form). The person concerned did not complete the required information. In view of the above, especially on the fact that it was possible to have doubts about the identity of the person concerned, as his identity was not properly verified and the fact that in connection with the processing of the application (by sending personal data to any extent) there would be a risk of unauthorized provision of this data to another person, the request of the person concerned was not processed.

24

6 APPROVAL AND CONSULTATION ACTIVITY OF THE AUTHORITY

6.1 Prior consultation

According to Art. 36 par. 1 Regulations "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 operator did not take measures to mitigating that risk."

According to Art. 35 par. 5 Regulations "The supervisory authority can establish and publish a list as well processing operations for which a data protection impact assessment is not required.

The Supervisory Authority sends these lists to the Committee; to the so-called of the list of processing operations which they will not be subject to an assessment of the impact on the protection of personal data (so-called white list) Slovak the republic has not yet joined.

According to Art. 35 par. 4 Regulations "The supervisory authority shall draw up and publish a list of those processing operations that are subject to a data protection impact assessment requirement according to paragraph 1. The supervisory authority sends these lists to the committee referred to in Article 68; list processing operations, which are always subject to an assessment of the impact of the Slovak Republic in terms of of the aforementioned article (the so-called black list), which is available on the office's website

"List of processing operations subject to personal protection impact assessment

data of the Slovak Republic". This list of processing operations serves, among other things, to

clarification of Art. 35 par. 1 Regulations and operators who intend the said processing

to be carried out if the processing intended by them would lead to a high risk for rights

and the freedom of the affected persons in the event that the operator does not take measures to mitigate this

risks, they are obliged to carry out a prior consultation with the office.

6.2 Transfer of personal data

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

or international organizations need to comply with additional protection requirements

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

personal data according to both legal regulations are the same, it is always necessary to examine the material

scope of the tool used.

Transfers can be divided into two groups:

☐ transfer to third countries (international organization) guaranteeing an adequate level

protection,

☐ transfer to third countries (international organization) not guaranteeing 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 whether it is a transfer of personal data to

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

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

decision. It is necessary for the third country to insure because of its national law or

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

equivalent to the level of protection guaranteed in the EU legal order.

The EC issues a decision on adequacy specifically for the substantive scope of the Regulation and specifically for

substantive scope of Directive 2016/680. Adequacy decisions issued by the EC over time

scope of Act no. 122/2013 Coll., remain in force unless the EC changes, replaces or

shall not be canceled by a decision adopted pursuant to the Regulation. The aforementioned decisions apply only to transmission

personal data within the scope of the Regulation, not Directive 2016/680. The office publishes

adequacy decisions on its website.

In the evaluated period, the EC issued a decision on adequacy

□ for the United Kingdom under the Regulation - Commission Implementing Decision (EU)

2021/1772 of 28 June 2021 pursuant to the Regulation of the European Parliament and of the Council (EU)

2016/679 on the adequate protection of personal data by the United Kingdom [announced under number C(2021) 4800] (Text with EEA relevance)

□ for the United Kingdom under Directive 2016/680 – Commission Implementing Decision

(EU) 2021/1773 of 28 June 2021 pursuant to the Directive of the European Parliament and of the Council (EU)

2016/680 on the adequate protection of personal data by the United Kingdom [announced under number C(2021) 4801]

□ and for South Korea according to the Regulation (at that time it had not yet been published in the Official Gazette of the EU Journal - Commission Implementing Decision (EU) 2022/254 of 17 December 2021

according to Regulation (EU) 2016/679 of the European Parliament and of the Council on adequate protection personal data by the Republic of Korea based on the Personal Data Protection Act

of information [notified under number C(2021) 9316]

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 tools offered by the Regulation and the tools that offered by Directive 2016/680.

6.2.2.1 Transfer according to the Regulation

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

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

a) a legally binding and enforceable instrument between public authorities or public entities

No such instrument was adopted in the evaluated period.

b) binding internal company rules

In the evaluated period, no binding internal company rules were adopted by the office according to Regulations.

c) standard data protection clauses adopted by the EC

In the evaluated period, standard clauses were adopted according to the Regulation, – Executive Commission Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for transfer of personal data to third countries according to the regulation of the European Parliament and the Council (EU) 2016/679 (Text with EEA relevance) – which cover transmission in the following situations:

- ☐ operator in the EU – operator in a third country
- ☐ operator in the EU – intermediary in a third country
- ☐ intermediary in the EU – intermediary in a third country
- ☐ intermediary in the EU – operator in a third country.

26

d) Standard data protection clauses adopted by the supervisory authority

In the evaluated period, the office did not adopt any standard clauses according to the Regulation.

e) approved code of conduct

In the evaluated period, no codes were approved by the office.

f) approved certification mechanism

In the evaluated period, no certification mechanisms were approved by the office.

g) contractual clauses

In the evaluated period, no contractual clauses were approved by the office.

h) provisions to be included in administrative arrangements between public authorities

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

In the evaluated period, no administrative arrangements were approved by the office.

i) exceptions for special situations according to Art. 49 Regulations

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

6.2.2.2 Transfer according to Directive 2016/680

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

to a third country or an international organization can be carried out with the help of the following tools:

a) a legally binding act providing adequate guarantees of personal data protection, or

b) the operator assessed all the circumstances of the transfer of personal data and came to the conclusion that

there are adequate safeguards for the protection of personal data,

c) exceptions for special situations according to § 76 of the Act,

d) transfer to a recipient from a third country according to § 77 of the Act.

27

7 CHECKS

Controls of the processing of personal data carried out from the position of the office as a supervisory body

are aimed at operators and intermediaries who are personal during processing

data are obliged to comply with the principles established by the Regulation and the law, as well as with respect to rights, by

law

protected interests and freedoms of the persons concerned, whose personal data are the subject of processing.

The results of the controls carried out by the authorized control body are formulated in the record

on control (if no violation of obligations was detected in the processing of personal data) or

in the control protocol (if contradictions with the requirements of generally binding legal

regulations). The results of the controls formulated in the control protocol initiate the initiation of the procedure

on the protection of personal data or are used as a basis for issuing a decision in

ongoing proceedings on the protection of personal data.

In 2021 (hereinafter referred to as the "evaluated period"), the control activity of the office was significantly influenced

unfavorable conditions resulting from the current pandemic situation, directly

(in the interest of protecting the life and health of natural persons representing entities processing personal data, as well as in the interest of protecting the life and health of office employees) and indirectly (closures accommodation and restaurant establishments, the mode of working from home applied by employers, and so on).

7.1 Controls recorded in 2021

In the course of 2021, the office registered 59 new checks on the processing of personal data.

Of the mentioned number, 18 inspections and 41 inspections (in various procedural control stage) were transferred to 2022.

Out of the total number of 59 inspections, 10 inspections were recorded in 2021 based on the inspection plan, 42 checks as part of proceedings on personal data protection and 7 checks based on suspicions from breach of obligations in the processing of personal data.

Structure of incentives for inspections registered in 2021:

50

40

30

20

10

0

Number of checks

42

10

7

Based on the control plan

As part of the proceedings

Based on suspicion

7.2 Inspections completed in 2021

In the period from 01.01.2021 to 31.12.2021, 61 inspections were completed, of which 19 were initiated (notified to the controlled person) in 2021 and 42 in the previous period. From the total of the number (61) of inspections completed in 2021, 26 inspections were completed with an inspection protocol (cases in which a violation of obligations was detected in the processing of personal data) and 35 checks with the control record (cases in which the violation of obligations in the processing of personal no data was found).

Structure of the results of inspections completed in 2021:

Number of checks

Inspections started by 31.12.2020

Checks started in 2021

Together

42

19

61

Ended

protocol

Ended

by recording

26

0

26

16

19

35

Out of the total number (61) of inspections completed in 2021, they were the inspected person in 24

in cases of natural persons, in the remaining 37 cases other than natural persons:

Controlled person

individual; 24; 39%

other than a natural person; 37; 61%

Out of the total number (61) of inspections completed in 2021, 38 inspections focused exclusively on

camera systems:

Control focus

focusing on the camera system; 38; 62%

other focus; 23; 38%

Controls of personal data processing completed in the evaluated period were carried out within

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

from the violation of obligations in the processing of personal data established by the Regulation or the law.

When creating a control plan, as well as during controls initiated by the office on the basis of

suspensions of violation of obligations in the processing of personal data, the office mainly drew on its own

experience gained while fulfilling their tasks in the field of supervision. The focus of the mentioned controls was

focused on the real state of personal data processing with an emphasis on processing compliance

activities with the requirements of legal regulation represented mainly by Regulations and laws.

Controls carried out as part of the personal data protection procedure were mainly focused on

the facts stated in the request of the administrative body of the office.

29

Structure of incentives for inspections completed in 2021:

Number of checks

34

16

11

40

35

30

25

20

15

10

5

0

Based on the control plan

As part of the proceedings

Based on guesswork

The subject of 61 inspections completed in 2021 were processing activities in 10 cases

state bodies and organizations, in 4 cases processing activities of medical facilities,

in 4 cases processing activities of local self-government bodies (cities and municipalities), in 3 cases

processing activities of banks, in 2 cases processing activities of mobile operators and in

in the remaining 14 cases, processing activities of other legal entities. In 2021 they were

checks on the processing of personal data also focused on the processing activities of 24 natural persons.

Within 61 inspections completed in 2021, no violation of the Regulation was found in 35 cases

or the law, as a result of which these checks were terminated by a check record. Performance

the remaining 26 controls were found to be inconsistent with the requirements of the Regulation, as a result of which these

inspections concluded with an inspection protocol.

Structure of inspected persons and results of 61 inspections completed in 2021:

Controlled persons

state authorities and organizations

bodies of territorial self-government

Banks

mobile operators

medical facilities

other legal entities

natural persons

Together

Deficiencies found

(control protocol)

No detected defects

(control record)

2

4

2

2

3

9

4

26

8

0

1

0

1

5

20

35

When creating a control plan, as well as during controls initiated by the office on the basis of suspicions of violation of obligations in the processing of personal data, the office mainly drew on its own experience gained while fulfilling their tasks in the field of supervision. The focus of the mentioned controls was focused on the real state of personal data processing with an emphasis on processing compliance activities with the requirements of legal regulation represented mainly by Regulations and laws. Controls carried out as part of the personal data protection procedure were mainly focused on the facts stated in the request of the administrative body of the office.

Violations were detected in the 26 inspections that were completed in 2021 with an inspection protocol the following provisions of the Regulation:

30

17

14

11

9

8

8

5

5

3

3

Article 5/1/a

Article 13

Article 5/1/c

Article 5/1/e

Article 5/2

Article 5/1/f

Article 32

Article 6

Article 35

Article 12

Article 28

2

Article 37

Article 30

Article 29

Article 15

Article 14

Article 9

Article 7

Article 5/1/d

1

1

1

1

1

1

1

1

0

2

4

6

8

10

12

14

16

18

From the graphic overview of detected violations of the provisions of the Regulation, it is clear that the most frequent (more than 5 times) non-compliance with processing principles was noted in the inspection reports personal data and incorrect, incomplete or no provision of information to the persons concerned when obtaining their personal data.

31

7.3 Selection from inspections completed in 2021

7.3.1 Controls of personal data processing in information systems, with the help of which ensures the practical implementation of the Schengen acquis

In the inspection plan, the office regularly includes inspections of the processing of personal data in information systems systems that ensure the practical implementation of the Schengen acquis competent authorities on the territory of the Slovak Republic, as well as representative offices of Slovakia republics abroad. In 2021, 4 inspections started in 2020 were completed (Národná Europol headquarters, Criminalistics and Expertise Institute of the Police Force, border crossing and computing center of the Ministry of the Interior) and 2 inspections started in 2021 (district department of the Police Force and the Criminalistics and Expertise Institute of the Police Force). All checks were ended with an inspection record, no deficiencies were found.

7.3.2 Processing of personal data by the pharmacy

In connection with the reported breach of personal data protection, a focused inspection was carried out to a medical facility providing pharmaceutical care. The security incident was unfolding from a burglary that occurred at night in the premises of a pharmacy operated

controlled person. In addition to the financial cash deposited in the cash desks of the registers cash registers, the electronic IDs of several healthcare workers were also stolen employees of the inspected person and paper tickets containing names, surnames and social security numbers customers. In relation to stolen electronic IDs of healthcare workers intended for identification and authorization when entering the electronic healthcare system (eHealth) and the controlled person for electronic signing of documents without delay asked the National Center for Health Information to block the aliens and extradite them new licenses. They had stolen tickets with the names, surnames and social security numbers of the customers to be made by two employees of the controlled person for the purpose of simplifying the selection of medicines prescribed by their family members. Control authority based on information and evidence obtained during the inspection found that the inspected person did not accept adequate security measures corresponding to existing risks, especially technical measures for security of the building and organizational measures consisting in instructing authorized employees to process personal data of affected persons (patients). Deficiencies detected by the inspection in question they were subsequently reflected in the control protocol.

7.3.3 Processing of personal data by the technical control station

The control carried out on the basis of the control plan was focused on the processing of personal data by the technical inspection station (STK) when verifying the technical suitability of vehicles for operation in road traffic, i.e. in connection with the performance of technical control. Personal data of holders of motor vehicles for the purpose of agreeing the date of technical inspection (so-called pre-contractual relations) obtains MOT through an online form published on its website, in the scope of: name and surname of the applicant, vehicle registration number, telephone number and email contact. During the performance of the technical inspection itself, it processes (obtains) personal data professionally qualified person – technician to whom technical inspection of the vehicle is assigned. Total conditions for carrying out technical checks, including the specified scope of processed personal data, including through monitoring recording devices (cameras

systems),

the law

on the operation of vehicles in road traffic. The aforementioned law also determines the conditions of operation

of the national information system of technical controls, which is operated by the authorized

technical inspection service according to § 70 par. 4 of this Act. Authorized MOT technicians

they record the performance of technical control in the national information system by creating

are monitored

control

edits

by which

MOT,

lines

32

electronic protocol for each technical inspection. During the inspection, the office emphasized on

provision of transparent information to affected persons, scope of personal data processed

data, processing security and the presence of another entity participating in the processing

personal data. In order to comply with the principles of personal data processing, it is an obligation

the operator to clearly and transparently inform the data subject about the processing operations

and the reasons that authorize the operator to perform specific processing operations.

The controlled person provided the concerned persons with information in a confusing manner, while the information

it also incorporated the consents of the persons concerned, which were not necessary for the processing and did not comply at

the same time

conditions of freely given consent. Controlled person except as specified by law

monitoring device with recording had its own camera system installed, which

operated for the purposes of legitimate interests without performing the so-called

proportionality test. Operation of the mentioned camera system without a pre-conducted test

proportionality, the controlled person acted in violation of the principle of legality according to Article 5 para. 1 letter a) Regulations. The inspection also revealed deficiencies in determining the retention period camera recordings, as the controlled person set an unreasonably long 10-day period their storage, thereby contradicting the principle of minimizing data storage according to article 5 par. 1 letter c) Regulations. When evaluating the level of security, it was found that the controlled person did not have prepared records of processing activities. They were the control terminological inaccuracies in contracts on the processing of personal data that were not found caused by the controlled person, since the contract in question is drawn up by the operator of the national information system for all MOTs. The inspection was completed with a protocol about control.

7.3.4 Processing of personal data by the medical facility

On the basis of notification of the person concerned, to whom it was in the past from the controlled party health care provided by the medical facility, the office dealt with the suspicion that the personal data of this person concerned were not processed in accordance with the principle of integrity and confidentiality according to article 5 par. 1 letter f) Regulations, as there was supposed to be a loss of the medical part documentation. Responsibility for the safe storage of medical documentation follows to the health care provider under the Health Care Act and how to the operator processing personal data related to the health of patients also from the Regulation. To carry out a check, during which it would be possible to get acquainted with data on the health of the person concerned person in connection with the verification of the loss of part of his medical documentation, it was necessary have the written consent of this person concerned. The institute was also used during the inspection cooperation, in which the law enforcement authorities provided expert opinions, which among other things, they also commented on the fact whether the medical documentation is related to the medical performance provided in a controlled medical facility is complete. The control dealt exclusively by maintaining health documentation as an integral part of providing health care care in the sense of its preservation by the controlled person as a healthcare provider

care had to be kept for 20 years from the last provision of health care care. The control was in connection with the processing of personal data in the health department in the documentation, at least one person found a contradiction with the principle of integrity and confidentiality, as the set of personal data forming the health documentation of the person concerned was not processed in a way that guarantees adequate security of personal data, including protection against unauthorized or illegal processing and accidental loss, destruction or damage through appropriate technical and organizational measures. They were found by inspection also other shortcomings in connection with the obligation of the controlled person to carry out an assessment of the impact on personal data protection when the controlled person did not assess the necessity and adequacy processing operations in relation to the purpose and did not deal with the assessment of risks for rights and freedoms of the persons concerned, which was largely related to the weak level of the controlled person's response to new legislation applicable to the field of personal data protection. A controlled person in a relationship

33

to information provided to data subjects through its website at the same time, it did not provide complete, clear and understandable information, as it did not provide the information on the purpose (providing health care as the basic activity of a medical facility) and the legal basis for the processing of personal data (the processing of personal data follows healthcare provider by law). Deficiencies detected by the inspection in question they were subsequently reflected in the control protocol.

7.3.5 Processing of personal data by the city's camera system

Inspection of the city's camera system initiated by suspicion of violation of duties at processing of personal data was focused on the obligations of the operator in monitoring spaces accessible to the public. During the inspection, it was found that the operator at processing of personal data of the persons concerned for the purpose of protecting property and ensuring safety of citizens and visitors to the city, he proceeded in violation of the principle of minimization of storage according to Article 5 par. 1 letter e) Regulations by keeping the personal data of the persons concerned for a period of time

longer than the time necessary to achieve the intended purpose. The inspection further revealed, that the operator acted contrary to the principle of data minimization according to Article 5 par. 1 letter c) Regulations by using some cameras to monitor the space beyond the range necessary for achieving the purpose of processing. In relation to the information provided to the persons concerned at obtaining their personal data, compliance with the requirements was noted by the control authority Regulations. Deficiencies found during the inspection were subsequently reflected in the protocol about control.

7.3.6 Processing of personal data for the purpose of issuing resident parking cards

On the basis of the suspicion of violation of obligations in the processing of personal data, the office carried out control of the processing activities of the operator entrusted with the operation of parking lots area of the city (city district). During the inspection, it was found that the inspected person based applications are issued to persons with permanent residence in the so-called resident parking cards (RPK), while for the purpose of issuing the RPK it requires personal data from the affected persons (applicants) in the scope of: first name, last name, address of permanent residence, apartment number, telephone contact, e-mail and the registration number of the vehicle for which the applicant requests the issuance of an RPK. Together with the request for extradition

RPK requires the inspected person to send a copy of the Vehicle Registration Certificate (Part I), a document proving the applicant's relationship to the apartment (ownership certificate, lease agreement or other document) and a certificate of permanent residence issued by the relevant city district (in the case of the first application or changes of permanent residence). In the past, the controlled person also required the applicant to send photocopies of the identity card. Control authority based on information and evidence obtained during the inspection, he found that the inspected person violated the principle minimization of personal data according to Article 5 par. 1 letter c) Regulations, insofar as it had data verify permanent residence and apartment number through the relevant city district (contract obligation of the city district) and only if the city district does not have certain data, it should for the purposes of prevention against the abuse of RPK, request a document proving it from the person concerned

the applicant's relationship to the apartment. During the inspection, a violation of Article 14 of the Regulation was detected by the fact that the controlled person did not inform the affected persons about the acquisition of personal data from the information systems of the relevant city district. The inspection was completed with a protocol about control.

7.3.7 Monitoring tables in a fast food facility

By checking the processing activities of an entity operating in the field of service provision of fast food, which the office carried out based on the initiative of the person concerned, was found unwanted monitoring of tables where customers were consuming food and drinks. Controlling

34

the authority concluded that the established fact collides with the principle of data minimization according to the article 5 par. 1 letter c) Regulations. At the same time, the controlled person did not prove that the monitoring is necessary for the purposes of the controlled person's legitimate interests, or she did not prove that her legitimate interests in such processing prevail over interests or fundamental rights and freedoms of affected persons (customers). Due to the identified processing deficiencies the control of personal data by the controlled person was terminated by the control protocol.

7.3.8 Monitoring of publicly accessible spaces by a state institution

The inspection was carried out on the basis of a tip pointing to a camera system in operation central authority of the state administration. The inspection found that the processing of personal data camera system is in a specific case aimed at the protection of state property under management controlled person and to protect the life, health and safety of employees and visitors, respectively is considered necessary by the controller for the purposes of legitimate interests which the controlled person is watching. The necessity of processing personal data and the condition predominance of their interests over the interests or fundamental rights and freedoms of the person concerned the controlled person was involved in the proportionality test, where he identified his authorized person interest, assessed its legitimacy, necessity and appropriateness, and subsequently assessed it proportionality in relation to the fundamental rights and freedoms of the persons concerned. Justifications

stated in the proportionality test, the office accepted as sufficient. Via camera the system monitored the entrance area to the controlled person's object and the immediate area the surroundings of the building (parking lot and entrance for vehicles). The inspected person had a set deadline storage of personal data by the camera system for 72 hours and records from all cameras were subsequently lubricated. During the inspection, the images of individual cameras were also checked - in the case of the camera monitoring the entrance for vehicles, it was found during the inspection that the inspected person except its entrance for vehicles also monitors part of the public footpath, i.e. the area of which monitoring is not necessary to fulfill the stated purpose of personal data processing.

On the basis of the detected contradiction with the principle of data minimization according to Article 5 par. 1 letter c) The inspection of the Regulations was concluded with an inspection report.

7.4 Conclusions

Despite the continuously modified bans and restrictions related to the disease pandemic In the evaluated period, the standard level of control activity of the office was maintained due to COVID-19. However, an increasing burden was identified with the checks of camera systems, which are to a significant extent operated by natural persons - individuals in their dwellings, while in these cases, the protection of the rights of the monitored affected persons often overlaps with those of the neighbors or other disputes.

35

8 PERSONAL DATA PROTECTION PROCEEDINGS

The purpose of the procedure on the protection of personal data is to determine whether there has been a violation of the rights of natural persons in processing of their personal data or there has been a violation of the provisions of the Regulation, or the law, and in case of detection of deficiencies, if it is reasonable and expedient, to impose corrective measures, as appropriate fine. The provisions of the administrative order apply to proceedings on the protection of personal data.

If the competence of the office is not given to act and decide on the matter, the office has the obligation to submit forward to the relevant administrative authority. In the monitored period, the office forwarded a total of 49 submissions

to another competent administrative authority for action and decision.

Legal regulations in the field of personal data protection allow the office to submit in exhaustive form

postpone in specified cases. The office had to postpone the submission in his case

groundlessness, in the event that the matter to which the submission was concerned was discussed by a criminal enforcement authority

proceedings, in case the applicant did not provide the necessary cooperation to the office at his request, while without

it was not possible to handle the matter without his active participation, and in the event that, from the event to which the submission was related,

more than three years have passed on the day of its delivery. The most common reason for postponement was

the groundlessness of the submission, when it was already clear from the evidence submitted by the person concerned,

that there was no violation of legal regulations in the field of personal data protection. In the watched

period, a total of 306 submissions were postponed.

The Office, as part of its supervisory activities, conducts proceedings on the protection of personal data with the aim of protecting rights

natural persons from unauthorized interference in their private life during their processing

personal data, while also examining compliance with the obligations set by the Regulation

and the law. If it detects a violation of the rights of the person concerned or non-fulfillment of obligations during processing

personal data, by decision, if it is reasonable and expedient, to the operator or

to the intermediary to take measures to eliminate deficiencies and causes within the specified period

of their occurrence, or imposes a fine on him, depending mainly on the seriousness of the detected violation.

Otherwise, the proceedings on personal data protection will stop.

Proceedings on the protection of personal data are initiated at the request of the petitioner or on his own initiative

office. Proceedings on the authority's own initiative are initiated on the basis of an initiative, on the basis of results

control, by which deficiencies were detected or based on the findings of the office from its own activities

on suspicion of violation of legal regulations in the field of personal data protection, as proceedings

started without a proposal.

In the monitored period, the office initiated a total of 218 administrative proceedings, of which 135 were initiated at the proposal of the person concerned, 43 started based on the initiative, 19 started based on the results inspections, which identified deficiencies and 21 proceedings were conducted by the office on its own initiative based on suspicions of violation of legal regulations in the field of personal data protection.

An overview of the ways of initiating proceedings within the monitored period

Year

2021

Based on

Based on

Based on

From my own

proposal

stimulus

of control results

initiatives of the office

135

43

19

21

The decision of the office, as an administrative body in the first instance in proceedings on the protection of personal data, it is based on a reliably ascertained state of affairs. For this purpose, the office is in the process of personal protection authorized to request cooperation from anyone, while in the evaluated period the office requested

36

by cooperation a total of 967 times. In the proceedings on personal data protection, there were two cases when the entity from which cooperation was requested did not respond to it and the office even after being asked to comply did not provide cooperation obligations (in the given cases, proceedings were initiated against the subjects

on a fine or on an orderly fine).

In connection with raising awareness of personal data protection among the public, cases or the media were also often interested in the results of the proceedings. The Institute of Legal Representation was evaluated period used in a considerable number of cases, and the cases where all the participants in the proceedings were represented by legal representatives.

The most frequent subject of proceedings on the protection of personal data was review or processing personal data of the persons concerned in the information system, which included cameras, there was no violation of legal regulations in the field of personal data protection.

Among the most frequent violations was the processing of personal data contrary to the policy legality, when personal data was processed without a legal basis, or in violation of the legal basis and processing in violation of the principle of integrity and confidentiality, which it was related to the failure to take adequate security measures.

37

9 COOPERATION AND CONSISTENCY MECHANISM

The functioning of the internal market requires that there is no free movement of personal data within the Union limited or prohibited, not even for reasons related to the protection of natural persons during processing personal data, which is also reflected in the provisions of Art. 1 paragraph 3 Regulations. On the said Regulation responds by introducing cooperation and consistency mechanisms to guarantee 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 the cooperation between supervisory authorities, whether the need is mutual cooperation will arise as part of the investigation of a specific suspicion of a violation of personal protection data or as part of other activities of the supervisory authority (e.g. solving legal issues, provision of consultations). Given that the rules of cooperation are regulated directly in the Regulation, no further special agreements between member states are required

for this purpose.

9.1.1 Cross-border processing

Pursuant to Art. 55 Regulations, each supervisory authority fulfills the tasks and exercises the powers published By regulation on the territory of your state. However, the regulation also specifically regulates the procedure and jurisdiction in proceedings for cross-border processing of personal data. Cross-border processing is within the meaning Art. 4 point 23 of the Regulations a) processing of personal data that takes place in the Union in the context activities of the operator's or intermediary's establishments in more than one member state state, while the operator or intermediary is established in more than one member state the state; or b) processing of personal data that takes place in the Union in the context of the activities of the sole establishment of the operator or intermediary in the Union, but which significantly affects or is likely to significantly affect data subjects in more than one Member State.

The Regulation regulates cooperation between supervisory authorities, primarily in connection with the mechanism of a single point of contact (the so-called one-stop-shop) regulated in Art. 56 para. 1 of the Regulation, according to which the supervisory authority is the main establishment or the only one establishments of the operator or intermediary authorized to act as a supervisor authority for cross-border of this operator, respectively intermediary. According to Art. 56 par. 2 of the Regulations, each supervisory authority is competent to deal with with a complaint submitted to him or a possible violation of the Regulation, if the facts are relevant only establishments in its member state or substantially affects the persons concerned only in its member state. In accordance with Art. 4 point 22 of the Regulations other supervisory authorities will be for this processing in the position of the concerned supervisory authorities, if a) the operator or the intermediary is established in the territory of the member state of this supervisory authority; b) affected persons residing in the member state of this supervisory authority are significantly affected or will be likely to be substantially affected by processing; or c) the complaint was submitted to this supervisor authority.

The determination of the lead supervisory authority and the concerned authorities is carried out in the IMI system (Internal Market Informational System - Information system about the internal market), within which there is an exchange of information about specific processing between the individual supervisory authorities and a specific suspicion of a violation of personal data protection, or as long as the investigation started on the basis of a complaint from the person concerned, as well as about the content of this particular complaint.

Exchange

information is provided in English.

processing carried out from

parties

38

In the monitored period, the office received 1071 notifications regarding determination in the IMI system the head and the supervisory authority concerned. Based on careful consideration of each item the office assessed that it is the concerned supervisory authority in 184 cases; most often for the reasons that the processing of personal data in question significantly affects or is likely to significantly affect will affect affected persons residing in the territory of the Slovak Republic. Most often it went o operators of social networks, various airlines, operators providing online games, various e-shops, etc. In some cases, the office was also concerned because the operator or intermediary is established on the territory of the Slovak Republic, i.e. on the territory The Slovak Republic has one or more establishments. If the office has assessed that it is the affected person supervisory authority, marked it in the IMI system and followed up the case further. In accordance with Art. 60 Regulations the office had the opportunity, as necessary, to comment on the requests of the head of the supervisory authority, on his the procedure and the results of the investigation and also to comment on draft decisions. If the office to the concerned supervisory authority due to the fact that it received a complaint, the office acts as point of contact for the person concerned and informs him of the decision of the head of the supervisory authority. A total of 31 submissions containing elements were delivered to the Office in the monitored period of cross-border processing and 13 notifications of violations of personal data protection, so-called data breach.

These submissions were received either from foreign persons or directed towards foreigners operators, among others, for example, towards operators established in Belgium, Austria, the Czech Republic or Ireland. The Office within each submitted submission first examined (the so-called preliminary examination of the complaint) whether the subject of the submission meets the requirements of the proposal, respectively initiative according to § 100 par. 3 of Act No. 18/2018 Coll. and also whether it meets the conditions cross-border processing according to Art. 4 point 23 of the Regulations, or whether the definition according to Art. 56 par. 2 Regulations. In the submissions in question, the Office also determined its substantive competence, whereas the office forwarded 6 submissions to another administrative body for processing. If the subject of the submission based on a reasonable suspicion of a violation of personal data protection, the statement stated by the office checked also in cooperation with the supervisory authority of the member state in whose territory it was the operator of the main or sole establishment. In 8 cases, the office submitted the received submissions into the IMI system and further resolved them in cooperation with the supervisory authorities responsible for the processing the leading supervisory authority. The Office forwarded the said complaint through the IMI system supervisory authority of Belgium, Austria, forwarded two complaints to the Czech Republic, and four the office forwarded the complaints to the Irish supervisory authority. In the monitored period, the office was marked as the leading supervisory authority in 3 cases, based on the location of the operator's headquarters, while these complaints were forwarded to the Office through the IMI system by the supervisory authorities of Hungary, Lithuania and Spain.

9.1.2 Mutual assistance

The Office cooperates with other supervisory authorities outside the one-stop-shop mechanism. This one cooperation also takes place in the IMI system, which enables the sending of specific requests selected supervisory authority. However, the office also handles email or written requests other supervisory authorities.

During the monitored period, the office received 67 requests from other supervisory authorities in the IMI system on cooperation in the sense of art. 61 Regulations. In the applications in question, the supervisory authorities requested the

office

for his legal opinion, especially regarding the interpretation of the provisions of the Regulation. The requests concerned e.g. legal basis for personal data processing, interpretation of the articles of the Regulation, practical experience and application of national legislation, processing personal data during pandemic, space monitoring with security cameras, special category processing personal data, the legal basis for the use of cameras in connection with health care, ways of handling complaints, interpretation of Art. 5 par. 2 Regulations (principle

39

responsibilities), etc. Some supervisory authorities informed the office about the delivery in this way notification of a breach of personal data protection or used this method for consultation specific case before starting the one-stop-shop mechanism.

During the monitored period, the office sent 14 requests for cooperation in the IMI system pursuant to Art. 61

Regulations. The requests concerned information about specific cross-border cases, consultations

individual cases or the legal opinion of other supervisory authorities regarding the interpretation

Regulations. For example, the office asked other supervisory authorities about the experience of others

supervisory authorities in connection with proving negative tests for the disease COVID-19

employees at the operator's workplace, to cameras monitoring the working environment,

for notifications of personal data breaches. Office through the IMI system in terms of

Art. 61 The regulations were investigated, for example, by the head office, or establishment of individual

operators against whom a complaint was filed and who did not have their registered office in the territory of Slovakia

of the Republic. The Office also used other forms of mutual cooperation with other supervisory bodies

communications such as the IMI system (email, written and telephone communication), which he used

contacts acquired during their activity, including contacts acquired within

membership in the Committee's expert groups.

9.1.3 Joint operations of supervisory authorities

As part of the cooperation mechanism, in accordance with Art. 62 Regulations can also carry out joint operations

supervisory authorities, taking into account joint investigations and joint measures in the area of enforcement. In the monitored period, the office did not initiate or accept a request for such implementation of joint operations of supervisory authorities.

9.2 Consistency Mechanism

An important attribute of the Regulation is its consistent application. In order to achieve this goal, the regulation regulates the consistency mechanism, which can be understood as cooperation between EEA supervisory authorities, and in relevant cases also with the EC.

9.2.1 Opinion of the EDPB

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

the authority plans to take concrete measures. For this purpose, the supervisory authority should notify the EDPB of its draft decision. The regulation regulates the cases when the supervisory authority is obliged to request the EDPB for an opinion (Art. 64 para. 1 of the Regulation) and when he has the opportunity to request an opinion (Art. 64 para. 2 of the Regulation).

In the monitored period, the Office asked the EDPB for an opinion pursuant to Art. 64 para. 1 letter c) of the Regulation aimed at approving the criteria for the accreditation of the monitoring entity for codes of conduct according to Art. 41 of the Regulation. In the opinion, the office was not given any recommendations for correction.

40

9.2.2 EDPB dispute resolution

The EDPB's dispute resolution enables a binding decision to be taken to ensure consistent application of the Regulation in the following cases:

- ☐ A relevant reasoned objection was raised by the concerned supervisory authority or rejected by the leading supervisory authority (Article 60 of the Regulation);
- ☐ Disagreement with the designation of the leading supervisory authority (Article 56 of the Regulation);
- ☐ Absence of EDPB consultation (Article 64 of the Regulation);
- ☐ The supervisory authority did not proceed according to the opinion of the EDPB (Article 64 of the Regulation).

In the evaluated period, the EDPB did not resolve any dispute concerning the office.

9.2.3 Procedure for urgent cases

Article 66 of the Regulation regulates the procedure mechanism for urgent cases. In exceptional in cases where the supervisory authority concerned considers it urgent to protect rights and freedoms affected persons, may take temporary measures with legal effects in its territory. Validity these measures may not exceed three months. In this case, the supervisory authority is concerned obliged to inform other supervisory authorities, EDPB and EC.

If the supervisory authority believes that it is necessary to urgently take final measures, it can request EDPB for an urgent opinion or for an urgent binding decision. Any supervisory authority can to request an urgent opinion or a binding decision from the EDPB in cases where appropriate the supervisory authority has not taken appropriate action and there is an urgent need to act. In the evaluated period the office did not apply this article.

41

10 SANCTIONING

Sanctions for violation of the Regulation and the law are a fine and a fine. Sanctions are in the data optional modified by legal standards, i.e. that not every detected violation is automatically required end by imposing a sanction. The Office imposes fines and administrative fines depending on the circumstances each individual case. Office when deciding on imposing a fine and determining its amount takes into account in particular the nature, seriousness and duration of the violation, the number of affected persons, the extent of the damage, if it arose, the possible culpability of the personal data protection violation and the measures that were taken to mitigate the damage suffered by the affected persons. The office also takes into account the previous ones violations of personal data protection, degree of cooperation with the office in the correction of the violation and mitigation the possible adverse consequences of the breach, the category of personal data that was breached concerns and the manner in which the Office learned about the breach of personal data protection.

As part of the approved budget for 2021, the Office also determined a binding indicator of income, which

means that an amount of EUR 100,000 has been approved for 2021.

The required mandatory indicator was not met in the monitored year, the office had to go to the state one of the budget as of 31.12.2021, return the difference between the planned and actual amount of the indicator in the amount of EUR 13,170.25.

Please note that the office registers two decisions in proceedings on the protection of personal data, by which a fine was imposed in the monitored year, while the participants in the proceedings paid the fines up to in 2022. These are fines in the amount of EUR 1,000 and EUR 40,000."

10.1 Fine

In the monitored period, the office for violating legal regulations in the field of personal data protection validly imposed 53 fines in the total amount of EUR 110,900. In the monitored period, he chose the office a total of EUR 89,289.10 in fines. The average fine was EUR 2,092. The lowest fine in the amount of EUR 100 was imposed by the office on a natural person who, in the position of operator, is not authorized processed the personal data of the persons concerned through cameras installed in the gardener's office settlement. The office legally imposed the highest fine in the amount of 40,000 euros on the operator for violation of the principle of responsibility (he did not prove that he had carried out an assessment of the impact on personal protection data), principles of justice and transparency as well as Art. 28 Regulations (the operator did not have an intermediary contract concluded with the intermediary).

Overview of imposed and collected fines in the monitored period

Watched

period

Count

fines

Total height

legally

imposed fines in Euros

Average height

fines rounded up to

whole Euro up

Total selected on

fines in Euros

2021

53

110,900

2092

89,289.10

The fine, as a type of sanction, performed a repressive as well as a preventive function in the evaluated period. At its filing office took into account, among other things, the position of the subject and its activity, 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 assessee periods for violation of legal regulations in the field of personal data protection can be established, that the imposed fines did not have liquidation effects.

42

10.2 Disciplinary fine

The disciplinary fine serves to ensure a dignified and undisturbed course of supervisory activity office. The office can impose a fine on the operator or intermediary, or to a representative of the operator or intermediary, if it hinders the performance of the control or if does not ensure adequate conditions for its performance. The office can also impose a fine to a person who is not an operator or an intermediary, for not providing the requested cooperation of the office in the exercise of supervision. In the monitored period, the office imposed one administrative fine in the amount of EUR 500 for non-cooperation.

10.3 Selected cases from the office's supervisory activities

10.3.1 Postponements

10.3.1.1 Forwarding of Anonymous Submission

The Office assessed the proposal of the petitioner, who turned to the operator with a submission where he requested, so that the applicant's identity is kept secret during its processing. The operator to whom the petitioner addressed the submission, forwarded it due to affiliation, while considering he did so in the form of a photocopy without personal data at the petitioner's request to conceal his identity the petitioner. The petitioner claimed in the proposal that despite the fact that the operator upon assignment of the submission, his request for anonymity was formally granted by the body to which the submission was made forwarded, he could, based on several circumstances, find out that the submitter is the petitioner and the operator thus violated the protection of the petitioner's personal data. Authority after review of the documents submitted by the petitioner stated that the circumstances from which the petitioner judged on the possibility of finding out that the submitter of the anonymized submission is the operator he could neither foresee nor have any influence over them; the operator based on the petitioner's the request for the secrecy of his identity assessed whether it is necessary to provide for the purpose of forwarding the submission personal data of the submitter, that he forwarded the petitioner's submission without data about his person, thereby proceeding in accordance with the principle of data minimization according to Art. 5 para. 1 letter c) Regulations and took appropriate measures to preserve the petitioner's anonymity. For the stated reasons, the Office postponed the proposal according to § 100 par. 5 letters a) of the Act no. 18/2018 Coll.

10.3.1.2 Disclosure of personal data in reports

In the monitored period, the Office received several submissions in which the submitters objected to publication personal data of the persons concerned through reports broadcast on television and later available on the operators' websites. Based on published by the operator personal data thus it was possible to identify a natural person. In case of publication of personal data data by the media, the right to personal data protection conflicts with the right to freedom

expression and the right to information, both of which represent fundamental rights in a democratic society companies. The regulation established the right for member states to harmonize national regulations for the protection of personal data and the right to freedom of expression and the right to information, including processing for journalistic purposes and establish exceptions or deviations from some chapters of the Regulation.

In relation to the submissions in question, the office stated that the operators upon publication of personal data proceeded according to § 78 par. 2 of the Act, according to which the operator can process personal data without the consent of the person concerned even if the processing of personal data is necessary for the needs of informing the public by means of mass communication and if personal data is processed by the operator, to whom it follows from the subject of the activity (subject the provision provided a legal basis for the given processing – publication of personal data).

Processing of personal data of affected persons by the operator for information purposes
in conclusion

Sat

43

to the public resulted from the subject of the activity. The operators are in accordance with the applicable legislation authorized to obtain true, timely and comprehensive information for the purpose of informing the public and are not responsible for the content of the information provided by a defined group of persons. However, it is also true that operators by processing the personal data of the persons concerned for journalistic purposes according to § 78 par. 2 of the Act must not violate the right of the person concerned to protect his personality or the right to protect privacy. Assessing the fact or publishing the personal data of the persons concerned the right to protection was interfered with by means of mass communication for journalistic purposes the personality and privacy of the persons concerned falls under the jurisdiction of the general court (personality protection). In the case of the publication of such personal data by means of mass communication, which would could cause an unauthorized interference with the right to protect the personality and privacy of the person concerned, the person concerned has the right to seek protection in court. Office for the stated reasons (existence of the legal basis of publication) postponed submissions (proposals and suggestions) due to their unfoundedness.

10.3.2 Proceedings

10.3.2.1 Processing of telephone number

The Office conducted proceedings on the protection of personal data based on the proposal, according to which the operator processed the petitioner's phone number in an illegal manner, as he contacted the petitioner by phone call with an offer of services, while the applicant does not give his phone number or consent did not provide it to the operator for processing, and the caller asked the petitioner where he got it from his phone number, he did not give him an answer, which the petitioner did not get even with a written request for this information with which he subsequently contacted the operator. The operator objected that in his information systems does not process any personal data of the applicant, does not process him phone number and he doesn't even know it. The phone call in question was made by an authorized employee acquire new clients for the operator, who, however, did not act in this way on the basis of instructions the operator, he does not in any case authorize employees to use it for the performance of work personal data that would not come from its databases and for which it would not have the legal right to process basis. Therefore, according to the operator, in the given case, there were no violations of the Regulation on his part, but about the individual misconduct of the employee in the field of labor law, where the operator carried out the remedy by re-instructing the employee on the performance of work duties.

The operator also communicated these facts to the petitioner in response to his request and has for equipping her with it properly. The office stated that even if the employee in a specific case he did not actually act on the operator's instructions, he made the given phone call as a person acting based on the authorization of the operator, i.e. j. as the person whom the operator entrusted with the acquisition new clients, which was the employee's own work activity and at the same time the only one the purpose of the given phone call; the employee processed the applicant's phone number for the purpose of the activity, which is carried out by the operator through its employees and is in accordance with the principle responsibility according to Art. 5 par. 2, Art. 24 par. 1, Art. 32 par. 4 Regulations obliged to ensure that employees processed personal data in accordance with the Regulation and only on the basis of instructions operator. The office concluded that the operator of the processing operation with the telephone

by the petitioner's number, which he carried out by contacting his employee by phone

the petitioner

whereas

to the appellant's question where he got his phone number, he did not give him an answer, he processed it

petitioner's personal data without a legal basis according to Art. 6 par. 1 Regulations and without compliance

obligations according to Art. 14 par. 2 letters f), par. 3 letters b) Regulations, thereby violating the principle of legality

and transparency according to Art. 5 par. 1 letter a) Regulations. At the same time, the Office stated that the petitioner

by a written request for information on how the operator obtained his phone number, properly applied

the right of the person concerned to access personal data according to Art. 15 par. 1 letter g) Regulations which

the operator's response was not fulfilled because it did not provide any information about the source

of the data in question, nor did he state that the requested information is partially or fully available to him

unavailable and for what reasons. The Office imposed a corrective measure on the operator according to Art. 58

to the operator

client,

new

purpose

gain

for

44

para. 2 letters c) Orders to provide the claimant with any available information unless

this is the source from which his phone number was obtained for the processing operation in question.

10.3.2.2 Processing of personal data as part of an insurance claim

During the monitored period, the Office conducted proceedings based on the petitioner's proposal, in which she objected

unauthorized processing of personal data listed in the technical license of the newly purchased product

motor vehicle for the purpose of payment of insurance benefits. According to the claims of the petitioner,

the operator in connection with the payment of insurance compensation for total damage to the motor vehicle

requested the documentation of the technical license for the newly purchased motor vehicle. The petitioner stated that the operator conditioned the technical license for the newly purchased vehicle payment of the insurance payment for the highway stamp and for the fee for registering a new vehicle. The petitioner stated that, based on this pressure, this technical license was finally issued provided to the operator. However, the petitioner claimed that the operator of this document he requested despite her warnings that this document was not necessary. The petitioner objected, that the newly purchased vehicle cannot have any connection with the insurance event that happened even before purchasing a new vehicle. The operator during the procedure on personal protection data in cooperation with the company that liquidated the claimant's insurance claim ensured, investigated the processing of data from technical license of the new vehicle petitioners, while the operator came to the conclusion that with regard to the application of the principle minimization, the liquidation of the insurance event in question could be processed even without data from the technical license of the applicant's new vehicle and these data subsequently from the information systems deleted. The office concluded that the operator violated Art. 5 par. 1 letter c) Regulations (principle of minimization of personal data) by the fact that during the process of liquidation of the insurance claim the petitioner also processed data from the technical license of the petitioner's new vehicle, while the operator, after re-investigating the liquidation process, concluded that the liquidation of the insurance premium the petitioner's events could have been processed even without this data. The office stated that the operator is authorized in accordance with legal regulations within the framework of the occurrence of a damage event from injured parties to request the documents necessary for a true explanation of the occurrence and scope of the insurance event as well as its consequences. However, the operator should require these documents in accordance with the principle data minimization according to Art. 5 par. 1 letter c) Regulations, and thus require only such documents and personal data that is reasonable, relevant and limited to the extent that is necessary considering the purposes for which they are processed. On the basis of the established facts, the Office did not impose corrective measures to the operator, because in view of the steps taken by the operator

(deletion of all records about

technical license of the petitioner's new vehicle

from the operator's information systems) the office did not consider it expedient and reasonable to impose on him corrective measures, however, the office imposed a fine on the operator for the detected violation.

10.3.2.3 Monitoring of employees through the location of their SIM card

In 2021, the Office conducted proceedings on the protection of personal data based on a proposal in which the petitioner stated that the operator, as his employer, monitors the petitioner's location

at the time of his vacation, i.e. at the time when the petitioner was not performing his duties as an employee

obligations. Through the investigation, the Office found that the operator, by the above procedure, without serious reasons violated the employee's privacy by monitoring him during his time off. Operator

therefore, he did not have an adequate legal basis for the said processing operation. Saving

it was further established that the operator did not even demonstrate an adequate legal basis in the proceedings

for the processing of personal data in the case of monitoring the location of employees within their

working time. Basic rights and freedoms on the one hand and legitimate interests of the operator

on the other hand, they must be carefully examined and compared. Operator within the proceedings

did not demonstrate an adequate legal basis for such a processing operation, as in the given

in this case, he did not deal at all with the comparison of the individual rights of the affected persons with his corrected one

45

interest. In the matter in question, the Office imposed corrective measures and a fine on the operator.

10.3.2.4 Publication of the social security number in the report

In 2021, the Office conducted proceedings on the protection of personal data based on an initiative in which

the applicant objected to the publication of personal data of the person concerned, including his social security number through news reports broadcast on television and available later

in the archive on the website of the operator. The personal data of the person concerned were not in the report

anonymized in any way. The operator must for each purpose of personal data processing

data have an adequate legal basis that defines the conditions under which it is

legal processing. When processing personal data, it can be used for the purpose of determining the physical a person's generally usable identifier - social security number only if its use is necessary to achieve the given processing purpose. The investigation revealed that it was not congenital in the given case the number of the person concerned needs to be processed at all, since the purpose of the processing operation (providing services to the public in the field of television broadcasting) could be achieved even without publication of the birth number of the person concerned (by anonymizing it). In addition, publish the birth number is law no. 18/2018 Coll. exclusively prohibited (unless it was published by the affected person person). The Office did not impose remedial measures on the operator for the given violation, as the operator, even before the start of the procedure, the birth number of the person concerned in the report available at anonymized the operator's website, thereby removing the illegal status and the imposition of measures for correction was no longer reasonable and expedient in the given case. However, the office imposed a fine for the given violation fine to the operator.

10.3.2.5 Sending correspondence containing personal data in unencrypted form

In 2021, the office conducted proceedings on the basis of a proposal in which the applicant objected to sending her personal data to the operator in the scope of name, surname, address, address of the insured real estate, insurance policy number, claim number, type and type of insurance through an email containing this data to a foreign email address. The investigation revealed that the petitioner the mentioned data were sent to a foreign email address in an unencrypted form. Address of the insured real estate, insurance policy number, claim number, type and type of insurance per se are not are personal data, but in connection with the name, surname or address of the applicant represent personal data relating to a specific person (applicant), which is possible on the basis of reliably and unmistakably identify the given data. In case of sending personal data at the same time, there was unauthorized access to the petitioner's email address personal data of the petitioner to another person (the operator did not have adequate legal basis in the sense of Art. 6 par. 1 of the Regulations). In terms of the principles of integrity and confidentiality, they must be

personal data processed in a way that guarantees adequate security of personal data including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, through appropriate technical or organizational measures measures (e.g. password security in the case of sending email attachments). Regarding unauthorized disclosure of personal data of the petitioner occurred on the part of the operator to the violation of the principle of integrity and confidentiality in accordance with Art. 5 par. 1 letter f) Regulations. Considering to the fact that, as part of the procedure, it was found that the operator additionally introduced the obligation to send electronic mail in encrypted form, the office did not impose corrective measures on the operator. However, the office imposed a fine on the operator for the given violation.

10.3.2.6 Evaluation and profiling of personality aspects related to natural persons employers

In 2021, the office, on its own initiative, conducted proceedings based on a notification of a breach of protection personal data through the form for the operator to report security

46

incidents in the sense of art. 33 of the Regulations and § 40 of Act no. 18/2018 Coll. The subject of the violation of personal data protection was an incident related to the activity of the operator in the matter evaluation and profiling of the personal aspects of the affected persons (employees operator) by a psychological survey, which was to be carried out without adequate legal basis, without securing a contract according to Art. 28 Regulations with and without an intermediary conducting a data protection impact assessment. The investigation revealed that the operator did not have an adequate legal basis for processing the personal data of the persons concerned, as it did not meet the consent to the processing of personal data required by the operator conditions of consent in accordance with Art. 4 par. 11 Regulations. Consent must be freely given, specific, informed and unambiguous expression of the will of the person concerned. Given the dependency that follows from the employer/employee relationship, it is unlikely that the person concerned would she could refuse to give consent for data processing to her employer without feeling

fear or real risk of adverse consequences of refusal (i.e. unlikely to consent was given freely). Consent is not considered freely given even if it is not possible to give separate consent to individual processing operations of personal data despite the fact that it would be appropriate in a particular case. As part of the procedure, it was also found that the operator did not fulfill the information requirements for the persons concerned in connection with the evaluation of their personality aspects

obligation according to Art. 13 Regulations at the latest when obtaining their personal data. Natural persons should be in addition to the identity of the operator, the purposes of processing and other information as well informed about the risks, rules, guarantees and rights in the processing of personal data, as well as how to exercise their rights in such processing. In particular, the specific purposes for which personal data process should be explicitly stated and legitimate and determined at the time of obtaining personal data data. The investigation also revealed a violation of the principle of responsibility, as the operator in the proceedings he did not prove in any way that at the time of the implementation of the psychological survey aimed at evaluating the personality aspects of the persons concerned had the contract concluded with the intermediary according to Art. 28 Regulations not even in connection with profiling of the persons concerned did not demonstrate that an assessment of the impact on the protection of personal data had been carried out. Within

principles of responsibility, the operator is obliged to the office as a supervisory authority (not the other way around) prove that the personal data of the persons concerned is processed in accordance with the Regulation. Regarding with the evaluation of the personality aspects of the persons concerned by a psychological survey by the operator several times to violate the principle of legality, justice and transparency in the sense of Art. 5 par. 1 letter a) Regulations, to violate the principle of responsibility according to Art. 5 par. 2 of the Regulation, as well as to the violation of some obligations established by the Regulation. Due to the fact that during the procedure it was found that the operator is processing personal data of the persons concerned in connection with the evaluation of their personality aspects ended and further with the following data

does not have, the office did not impose corrective measures on the operator. However, the office to the operator imposed a fine for the given violation.

47

11 REMEDIES AND DECISION ON THEM

Regarding the decision of the office in the matter of personal data protection proceedings, as well as the decision on the non-accessibility of information or a decision on non-disclosure of information can be filed in part proper remedy - dissolution, while the provisions on remedies are applied subsidiarily means established in the administrative order. The chairwoman decides on the submitted breakdowns of the office, after her appeal, the vice-president of the office decides on them based on the recommendations of the board of directors commission, while the submitter of the breakdown can expand or supplement it with another proposal or others points only in the period designated for submission of the breakdown, i.e. a period of 15 days from the date of notification of the decision.

During the monitored period, 64 reports were submitted to the vice president of the office for decision.

In the monitored period, it decided in 41 cases as an appeals body. In the monitored period 11 more decisions on dissolution were issued, when the dissolution was presented to the vice president of the office for a decision in 2020. Two reviews were carried out within the monitored period decisions outside the appeal procedure. Together in the monitored period it was the appeals body issued 52 decisions.

The vice president of the office confirmed the decision of the administrative body of the office in 32 of them.

In 13 cases, the matter was returned to the administrative body of the office for a new decision on the matter.

In the remaining 7 cases, the decision of the administrative body of the office was changed.

In 9 cases, the subject of the decision on dissolution was the decision not to make information available/ non-disclosure of information in part in accordance with Act no. 211/2000 Coll.; in all cases se confirmed the decision.

A participant in an administrative proceeding may appeal against the valid decision of the head of the office and from

29.04.2020, after her appeal, against the valid decision of the vice-president of the office, submit a lawsuit for review of the legality of the decision, within two months of its notification.

Within the framework of substantive and local jurisdiction, the Regional Court in Bratislava is responsible for proceedings.

In the monitored period, 9 lawsuits were submitted to the Regional Court in Bratislava for review

the legality of the office's decisions, the office commented on all of them upon request (file no.: 5S/228/2021,

2S/225/2020, 2S/121/2021, 1S/216/2021, 2S/288/2020, 1S/214/2020, 6S/37/2021, 2S/93/2021,

5S/71/2021). In the monitored period, two judgments were issued in the matter of legality review

decision of the office, one issued by the Regional Court in Bratislava (registered stamp: 2S/198/2018) and one by the Supreme court of the Slovak Republic (8Asan/30/2020).

The Regional Court in Bratislava decides on the matter of the administrative action with a judgment against which they can

participants in administrative court proceedings to file a cassation complaint. The Supreme Court of the Slovak Republic,

as a court of cassation, on the basis of a filed cassation complaint, it reviews the judgment as well as the proceedings

of the regional court that issued it. For the monitored period, the Office in the matter of legality review

he did not file a cassation complaint with the decision-making authority.

48

12 COMPLAINTS UNDER THE COMPLAINTS ACT

As a public administration body, the Personal Data Protection Office also fulfills its obligations

resulting from Act no. 9/2010 Z. z. on complaints as amended (hereinafter referred to as

"Law No. 9/2010 Coll.).

During the observed period, the office received 82 submissions from only one and the same natural person, who

assessed according to Act no. 9/2010 Z. z. In 11 cases, the complaints were evaluated as

unfounded, in 1 case the complaint was evaluated as justified. In other cases

if the submissions did not meet the formal or content requirements of the complaint, they were postponed according to

§ 6 of Act no. 9/2010 Coll., or if the submissions were not evaluated as complaints, they were dealt with

according to § 4 of Act no. 9/2010 Z. z. Among other things, this person submitted 18 applications to the office

for disclosure

information in accordance with the law

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

(Act on Freedom of Information) as amended and 1 complaint about non-handling of the objection

bias.

Subsequently, in the monitored period, the department of administrative proceedings of the office led 3 proceedings on protection

personal data based on the submission of the aforementioned natural person. Department of Administration

the proceedings of the office dealt with 5 submissions from the mentioned person, which were delivered electronically by mail (e-mail), within which this person requested to make available information regarding

processing of her personal data, she subsequently requested scans of the proceedings on the protection of personal data, in which he is a party to the proceedings.

the information she requested

open

49

13 EUROPEAN AND INTERNATIONAL

LEGISLATIVE

PACKAGE

PROTECTION OF PERSONAL DATA

13.1 Legislative process at EU level

On January 10, 2017, the EC submitted a draft regulation on respect for private life and protection

personal data in electronic communications and on the repeal of Directive 2002/58/EC (Directive

on privacy and electronic communications) (hereinafter: "Draft e-privacy regulation) with the aim

ensure compliance with a uniform approach to personal data protection across the EU. Draft regulation

e-privacy will be in relation to the lex specialis Regulation. For this reason, the office is a co-manager

in the legislative process of adopting the draft e-privacy regulation at the European level. The goal

the proposal of the e-privacy regulation is to ensure strict privacy protection rules for users

electronic communication services and equal conditions for all market participants.

Data of electronic communications means their content, such as content of private messages but also metadata, which includes e.g. numbers called, websites visited, geographic location, call or message time data.

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

Negotiations of representatives of individual states in the Council of the EU took place at the same time, but neither it did not adopt a joint agreement on the text in the monitored period. Portuguese Presidency in February 2021 received a mandate to start negotiations with the European Parliament. Slovenian Presidency The EU Council continued its trilogues on the draft regulation.

On July 14, 2021, Regulation (EU) 2021/1232 of the European Parliament and of the Council was adopted 14 July 2021 on a temporary exemption from certain provisions of Directive 2002/58/EC as regards o the use of technologies by providers of independent interpersonal communication services from numbering to processing personal and other data for the purpose of combating online sex child abuse, which applies until August 3, 2024. The reason for the proposed regulation was the entry into force of the European Electronic Communications Code, which among other things introduces a new definition of electronic communication services, which also includes providers services without a number (applies from December 21, 2020). This day will be the provisions of e-privacy directives also apply to independent providers of interpersonal communication services from numbering, making it difficult/impossible for them to continue using technology for purposes fight against online child sexual abuse. This Regulation provides for a temporary exemption from article 5 par. 1 and article 6 par. 1 of Directive 2002/58/EC, which protect the confidentiality of communications and operational data. The processing of personal data is subject to the Regulation and its monitoring is carried out by the supervisory authority also designated by this regulation.

On March 4, 2021, a second corrigendum was published in Eurlex (Official Journal of the European Union) to the Slovak version of the General Regulation on Data Protection. The wording of Article 42 was corrected para. 2, last sentence.

On June 4, 2021, the European Commission adopted standard contractual clauses between operators and intermediaries according to Art. 28 par. 7 of the General Data Protection Regulation. Regarding with the relationship between the operator (or operators) and the intermediary (or intermediaries) when processing personal data, Article 28 of the Regulation includes a file provisions relating to the conclusion of a special contract between the participating contracting parties and mandatory provisions that should be included in the contract. Operator and intermediary they can also choose to use these standard contractual clauses to fulfill these provisions adopted by the European Commission. Standard contractual clauses alone do not ensure compliance obligations regarding international transfers in accordance with Chapter V of the Regulation.

50

The European Commission also adopted several implementing decisions in connection with the transfer of personal data data to third countries, which are described in more detail in chapter 6.2 Transfer of personal data.

13.2 European Data Protection Board

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

The EDPB is represented by its chairperson, who is the chairwoman of the Austrian supervisory authority, Andrea Jelinek. The EDPB consists of the head of one supervisory authority of each member of the EEA state and the EDPS. The EC has the right to participate in the activities and meetings of the EDPB without voting rights.

The EDPB works in accordance with the rules of procedure, which were not changed during the evaluated period.

The activity of the EDPB is divided between 11 expert subgroups and 3 working groups groups (task forces) that are divided thematically. For example technology expert group, fines, cooperation, and others. These expert subgroups work on documents that contributes to the consistent application of the Regulation. After the establishment of TikTok in the EU and the identification of its principal place of business in Ireland for pending cases relating to the application

TikTok The EDPB decided to dissolve its TikTok working group during the reporting period.

In the evaluated period, a cookie banner taskforce was established to coordinate responses to complaints regarding cookie banners filed with several supervisory authorities by the company NOYB. The office participates in the work of 10 expert subgroups and all working groups personal participation, sending written comments, active participation on video and tele conferences, possible related workshops.

The documents on which the expert subgroups work are approved at the EDPB plenary session.

In the evaluated period, 1 personal plenary session was held in Brussels and 15 online plenary sessions session. The office did not participate in the evaluated period due to the then valid pandemic measures 1 of the personal plenary session held in Brussels.

The EDPB's greatest contribution to the public is the issuing of guidelines and recommendations on various areas of personal data protection. In the evaluated period, the EDPB issued 14 guidelines and recommendations, 9 after public consultation and 6 for public consultation. The EDPB issued in the evaluated period and several documents focused on the processing of personal data in connection with digital EU ID card, virtual voice assistants, additional measures when transferring personal data to third countries, to the concepts of operator and intermediary and other. Guidelines and recommendations are published on the EDPB website. Office on its own also publishes these guidelines and recommendations in Slovak and English on the website language. During the period under review, the EDPB organized an online event for interested parties at topic "GDPR application for the processing of personal data for the purposes of scientific research".

EDPB receives according to Art. 71 of the Regulations own annual report.

13.3 Extensive information systems and bodies, offices and agencies of the Union

The EU has created several European large-scale information systems and agencies whose supervision it is shared between national data protection authorities and the EDPS. EDPS and national supervisory authorities the authorities within their respective powers actively cooperate in their tasks with the goal to ensure effective supervision of large-scale information systems and authorities

and Union agencies.

51

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

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

National supervisory authorities and the EDPS cooperate in order to ensure coordinated supervision. On the for this purpose, representatives of national data protection authorities and the EDPS meet regularly - usually twice a year to discuss common supervisory issues.

Within their respective powers and tasks, they exchange as necessary relevant information, assist in conducting audits and inspections, investigate related difficulties with the interpretation or application of Union acts in the field of personal data protection, they study problems connected with the exercise of independent supervision or with the exercise of the rights of the persons concerned, they elaborate harmonized proposals for solutions to any problems and promote awareness of the rights to data protection.

These are specifically the following groups:

- ☐ Council for cooperation over Europol,
- ☐ Joint Supervisory Body for the Customs Information System,
- ☐ SCG working group for coordinating the supervision of Schengen information system II,
- ☐ Working group for the coordination of the supervision of the Visa Information System,
- ☐ Working group for the coordination of supervision over the Eurodac system

□ Committee for coordinated supervision (it includes the IMI system - information system

internal market, EPPO - European Public Prosecutor and Eurojust - EU Agency for Justice cooperation in criminal matters).

from the assessment

of 2021. Report

Each group had two online meetings in the evaluated period. A representative of the office attended meeting of all the above groups.

13.4 Schengen assessment

In October 2019, the Schengen evaluation of the Slovak Republic in the field of protection took place personal data. The processing of the results of the 2019 Schengen evaluation of the Slovak Republic has been completed at the beginning

this link:

<https://data.consilium.europa.eu/doc/document/ST-5534-2021-INIT/en/pdf>.

Conclusions and recommendations contained in the Schengen evaluation report, especially the increase financial and personnel resources of the office for the proper provision of its operation and effective implementation of his tasks, still remain current and waiting to be fulfilled as well as recommendations to ensuring the institutional and financial independence of the office.

13.5 Consultative Committee on Convention 108

The Consultative Committee established by the Council of Europe for Convention 108 consists 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 the interpretation of the provisions and for improvement implementation of Convention 108 and for the compilation of reports, guidelines and guiding principles

is available at

in different areas. Representatives also regularly attend the meetings of the consultative committee

office, whether at plenary sessions or smaller committee meetings. It was held in 2021

5 online meetings. The office attended all of them.

In the evaluated period, the Consultative Committee on Convention 108 issued documents as recommendations, which are aimed at the protection of personal data in the context of facial recognition, the right to personal data protection in the context of political campaigns and various opinions on current topics such as, for example, the second additional protocol to the Budapest Convention or to the recommendation of the Parliamentary Assembly to artificial intelligence in the field of provision health care.

Slovakia has already been invited several times to sign and ratify Protocol no. 223 modernizing Convention 108, both by the Council of Europe and the EU.

In the watched

to the interdepartmental

of the comment procedure, material LP/2021/697 Proposal for the ratification of the Protocol, by which it is amended and supplements the Convention on the Protection of Individuals in the Automated Processing of Personal Data.

The process was not completed in 2021.

period Ministry

justice

submitted

53

14 MEETINGS WITH PARTNER SUPERVISORY AUTHORITIES,

CONFERENCES AND WORKSHOPS

14.1 Challenges of international data transfer from the perspective of the Convention 108+ and GDPR

In January 2021, the representative of the office participated in the above-mentioned conference, which was held online.

The conference was held under the auspices of the Federal Ministry of the Interior, Building and

Community and the Conference of the Independent Data Protection Authorities of the Federation and the Federal States of Germany. The conference was mainly focused on the field of international transmissions in the light of the decision of the Court of Justice of the EU in case C-311/18 – Facebook Ireland and Schrems. The aim was to examine the challenges of international data transfer from the point of view of the Regulation and Convention 108+. Prof. was one of the speakers. Dr. Dr. h. c. Thomas von Danwitz, Judge of the Court of Justice of the EU, which participated in the creation of the decision in case C-311/18.

14.2 PL&B 34th Annual International Conference

A representative of the office participated in the PL&B 34th Annual International Conference, which took place online in July. The conference discussed interesting topics such as the interaction of the right to protection personal data and competition law, the UK's position on transfers of personal data in the current situation and there was also a statement from the representative of the Commission on transmissions according to the Regulation.

It was the last mentioned speaker who commented on the current state of transmission according to Chapter V of the Regulation and at least partially clarified the position of the Commission on the given issue.

14.3 Qubit Conference Prague 2021

In September, a representative of the office took part in an international conference in Prague, which dealt with the issue of cyber security. The topics were current trends in cybernetics security as existing threats and everyday attacks in the digital space. They were presented methods of defense as well as the current state of readiness of the organization to defend against these threats. Leading experts in the field of cyber security presented practical cases from practice such as products and methods to minimize such risks. Linking cyber threats it is also closely related to the issue of personal data protection. Identification of knowledge acquired on it will help the conference to work on and improve the existing procedures of the office for analyses and data protection as well as to help find the most suitable solution in cases where citizens request consultation support from the office.

14.4 Privacy Conference 2021

In September, a representative of the office participated in a two-day online conference called Privacy Conference 2021 organized by the company "bitkom". The central theme of the conference was international transfers of personal data. Specifically, the contributions focused on the new standard contractual clauses for the transfer of personal data issued by the Commission and assessment of the impact of the transfer (Transfer Impact Assessment). Other topics were the upcoming EU regulations - the act on administration data (Data Governance Act) and the data act (Data Act). The conference also had several contributions aimed at technical security of data, for example as pseudonymization and encryption.

14.5 GDPR Conference 2021

In October 2021, a representative of the office personally participated in the GDPR 2021 Conference in Prague.

54

The conference was organized by the Association for the Protection of Personal Data in cooperation with the Business Union lawyers and Microsoft. Several experts from not only the Czech Republic spoke at the conference Republic, but I am from Slovakia, Germany and Liechtenstein. The conference covered a wide spectrum topics and was divided into blocks and workshops. The workshops were focused on the transfer of personal data, GDPR in practice for municipalities and cities, privacy protection and new technologies, processing personal data in pharmaceutical research and the correct setting of the cookie bar. Representative office participated as a guest in a panel discussion on transfers of personal data outside the EU/EEA in English, where she also had an introductory presentation on this topic.

14.6 Global Privacy Assembly Conference 2021

A representative of the office participated in the Global Privacy Assembly Conference 2021 event in October.

The office is a member of this unique global platform. The conference was held in October 2021 via online form. The topics of the conference were wide-ranging: technological development and personal protection data protection, personal data protection in connection with the coronavirus pandemic: issuance of certificates, ethical approach to privacy protection or regional cooperation of supervisory authorities. They were an enrichment

interesting lecturers, either from the academic environment, from supervisory bodies or members executive power of different states. The opportunity to ask questions of experts was also a big plus on individual topics, which brought an interesting discussion between the participants.

14.7 Privacy in video games: the darkest of patterns

In November, a representative of the office participated in an online seminar entitled: "Privacy in video games: the darkest of patterns" organized by the University of Oslo. Various were presented at the seminar scenarios of how the position of entities involved in the business model of video games should be viewed. Also, how complicated it is to exercise rights under the Regulation and the ambiguity of information obligations of providers of online video games, from which it is not possible to determine what personal data is used while playing they collect and to whom they are provided. This is an area of personal data protection that deserves a future special attention and has a significant impact on future generations and their development.

14.8 GDPR and the Personal Data Protection Act 2021

In November 2021, representatives of the office participated in the IV. year of the EPI conference, which was organized under the auspices of the office. The conference took place in Bela, but it was also possible to participate in an online form so that as many interested parties as possible can participate. The conference lasted two days and a speech was delivered on behalf of the vice-president of the office.

The program of the first day was focused on the new law on electronic communications that came into force effective in February 2022. Contributions were mainly focused on direct marketing and cookies from the point of view of the new law on electronic communications and GDPR. The representative of the office had contribution entitled GDPR and consent to cookies and at the end of the day she participated together with the others speakers of the panel discussion. The second day of the conference was focused on social networks and protection personal data. The contributions focused mainly on the review and analysis of the jurisprudence of the Court of Justice EU in this area. The representative of the office gave a final lecture on the topic of Transfer of personal data to third countries and participated with some speakers in a panel discussion.

The conference was also attended by representatives of other state bodies - the Ministry of Transport of the Slovak Republic and the Office for the Regulation of Electronic Communications and Postal Services of the Slovak Republic, lawyers and experts at

personal data protection from practice, not only from Slovakia, but also from the Czech Republic. All in all, there were states experts on the topic of the conference and interpretations of the new law on electronic communications, were application problems were presented and an interesting discussion took place. We consider the conference to be beneficial, as it provided the basis for developing the discussion of this current topic.

56

15 ASSESSMENT OF THE STATUS OF PERSONAL DATA PROTECTION

IN THE MONITORED PERIOD

Citizens undoubtedly always ranked their health high on their list of values, but in 2021, when the pandemic continued, they perceived it more sensitively and cared for it more than before by that, we all realized its value and fragility.

Nowadays, when personal data is no stranger to anyone, they also require a lot of attention in the health sector, while the need for their protection was inevitable. Therefore, it can be concluded that The pandemic drew attention and also raised citizens' awareness of the topic of personal data in general, as well as health data, which represent a special, sensitive category.

In 2021, the processing of personal data reached a different dimension, as the influence still persisted pandemic, and thus the transition of work and private life to the online more and more often occurred environment. Citizens have realized that the changes associated with their "online life" represent a big one measures of personal data that are the subject of protection but also of interest. In connection with the overall situation there was a need to pay more attention to protection and information about personal protection data in the online environment. In addition to being the subject of trading and interest, personal data are also confronted with information security.

The year 2021 can also be marked as the year when personal data also became the subject of interest for hackers, who didn't just want to draw attention to the imperfection of the system, but who wanted them at the same time

to appropriate for one's own interests. It is all the more necessary to ensure the protection of assets, including personal assets data in the private sector as well as in the public sector.

It remains only to believe that the year 2022 will be successful for the office also from the point of view of the election of the chairman of the office, as

there are enough people in the Slovak Republic who are not indifferent to the protection of personal data and who want to change, improve or streamline the functioning of the office they represent in this regard an institution focused on the protection of personal data of natural persons, while its employees perceive work not only as an obligation, but also as a mission.