print 1127

PERSONAL DATA PROTECTION STATUS REPORT

FOR THE PERIOD 1 JANUARY 2017 TO 24 MAY 2018

Office for Personal Data Protection of the Slovak Republic

September, 2018

Office for Personal Data Protection of the Slovak Republic

Hraničná 12

820 07 Bratislava 27

http://www.dataprotection.gov.sk

Electronic version of the report available at

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

IČO: 36064220

Steuernummer: 2021685985

REPORT ON THE STATUS OF PERSONAL DATA PROTECTION PERIOD

1 JANUARY 2017 TO MAY 24, 2018

The Office for Personal Data Protection of the Slovak Republic in accordance with the provisions of § 81 par. 2 letter k) of Act no. 18/2018 Coll. on the protection of personal data and on the amendment of certain of the Act submits a Report on the Status of Personal Protection to the National Council of the Slovak Republic data for the period from 1 January 2017 to 24 May 2018.

"On the basis of the above provision, I am submitting the Report on the Status of Personal Protection data for the period from 1 January 2017 to 24 May 2018, which will be discussed in the National Council Of the Slovak Republic in accordance with Act no. 18/2018 Coll. on the protection of personal data and on change amendments to certain laws published on the Office's website. ".

Soňa Pőtheová

President of the Office

LIST OF ABBREVIATIONS USED IN THE TEXT OF THE STATUS REPORT

PROTECTION OF PERSONAL DATA FOR THE PERIOD 1 JANUARY 2017 TO

24. MAY 2018

office

Office for Personal Data Protection of the Slovak Republic

NR SR

National Council of the Slovak Republic

a message

Report on the state of personal data protection for the period from 1 January 2017 to 24 May 2018

the law

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

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

IS

Information System

ISOU

personal data information system

CIS

Customs Information System

Directive 95/46

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

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

Regulation

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

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

Directive 95/46 / EC (General Data Protection Regulation) is repealed (Text with EEA relevance)

EEA)

Directive 2016/680

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

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

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

sanctions and on the free movement of such data and repealing the Council Framework Decision

2008/977 / JHA

bill or law no. 18/2018 Coll.

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

MPK

Interdepartmental comment procedure

Portal

Legislation Portal Slov - Lex

5

e-privacy directive

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

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

(Directive on privacy and electronic communications)

proposal for an e-privacy regulation

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

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

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

Convention 108

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

personal data

Regulation 45/2001

Regulation (EC) No 1/2003 of the European Parliament and of the Council 45/2001 of 18 December 2000 on protection

individuals with regard to the processing of personal data by the Community institutions and bodies

and on the free movement of such data

decision no. 1247/2002 / EC

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

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

the Data Protection Supervisor

Act no. 211/2000 Coll.

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

certain laws (Freedom of Information Act)

supervisory officer

European Data Protection Supervisor

EU

European Union

EK

European Commission

EEA

European Economic Area

WP29

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

Committee 31

The Committee established under Art. 31 of Directive 95/46

Europol

European Police Office

CONTENTS

1. INTRODUCTION

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

At a time of massive electronic and data sharing, including personal, privacy is being protected

and thus the protection of personal data reaches the imaginary top of the ranking of basic human

rights and freedoms, which, guaranteed by the Constitution of the Slovak Republic, are one of the pillars democratic society. Pursuant to the provisions of § 81 par. 2 letter k) of Act no. 18/2018 Coll. the Office of the National Council of the Slovak Republic submits this report.

The report is a summary of the Office's activities for the period under review, and is the most appropriate means of informing the public, both lay and professional, about the Office's activities, its findings, and on developments in personal data protection during the period under review.

1.2 Follow-up to the report on the state of personal data protection for 2015 and 2016

The presented report is the eleventh in the history of the independent Slovak Republic and the ninth in the history of the existence of a separate office.

The report follows on from the latest report, in particular in the area of the Office 's legislative activity, as the process of adopting the harmonization bill continued in 2017 and was completed in January 2018 with the publication of Act no. 18/2018 Coll. in the Collection of Laws of the Slovak Republic.

The previous report was delivered to the National Council of the Slovak Republic on 15 August 2017. Committee of the National Council of the Slovak Republic for Human Rights and national minorities discussed the previous report on 5 September 2017; the message was by a vote of the Plenum of the National Council of the Slovak Republic on 11 September 2017.

10

STATUS, PERSONNEL SECURITY AND BUDGET OFFICE

2.1 The position of the Office

The protection of personal data in the Slovak Republic is entrusted by law office. The Office is a state administration body with nationwide competence supervising personal data protection and involved in the protection of fundamental rights and freedoms of individuals persons in the processing of their personal data. In exercising its powers, the Office shall proceed independently and in the performance of its tasks, it is governed by the constitution, constitutional laws, laws, others generally binding legal regulations and international treaties, which is Slovenská

Republic bound.

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

2.2 Staffing of the Office

2.2.1 Public functions of the Office

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

The term of office of the President of the Office shall be five years. Mgr. Soňa Pőtheová, who was elected to this position by the National Council of the Slovak Republic on 14 May 2015 by a resolution of the National Council of the Slovak Republic no. 1736/2015.

In the absence of the President, the Office shall be represented by the Vice-President, who shall be appointed and removed the Government of the Slovak Republic on the proposal of the President of the Office. The term of office of the President of the Office shall be five years. JUDr. Anna Vittek, who was with efficiency from 2 January 2016 to this position appointed by the Government of the Slovak Republic by resolution no. 658/2018 of 2 December 2015.

Until May 24, 2018, the inspectors were headed by the Office's Chief Inspector, whom she appointed and recalled by the Government of the Slovak Republic on the proposal of the President of the Office for a term of five years. Until May 24, 2018, Mgr. Tatiana Valentova, who was appointed to this position by the Resolution of the Government of the Slovak Republic no. 539/2012 on October 3, 2012. As of May 24, 2018, the total number of inspectors was three.

2.2.2 Personnel area of the Office 's staff

The employees of the Office perform professional tasks in accordance with the law and other operational activities and obligations under generally binding legislation. It requires their provision

a sufficient number of qualified staff qualified to carry out professional activities at

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

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

in civil service. Selection of employees and filling of vacancies

places is realized according to the conditions stipulated by law for individual state functions

employees.

11

As of 1 January 2017, the Office had 39 posts, of which 38 were employees

in a civil service relationship and one employee performing work in public

interests.

As of 1 January 2018, the Office had 42 seats, of which 41 were employees

in a civil service relationship and one employee performing work in public

interests.

As of May 24, 2018, the office had 43 seats, of which 42 were employees

in a civil service relationship and one employee performing work in public

interests.

The average age of employees in 2017 was 40 years, while the average age for men was 36

years and 40 years for women. The average age of employees in 2018, until May 24, 2018, was 41

years, with an average age of 43 years for men and 40 years for women.

The Office places great emphasis on the training of employees and enables them to constantly deepen themselves

professional qualifications. In 2017, 94.8% of employees had a university degree, of which

higher education II. degree 94.8% and higher education III. degree 2%. In year

2018, until May 24, 2018, 95.1% of employees had a university degree, of which

higher education II. degree 95.1% and higher education III. degree 2%.

Overview of the number of employees of the Office

Actual staffing of the Office

Year

2017

2018

to 24.5.2018

Civil service

ratio

38

Performance of work in public

interests

1

Together

41

1

42

40

Overview of other personnel data

Year

2017

to 24.5.2018

Employees are

changed

working

ability

3

Employees working at

out-of-work agreement

ratio

Number of women

Number of men

2

1

1

3

3

2

1

An overview of the number of employees of the Office according to their education

College

II. degree

37

College

III. degree

1

Together

2

University I.

degree

0

2

0

39

1

42

Year

High school

2017

to 24.5.2018

12

40

2.3 The Office 's budget

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

For the year 2017, the Office approved a budget of 1,018,835.00 euros, which during the year 2017 edited several times; the budget for 2017 has been increased to a final amount of 1,196,279.00 The Office had EUR 40,000.00 available for current and capital expenditures. Because of non-compliance with the mandatory revenue indicator in 2017 was a budgetary measure for the Office no. 281/2017 tied 23,000 Euros, which was realized within the General chapter treasury administration - organization Všeobecná pokladničná správa.

A budget of EUR 1,163,853.00 was approved for the Office for 2018.

Overview of the Office's budget for 2017 in Euros

Approved budget

for 2017

to 01/01/2017

Adjusted budget

to 31/12/2017

Pumping

to 31/12/2017

Wages, salaries, service income

and OOV (610)

576 263.00

63,816.00

65 3812.77

Wage premiums (620)

204,527.00

2,360 44.00

236,034.74

Goods and services (630)

226 045.00

219,469.00

217,905.93

Current transfers (640)

1,000.00

5,950.00

5,945.31

EKW02 (630) common

expenses

11,000.00

36,000.00

34,920.02

0

45,000.00

44,684.43

Total current expenditure (600)

1,018,835.00

1,196,279.00

119 3303.20

Capital expenditures (700)

0

40,000.00

38,644.39

Pointer

EKW02 capital expenditures

Overview of the Office's budget for 2018 in euros

Approved budget for the year

2018 to 1.1.2018

Pumping

to 24.5.2018

673 121.00

221 440.59

237,498.00

61,308.17

Goods and services (630)

237 234.00

217,905.93

Current transfers (640)

5,000.00

5,945.31

11,000.00

418.95

1,163,853.00

400 184.50

Pointer

Wages, salaries, earnings and OOV

(610)

Wage premiums (620)

EKW02 (630)

Total current expenditure (600)

13

3 LEGISLATIVE PROTECTION OF PERSONAL DATA PROTECTION

3.1 Interdepartmental comment procedures of generally binding legal regulations

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

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

personal data

data of natural persons. The Office partially fulfills its role in the field of processing supervision

personal data also by supervising and commenting on the texts of draft laws and texts

other generally binding legislation governing processing

personal data of natural persons. It formulates its comments on draft legislation

through the Portal within the MPK. The purpose of the Office's comments on the legislative

The proposal is to ensure the quality of legislation regarding the processing of personal data

was high so that the legislation was precise, unambiguous, and so in the relationship

to the controller as well as in relation to the data subject whose personal data will be the subject of

processing.

During the reporting period, the Office submitted a total of 80 comments on 29

legislative proposal; of the comments submitted, 62 were substantial. Among the frequently mentioned

the Office 's comments included those by which the Office requested an amendment to the list; or

the extent of the personal data processed in relation to the purpose of the processing, the Office also frequently demanded that the responsibilities for processing be clarified in the legislation to the information system or register, for reasons of legal certainty as to the position the controller and thus his responsibility for the processing and protection of personal data.

In relation to the comment proceedings from previous periods, it can be stated that that the work of the Office makes sense in this area, as the number of the number of key comments is reduced and the number of key comments also decreases, which indicates a positive development in terms of the processing of personal data national legislation. Law enforcement pay more attention to the provisions processing of personal data, this positive trend the Office observed especially with the upcoming the date of application of the Regulation in practice, which was 25 May 2018.

3.2 European legislative package on personal data protection

In the last report, the Office briefly stated that it had been adopted at European level the so-called "European data protection package", which includes three legal acts: Regulation, Directive 2016/680 and Directive (EU) No 182/2011 of the European Parliament and of the Council 2016/681 of 27 April 2017 on the use of Passenger Name Record (PNR) data and records for prevention purposes, detection, investigation and prosecution of terrorist offenses and serious crime.

From this package, the activities of the Office and its scope were directly affected by the Regulation and the Directive 2016/680. As the Office is not a central body of state administration, it is the body responsible for harmonization and transposition law no. 18/2018 Coll. became the Slovak Ministry of Justice of the Republic and co-manager of the Ministry of the Interior of the Slovak Republic; the office was in the legislative process of the prepared bill by its submitter.

3.3 Legislative process of the bill

The first works within the legislative process on the bill were started in July 2016 with the establishment internal working group to ensure the fulfillment of the Office's tasks in aligning the Regulation

with the legal order of the Slovak Republic. The purpose of the internal working group was detailed
study of the Regulation in order to determine the final content of the draft law
and also to determine whether the draft law will follow the amendment of the law or not
prepare a new law on personal data protection. Based on the internal negotiations of individual
departments of the Office and also on the basis of guidelines on the scope of the Regulation from the Office of the Government
Of the Slovak Republic and also on the basis of the fact that the law was supposed to be in addition to the harmonization law
of the Act with the Regulation, as well as the Transposition Act for Directive 2016/680 was adopted
decision that a new bill will be prepared in the legislative process, that is, that
the law will not amend.
Subsequently, an external inter-ministerial working group was set up to prepare a bill,
the establishment of which the Office initiated with the intention of harmonizing the legal order with the Regulation
at the same time across all laws that may be affected by the regulation. With this
The invitation was sent in October 2016 to all central state bodies
reports to comment by January 2017 on whether the legislation they have in
have identified the provisions that need to be amended following the Regulation
and thus to be listed as amending articles in the draft law within its legislative process.
The results of the meeting of the members of the external working group led to the fact that of all
most of the institutions contacted stated that legislation was not needed under their responsibility
with the Regulation to amend, or that the amendment will be carried out separately within the already
approved plan of legislative tasks for 2017. Entities that were interested in amending
legislation within the time limit set by the Office, the text of their amending articles
subsequently incorporated into the bill.
According to § 9 of Act no. 400/2015 Coll. on the creation of legal regulations and on the Collection of Laws
Of the Slovak Republic and on the amendment of certain laws was on the Portal on 10 January
Preliminary information published, PI / 2017/3, on the draft law, when
the opportunity to comment ended on January 30, 2017.

After the completion of the preparatory work on the bill, the bill was together with all required
sent to the preliminary comment procedure on 31 May 2017, the so-called PPK,
Permanent Working Committee of the Legislative Council of the Government of the Slovak Republic for assessment
selected impacts in accordance with the Unified Methodology for the Assessment of Selected Impacts. On
On 14 June 2017, the Office withdrew the assent of the Standing Working Committee of the Legislative Council
of the Government of the Slovak Republic to assess selected impacts.
On June 15, 2017, the bill was included in the MPK, when it was commented on
set normal deadline, 15 working days, MPK was terminated on July 6, 2017. Within
According to the Portal, a total of 1,012 comments were submitted to the draft law, of which 201
essential. The Office dealt with the comments on the draft law by the end of August 2017.
Subsequently, the material was discussed on September 12, 2017 as the 4th item in the 37th session
Legislative Council of the Government of the Slovak Republic, on the basis of its comments was a meeting
interrupted on this point with a recommendation to incorporate its comments into the proposed material
and resubmit it to the Legislative Council of the Government of the Slovak Republic.
Based on this recommendation, the Office finalized the bill and it was re-submitted
negotiations at the 38th session of the Legislative Council of the Government of the Slovak Republic on 19 September
2017.
15
The Legislative Council of the Government of the Slovak Republic drafted the bill at its 38th session
discussed and recommended that the proposal be amended in the light of its observations and that its amended version be
amended accordingly
its recommendation to submit to the Government of the Slovak Republic.
The bill was also the subject of negotiations of the Slovak Economic and Social Council
Republic, was specifically discussed at its plenary session on 18 September 2017 as
second point in order. During the plenary session, the Republican Union applied
employers a fundamental comment on § 15 par. 1 of the bill (consent to processing

personal data of a child with information society services, Republican Union
employers proposed lowering the age of children to consent to services
information society with the proposed 16 to the age of 13, subsequently a compromise proposed
reduction to the age limit of 14 years), as the Republican Union
employers, nor did it identify with its compromise text by the other members of the board
and the Republican Employers' Union did not back down from its comment, the council did not succeed
to the agreement due to the disagreement of the Republican Employers' Union; however, he did not have this disagreement
resulting in the suspension of the legislative process of the bill.
Subsequently, on 19 September 2017, the material of the draft law was amended on the basis of a recommendation
Legislative Council of the Government of the Slovak Republic delivered to the meeting of the Government of the Slovak
Republic
of the Republic. The Government of the Slovak Republic discussed the bill on September 20, 2017
at its 70th meeting; Resolution of the Government of the Slovak Republic no. 441/2017, the government approved
government bill and instructed the Prime Minister to submit the bill to the President of the National Council of the Slovak
Republic
for further constitutional discussion. The government entrusted the Deputy Prime Minister and Minister with a resolution
Justice Lucie Žitňanská to introduce the government bill in the National Council of the Slovak Republic and the President of the
Office
Soňa Pőtheová to justify the bill in the committees of the National Council of the Slovak Republic.
The National Council of the Slovak Republic was delivered the bill on September 22, 2017 and was assigned a number
704. The Chairman of the National Council of the Slovak Republic nominated the National Council of the Slovak Republic for
Human Rights as the responsible committee
and national minorities with a deadline of 27 November 2017 and as committees that
have a bill to discuss proposed by the Committee of the National Council of the Slovak Republic for Human Rights and
National Minorities
and the Constitutional Law Committee of the National Council of the Slovak Republic with a deadline for discussion by 24

November 2017. In the first

reading, the bill was discussed at the 21st meeting of the National Council of the Slovak Republic; by the resolution of the National Council of the Slovak Republic of 12 October

2017 no. 872 assigned the government bill to the Constitutional Law Committee of the National Council of the Slovak Republic and the National Committee

Council of the Slovak Republic for Human Rights and National Minorities. It also appointed the NR Committee

SR for Human Rights and National Minorities as the responsible committee and deadlines for discussion

the bill in question. Deputies of the National Council of the Slovak Republic who are not members of the committees to which the bill was granted, they did not notify the committee responsible within the set deadline

to the bill in question.

The draft committees designated by the committees discussed as follows: The Constitutional Law Committee of the National Council of the Slovak Republic drafted

discussed on 14 November 2017 and did not adopt a resolution as the draft resolution was not approved

of the majority of the present deputies according to § 52 par. 4 of the Rules of Procedure.

The Committee of the National Council of the Slovak Republic for Human Rights and National Minorities discussed the proposal on 23 November 2017

and resolution no. 68, the National Council of the Slovak Republic recommended approving the bill with comments. In the second reading

the bill was discussed at the 23rd meeting of the National Council of the Slovak Republic on 29 November 2017 and proceeded to III. reading.

The bill was discussed at the 23rd meeting of the National Council of the Slovak Republic, Resolution No. 930 of 29 November 2017

with the result that the bill is forwarded to the editorial board of the Collection of Laws of the Slovak Republic.

The approved bill was sent to the Collection of Laws of Slovakia on 19 December 2017

of the Republic. The approved bill was published in the Collection of Laws of the Slovak Republic

on January 30, 2018, under number 18/2018. Act no. 18/2018 Coll. entered into force on 25.

May 2018.

3.4 Legislative process of the Office 's draft decree on the impact assessment procedure for

personal data protection

Act no. 18/2018 Coll. is a legal norm that harmonizes the legal order

with the Regulation and transposes Directive 2016/680. In order to achieve full harmonization,

necessary for the Office to issue an implementing regulation pursuant to Section 42 of Act no. 18/2018 Coll. in context

of the empowering provision of § 108 par. 2 of Act no. 18/2018 Coll.

With the submitted draft decree, the Office proceeded in accordance with § 108 par. 2 of Act no. 18/2018 Z.

from. and laid down in a decree the details of the processing impact assessment procedure

personal data. The purpose of the impact assessment is to assess the processing operation

the nature, extent, context and purpose of the processing

personal data, where such processing may lead to a high risk for natural rights

persons. The obligation for the operator to carry out an impact assessment follows directly from the law

no. 18/2018 Coll. and for the operator is an obligation especially if he plans to carry out

processing operations according to § 42 par. 3 letter a) to c) of Act no. 18/2018 Coll. Contents

impact assessment is partially defined in Act no. 18/2018 Coll., Specifically in the provision

§ 42 par. 4. The details of the impact assessment, in particular as regards the description of the intended processing,

assessment of necessity and proportionality in conjunction with measures to demonstrate compliance,

risk assessment for the rights of individuals in connection with risk management measures,

documentation and monitoring and review should be established and adjusted in more detail

Decree of the Office on the procedure for personal data protection impact assessment.

The legislative process of the decree was started by the internal activities of the office, the creation of an internal working one

the group that drafted the text of the decree, which was then made available to the selected

experts from the professional community who were to comment on the draft decree, and so on

contributed to its clarification and final wording. At the end of this process, which preceded

On the creation of the final text of the draft decree, the Office held a meeting on 9 January 2018
the ground of the Office, where the text of the decree for final comment was provided to the selected
representative of the professional community. The text of the proposal was based not only on their observations and
suggestions
of the Decree was finalized and Preliminary Information PI / 2018/46 was published on the Portal, namely
within the deadline for its comments from 27 February 2018 to 9 March 2018. Subsequently, on 4 April
In 2018, the Office submitted to the Standing Working Committee for the assessment of selected preliminary effects
comment procedure material of the draft decree. On April 10, 2018, the Office received approval
the opinion of the commission, in which the commission did not comment on the material either
recommendations. On 13 April 2018, the Office published information on the launch of the MPK on the Portal,
LP / 2018/222, lasting from 13 April 2018 to 23 April 2018.
As part of the inter-ministerial comment procedure, the comment subjects applied
A total of 137 comments on the draft decree, 19 of which were fundamental. After the settlement
with comments on the draft decree, the text of the draft was sent to the Standing Working Group for consideration
Commission of the Legislative Council of the Government of the Slovak Republic for technical legal regulations.
The meeting of the Standing Working Committee on the draft decree took place on 28 May 2018, when
at its 59th meeting, the commission discussed the draft decree and adopted conclusions on the text of the draft
and recommendations when, after their incorporation, the commission recommended publishing the decree in the Collection
laws of the Slovak Republic. After incorporating the comments of the Standing Working Committee, the text
Decree sent for publication in the Collection of Laws of the Slovak Republic. Decree of the Office

on the protection of personal data of the Slovak Republic on the procedure for impact assessment on
protection of personal data was published in the Collection of Laws of the Slovak Republic under
No. 158/2018 Coll.

3.5 Methodological guidelines of the Office

According to § 64 par. 1 letter m) of the Act is the guidance of operators and intermediaries

one of the tasks performed by the Office in supervising the protection of personal data. Proven
in the form of guidance of operators and intermediaries, based on the practice of the Office
The Office's methodological guidelines, which are published on the Office's website, are available to all
operators and intermediaries and the general public. Office with their publication
and by publishing he had and still has very good experience, as he can cover through them
current problems of personal data processing.
The year 2017 was held in the spirit of legislative changes and preparations for arrival and implementation
Regulations and Act no. 18/2018 Coll., Therefore the Office did not issue any new methodologies this year,
as operators have been intensely interested in the Regulation since the beginning of 2017
and the changes that will have to be made in the processing and transition to the Regulation. Office everything
focused its activities within the methodology on the preparation of new methodologies and guidelines,
reflecting the arrival of the Regulation. Methodologically, of course, the office further guided
operators, but in the form of answers to their individual questions.
The beginning of 2018 was already in the methodology of the transition to the Regulation
and the methodologies of the Office, the basis of which was to inform, were also focused in this direction
operators
about boarding
changes.
In order to
methodically
guide
The Office created a separate web bookmark for operators in the course of 2017
"Regulation", where operators and intermediaries could find both the text of the Regulation and
basic methodologies for the transition from the law to the Regulation. Among the documents they informed
operators on the transition from the law to the Regulation belonged to the Office's methodology "Major changes
in personal data protection legislation ". A similar document comparing the law

and the Regulation was the document "Comparison Law vs. Regulation ', which tabulated

compared the various provisions of the legal norms.

18

COMMUNICATION OF THE OFFICE WITH THE PUBLIC

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

The issue of personal data protection is not limited to operators or

intermediaries who are obliged to apply personal data protection legislation

in practice, of course, this issue also affects people affected by those who have questions

resulting from everyday life situations related to their personal data. Operators

and intermediaries asked the Office of a professional nature related to their duties

resulting from the Regulation, how its specific provisions are to be applied in practice, or

whether the described and performed processing will fall within the scope of the Regulation or the law at all

no. 18/2018 Coll.

The Office also continued to contact the public through telephone consultations.

The public very much welcomed the possibility of such a consultation, and the Office was in favor

evaluated by callers as one of the few who communicates directly and in writing with the public

and helps address the agenda it has.

In the period under review, the most common issue was the incoming Regulation

and how to apply it in practice, what changes with its onset, and how operators in particular

and intermediaries should set up personal data processing and protection processes so that

they were in tune with him. Also resonating with the bill was the interest in its current state

within the legislative process and also when it will be published in the Collection of Laws of Slovakia

of the Republic.

Especially at the turn of 2017 and 2018, it had a number of questions, both written and

emails significantly rising in nature. Public interest in personality has also increased

consultation on the premises of the Office, to the extent that the Office had to undertake some

requests for personal consultations were rejected on time and staffing grounds as they were not

to be able to physically secure their equipment at the required time.

The Office, Department of Legal Services and International Relations, in 2017 equipped 1818

telephone consultations and in 2018 by 24 May 2018 the staff of the department provided 611

telephone consultations.

As for written and e-mail questions to the public, in 2017 it was equipped

staff of the Legal Services and International Relations Department 788 documents

and e-mail questions and by 24 May 2018 they were processed 348. In general, it is possible

state that also the level and number of questions in one document or e-mail request

increased significantly, on average the inquiring office was addressed via a single e-mail

or a sheet of 3 to 5 questions, but with the approaching date of application of the Regulation sometimes

there were ten or more in one document or e-mail request.

The Office also conducted personal consultations, in 2017 there were a total of 103 of them, until 24 May 2018

40 were made.

4.2 Communication of the Office with the media

Since April 2016, when the text of the Regulation was published in the Official Journal of the European Union

it has also increased media interest in the protection and processing of personal data. Increased interest

Of course, it persisted in 2017 and escalated until the end of the period under review, ie

until 24 May 2018. In view of the advancing time when Regulation and Act no. 18/2018 Coll.

should have begun to exert interest in both print and electronic media initially

to the questions which called for a description of the fundamental changes and differences between the "old" and

"New" legislation. Gradually, the interest became more and more focused and concretized on the concrete

areas in which personal data are processed and how the new legislation will affect

which specific sector.

In 2017, the office answered and responded to 40 questions, a set of questions from the journalistic community.

By 24 May 2018, 31 questions had been addressed and answered by the Office.

However, media interest was no longer focused only on specific issues, but the media, newsrooms,

in some respects directly by the actors and organizers of some of the events involved

personal data processing, organized conferences in which they actively participated as well

office staff. Mention may be made of the conference organized by the weekly Trend on 25 April

2017 devoted to the issue of the Regulation, at which the Office was also represented in the panel discussion

also among presenters.

Over the period under review, media interest has also changed in part with the output from the office

demanded by the media, it was no longer just short questions on current topics, but interest also increased

media on the Office's replies in the form of complete information, which was subsequently published

in one article, sometimes confronted with a private sector expert. In particular

The print media paid wider attention to the area of personal data protection and legislation

they often devoted an extensive article to the change, or even the entire issue, or a substantial part of the issue

one or more issues of the periodical.

The interest of the media also remained focused on specific ad hoc issues that currently resonated

in society, such as how the Regulation and the new legislation will affect them in general

the field of education, especially children and their parents. Fines and theirs were a similarly resonant topic

granting to the authorities, their amount and the resulting fear of Regulation and Act no. 18/2018 Z.

from.

4.3 Privacy Day

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

signed in Strasbourg in 1981. This day was announced by the committee with the support of the EC

Council of Europe Ministers for Personal Data Protection Day.

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

data within the general public. The years 2017 and 2018 were no exception to this plan.

In both years, the Office followed up on the successful format of organizing an open day

doors when it is possible for the public, both lay and professional, to come to the premises of the office and consult experts on the protection and processing of personal data, where appropriate, so that the general public can find out how to proceed in cases which concern the protection of personal data.

20

Both open days, both in 2017 and in 2018, were in the spirit the incoming Regulation. The public interest, which was enormous and was, also corresponded to this almost entirely focused on how to harmonize operators with the forthcoming Regulation, or what all and how will change from May 2018.

In both years, the office was visited by an average of about 50 people. Due to the great interest and number The initial consultation time had to be extended to each applicant he was consulted and his questions were answered. Despite that both days open doors were mentally and physically demanding, the public interest pleased us and also thanks direct contact with the public, the Office could subsequently respond more flexibly to requests the general public and to include in the FAQ section those that have been in the center of attention during open days.

4.4 Office website and its traffic

The Office's website, as an electronic means of presentation, has undergone a strong graphic adjustment on the occasion of the implementation of the Regulation into national legislation. Next expansion of functionalities and subsequent redesign focused on easy availability of required information for state administration and public administration bodies, but also for the general public. On the web The registered office does not lack mandatory disclosure, but has expanded with regard to the Regulation not only the legislative range of published materials, but also the range of questions and answers for public.

The Office's website meets the conditions and technical criteria in accordance with the Ministry's Decree Finance of the Slovak Republic on standards for public administration information systems, reflects on the new

legislation in the field of personal data protection, where the controllers are

and intermediaries are obliged in some cases to designate a responsible person. Operator

and the intermediary is obliged, according to the new legal norm, to notify the Office of the contact details

designated responsible person. As the responsible person acts as a contact point for

the operator and the intermediary are obliged to notify the Office of the identification data

responsible person. For easier reporting of responsible persons, already before May 24

2018 office for this purpose created, as a public service, a new contact form for

administrative burdens and burdens on operators and intermediaries.

The implementation of the Regulation into national legislation was also reflected in the number of visitors to the Office's website,

when the website was searched a total of 507 476 times, most often

through various web browsers.

21

An overview of the websites through which the website is accessed

office

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

TOP 10

The order

URL

Impressions - Count

1

https://www.google.com/

327276

2

https://www.google.com/

75836

3

https://www.bing.com/

12453

4

https://www.google.com/

8412

5

http://m.facebook.com

7082

6

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

2204

7

https://www.google.de/

2131

8

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

1876

9

https://l.facebook.com/

1333

10

https://www.google.at/

1183

Compared to the period from 2013 to 2017, there was a significant increase in traffic to the Office's website, which was caused by the upcoming implementation of the Regulation and Act no. 18/2018 Coll.

practice and preparation for it.

22

5 PERSON RESPONSIBLE

He is responsible for supervising the protection of personal data processed in accordance with the law the controller who processes the personal data. The operator may supervise personal data protection to authorize the responsible person in charge of compliance legal provisions for the processing of personal data.

Only a natural person who has the legal capacity can be a responsible person in full, is of good repute and has a valid certification of the Office on passing the performance test responsible person.

In the monitored period, the Office registered and issued certificates of passing the examination of a natural person to perform the function of the responsible person in accordance with the needs of the operators.

Overview of the number of responsible persons reported to the Office

Resposible people	Period	Count
Total number of reported persons with a valid exam	1.1.2017 to 24.5.2018	637
Total number of credentials of responsible persons	1.1.2017 to 24.5.2018	1634

23

6 APPROVAL ACTIVITY OF THE OFFICE IN THE NOTIFICATION SECTION AND SPECIAL REGISTRATION

6.1 Notification obligation

The law in its sixth chapter of the second part imposes an obligation on operators to ISOU in which process the personal data of the data subjects, taking into account in particular the nature and sensitivity of the data the legal basis for their processing and the establishment of the institute of the responsible person, to notify the Office, request the Office for special registration or keep IS records.

All IS in which personal data are completely processed are subject to the notification obligation or by partially automated means of processing, the law being exhaustive lists which IS are not covered by the notification obligation. For notification of IS to the Office the administrative fee is not collected and it was possible to do so in addition to the written form by means of an electronic form published on the Office's website.

In 2017, a total of 2,467 ISOUs were notified to the Office, of which it was subject obligations of 1 955 information systems. In 2018, the operators of the office announced together 769 IS, of which 648 were subject to the notification obligation. The most common type operators who reported to the IS Office in the period under review were e-shops, pharmacies, real estate and travel agencies. The most frequently reported IS were those in which they were processed personal data for marketing purposes and personal data of clients for the purpose of providing bonuses and discounts in the form of a loyalty program.

An overview of the number of notified IS according to the law

Number of notifications performed via electronic form

The number of IS that actually subject notification obligations

The number of IS that

were not subject

notification

obligations

Year

Number in writing

delivered

IS notification

2017

1303

1164

1955

512

to 24.5. 2018

352

417

648

121

6.2 Special IS registration

The special registration of IS is regulated by the provisions of Sections 37 to 41 of the Act, which are also exhaustive

define the conditions under which the IS is subject to special registration. These are the cases when

the processing of the personal data of the persons concerned is more sensitive in terms of invasions of their privacy

and it is necessary to examine individually the degree of risk of infringement of the rights and freedoms of those concerned

persons. In a special registration procedure to which the provisions of the Administrative Procedure Code apply

the Office evaluates the documents necessary to assess whether the processing of personal data creates

the risk of the rights and freedoms of the persons concerned being infringed; such as scope

personal data processed, the nature of their sensitivity, the purpose of their processing, the method of their processing

the means by which personal data are to be processed,

the diversity of processing operations to be carried out on personal data,

the nature of the premises in which the personal data will be processed, the extent of the data received

security measures, location and description of technical means, by means of

whose personal data will be processed, the internal regulations of the controller and the documents received

(eg standard contractual clauses for cross-border transfers that have been accepted without reservations),

on the basis of which personal data will be processed. Special registration

is subject to a fee obligation under Act no. 145/1995 Coll. on administrative fees

as amended. Special registration is one of the tools for compliance

laws in the processing of personal data from the point of view of preserving human rights guaranteed

Constitution of the Slovak Republic.

The Operator is entitled to start processing personal data in the IS registered for the special

registration only after receipt of the certificate of special registration from the Office.

In 2017, a total of 98 applications for special IS registration were received by the Office, with

after assessing the legal preconditions and the degree of risk of personal data processing in these IS,

a certificate of special registration was issued by the Office in 85 cases. In 2018

A total of 24 applications for special registration were received by the Office, and the Office also received this

period carefully assessed the lawfulness and impact of the processing of personal data on those concerned

persons in these information systems; a certificate of special registration has been issued

in 23 cases. The most frequently registered IS for special registration in the evaluated period

were ISs in which operators processed biometric data (for example, biometric data)

fingerprint or palmprint) in order to record attendance or entry into the defined

premises of the operator.

An overview of the number of special IS registrations according to the law

Year

Number of delivered

requests for special

IS registration

Number issued

certificate of special

IS registration

Number of stopped

special proceedings

IS registration

2017

98

85

13

to 24.5. 2018

24

23

1

6.3 Cross - border transfer of personal data

Cross-border transfer of personal data is an important part of personal data processing

in the conditions of increasingly frequent cross-border cooperation associated with the necessary exchange

information, including personal data.

Within the cross-border transfer of personal data, a distinction is made between cross-border transfers

within the EU Member States or the Contracting Parties to the Agreement on the European Economic

(hereinafter referred to as "Member States") and transfers to third countries. Transfer of personal data

within the Member States is not subject to any additional criteria and is governed by

provisions of Section 32 of the Act.

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

When transferring personal data to third countries, a distinction is made between the transfer of personal data to a third country guaranteeing or not guaranteeing an adequate level of personal data protection.

The status of the country that guarantees an adequate level of personal data protection is determined by the EC

decision. In assessing such adequacy of personal data protection, the level is examined local legislation, the existence of relevant legal acts, the enforceability of the law concerned obligations of the controller as well as the principles of personal data processing. In area institutional, the independence of the national supervisory authority, its powers and competences are examined.

As regards the status of the country, which guarantees an adequate level of personal data protection, the adequacy of the level of protection was not approved by the EC during the evaluated period personal data for any third country.

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

The cross-border transfer of personal data is a sensitive processing operation with personal data data in which personal data are transferred outside the territory of the Slovak Republic. The law defines a flexible cross-border transmission system, especially for transfers to third countries allows operators to make greater use of standardized safeguards privacy and personal data in the form of standard contractual and binding clauses internal rules.

Standard contractual clauses can be found in the relevant EC decisions. In case of the controller uses in the contract on the transfer of personal data to a third country without reasonable levels of personal data protection clauses that are different from the standard contractual clauses intended for transmission by the operator or intermediary, or they show a clear discrepancy with them, or if he does not use any contractual clauses, he is obliged ask the Office for consent to the transfer before starting the transfer. There was no office in the period under review

requested to give such consent to the cross-border transfer of personal data.

A very important legal institute in the transfer of personal data are the so-called binding internal rules; their importance is growing, as for large multinational companies represent an attractive possibility for cross-border transfers of personal data, which removes a lot of administrative burden.

Binding internal company rules can be applied only within one company, resp. her organizational units. A company that decides to introduce a binding in-house the rules must commit themselves to the adoption of the rules on personal data protection throughout the company (by all organizational units) and at the same time that it will be ensured compliance through established supervisory mechanisms. Introduction of binding in-house rules should create comprehensive privacy protection within multinational company, even in connection with cross-border exchange or personal transfer data within the company. Procedure for approving binding internal rules supervisory authorities is set out in the opinion and recommendation WP29. In the evaluated period In no case was the Office the main supervisory body in assessing the binding internal rules.

7 PERSONAL DATA PROCESSING CONTROL

During the period under review, the Office checked the processing of personal data by the supervisory authority empowered to act if at least two members were present at the same time inspection body (including the inspector).

The Office carried out regular inspections on the basis of the inspection plan for 2017 and 2018, exceptionally inspections were carried out by the Office in the framework of personal data protection proceedings or on the basis of suspected breaches of personal data processing obligations laid down by law.

Regular and extraordinary inspections carried out by a written inspection body have always been carried out focused on a specific operator or intermediary and their results were

formulated in the inspection report (if no breach of obligations has been identified
in the processing of personal data) or in the inspection report (if discrepancies have been identified
with the requirements of generally binding legislation). Results of inspections formulated
in the control protocol they initiated the initiation of personal data protection proceedings or were used
as a basis for issuing a decision in ongoing proceedings.

The focus of the inspections was on the real state of personal data processing with an emphasis
on the adequacy and practical application of the security measures taken, which has become apparent
on the time and professional complexity of the implementation of the inspections themselves.

In the area of proper controls, the Office placed particular emphasis on the basic principles of personal processing
data and information security risk management, including the possible effects of processing
personal data on the rights and legally protected interests of the persons concerned, as the setting
appropriate security measures (technical and organizational) and ensuring them
Continuous updating under the conditions of the operator or intermediary are essential
preconditions for successful minimization of security risks, resp. prevention
unwanted processing operations with personal data (for example, unauthorized disclosure
or disclosure of personal data). The security of personal data processing has resonated
also in carrying out extraordinary checks, which were generally initiated by the persons concerned
indicating insufficient security measures or processing operations
raising suspicion of a breach of the law.

The number of regular (planned) inspections performed in the evaluated period was affected
the number of exceptional checks that the Office is required to carry out ex lege as well as the number
pending checks carried over from the previous reporting period (2015-2016).

In the period under review, the Office completed 18 inspections initiated in 2016, of which 14 inspections
inspection report and 4 inspections by inspection record, and at the same time performed 20 regular
inspections, of which 12 inspection protocols and 5 records were completed by 24.05.2018
on control. In the evaluated period, the Office performed 33 extraordinary inspections, of which there were

by 24.05.2018 terminated by 6 inspection protocol and 17 inspection record.

27

Overview of inspections in the evaluated period

Results of inspections

completed during the period under review

Deficiencies found

(inspection report)

No detected

shortcomings

(inspection record)

14

4

18

22

Checks started from 01.01.2017 to

12/31/2017

Checks started from 01.01.2018 to

05/24/2018

7.1 Regular inspections (inspection plan)

During the period under review, the Office performed regular inspections on the basis of the inspection plan for 2017

and 2018. The control activities included in the control plan for a specific year were focused

to verify the compliance of personal data processing with generally binding requirements

legislation represented in particular by law. Taking into account technological developments

used in the processing of personal data, public activities were included in the control plan

and the private sector, with the Office focusing on the processing of personal data

presupposed an increased risk of unauthorized interference with the rights and rights protected

interests of the data subjects as well as the processing of personal data in the areas in which they have been repeatedly identified errors by operators or intermediaries when setting the conditions for the processing of personal data and their subsequent observance.

When creating inspection plans, as well as when selecting target areas for extraordinary inspections initiated by the Office, the Office drew on its previous experience and knowledge from supervisory activity (empirical-intuitive method).

7.1.1 The Schengen acquis

The Office regularly includes ISOU inspections in the inspection plan, by means of which it is ensured practical implementation of the Schengen "acquis" by the competent authorities in Slovakia Republic, as well as embassies of the Slovak Republic abroad. National inspections part of the second generation Schengen Information System (N.SIS.II) operated by Ministry of the Interior of the Slovak Republic and the national part of the Visa Information System (N.VIS) operated by the Slovak Ministry of Foreign Affairs and European Affairs Republics are included in the control plan on the basis of the recommendation resulting from the resolution of the Government of the Slovak Republic no. 755 of 30 November 2011, which the government approved Schengen Action Plan of the Slovak Republic as a priority of the Government of the Slovak Republic.

In connection with the change of the national access point of the EURODAC information system for the EURODAC II version (2015) was acquired by the operator, which is the Ministry of the Interior Of the Slovak Republic, new competencies and responsibilities; following that fact at the same time, the office was obliged to carry out an annual inspection of the processing of personal data at the EURODAC National Access Point.

In the national parts (subsystems) of the information systems in question, they are in addition to the usual ones specific categories of personal data are also processed (eg identification) data, in particular biometric data, data on racial or ethnic origin, data on infringements criminal liability or administrative liability and in general usable identifier, ie personal data capable of significantly infringing rights and rights

protected interests of the persons concerned. 7 inspections were performed in the evaluated period
processing of personal data of the persons concerned, namely two controls of the National
28
SIRENE (N.SIS II - national part of the second generation Schengen Information System),
four inspections of consular departments of embassies of the Slovak Republic (N.VIS national part of the Visa Information System) and one inspection of IS AFIS - EURODAC
(international comparison of fingerprints). Responsibility with which concerned
departments approach the implementation of the Schengen "acquis", also confirms the
that none of the above inspections revealed a conflict with the requirements of the generally binding ones
legislation.

7.1.1.1 Consular departments of selected embassies of the Slovak Republic

In the evaluated period, the Office performed 4 inspections of personal data processing
operated by the Ministry of Foreign Affairs and European Affairs of Slovakia
Republic, in the premises of the Consular Section of the Embassy of the Slovak Republic
in Beijing, Consulate General of the Slovak Republic in St. Petersburg, Embassy
Of the Slovak Republic in Ankara and the Embassy of the Slovak Republic in Tehran. Subject
inspections were focused on the security of personal data processing, compliance with obligations
associated with the duly exercised rights of the data subject, the functionality of the technical
and organizational mechanisms affecting the truthfulness, accuracy and timeliness of personal
data as well as their disposal. The purpose of the inspections was to identify the state of compliance
selected provisions of the law in the processing of personal data in the Visa Information
(VIS) in connection with the issuance of Schengen visas to the persons concerned and others
information systems in which the personal data of the persons concerned are processed
in the conditions of embassies. Based on the results of inspections of the national part of Visa
information system implemented in the premises of the said embassies
Of the Slovak Republic, the Office stated the compliance of the processing of personal data with the requirements

generally binding legislation.

7.1.1.2 SIRENE Bureau

Based on the fulfillment of tasks arising from the Schengen Action Plan of the Slovak Republic
the Office carried out two inspections of the National SIRENE Bureau, which is an organizational part of the Office
international cooperation of the Presidium of the Police Force of the Slovak Republic. Subject
controls focused on the security of personal data processing (including criteria
established by the Schengen Catalog of Recommendations and Best Practices), compliance with
associated with the duly exercised rights of the data subject and the functionality of the technical
and organizational mechanisms operating to ensure truth, correctness
and the timeliness of personal data. The purpose of the inspections was to verify the lawful use
and processing of personal data in the national part of the Schengen Information System II
generation (N.SIS II) in the performance of the tasks of the Police Force of the Slovak Republic for the purposes of
Art. Regulation (EC) No 2457/2006 of the European Parliament and of the Council 1987/2006, on the basis of which
data on third-country nationals in connection with refusal of entry are processed
or residence, as well as under Art. 36 Council Decision 2007/533 / JHA, according to which
processed data on persons and objects in N.SIS II for the purpose of discreet surveillance; or
targeted controls. Based on the results of both inspections focused on the procedures of the National
SIRENE Bureau, the Office noted the compliance of personal data processing with the general
binding legislation.

7.1.1.3 Automated European Fingerprint Identification System AFIS-EURODAC

In accordance with Art. Regulation (EU) No 32 of the European Parliament and of the Council. 603/2013 on the establishment
Eurodac for the comparison of fingerprints for the effective application of Regulation (EU)
no. 604/2013 laying down the criteria and mechanisms for determining the Member State
responsible for examining the application for international protection lodged by the national
third country or stateless person in one of the Member States, and

Member States' law enforcement authorities and Europol for comparison with the data in the system
Eurodac for law enforcement purposes and amending Regulation (EU) No 1077/2011 laying down
is set up by the European Agency for the Operational Management of Large-Scale Information Systems
in the area of freedom, security and justice, an obligation arose on 20 July 2015
carry out an annual review of the processing of personal data for law enforcement purposes
and comparing the fingerprint data with the data stored in the central system.
Control of the processing of personal data within the national access point
AFIS-EURODAC system focused on the consistency of the use of the communication infrastructure
with the basic principles of personal data processing, security of personal data processing
data and their destruction, the fulfillment of obligations related to the duly exercised rights of the data subject
persons and the functioning of technical and organizational mechanisms affecting the truth,
accuracy and timeliness of personal data.
The operator of the AFIS-EURODAC information system, which is the Ministry of the Interior
Of the Slovak Republic, ensured the fulfillment of related obligations through national
access points established within the Criminalistics-Expertise Institute of the Presidium
Police Force, Border and Alien Police Office Presidium of the Police Force
and the Migration Office of the Ministry of the Interior of the Slovak Republic. Control of personal processing
data in the AFIS-EURODAC system was carried out in 2017 under the conditions
Criminalistics-Expertise Institute of the Presidium of the Police Force. Based on the result of the inspection
procedures of the Ministry of the Interior of the Slovak Republic in the processing of personal data
the Office found compliance in the automated European fingerprint identification system
processing of personal data in accordance with generally binding legal regulations.

7.1.2 Foreign bank branch

Control of a branch of a foreign bank operating in the territory of the Slovak Republic
(operator) was based on the inspection plan focused on the principles of personal processing
the existence and application of an appropriate legal basis for processing, the manner in which

obtaining the consent of the persons concerned, fulfilling the information obligation towards the persons concerned,
destruction of personal data, relations between the controller and the intermediary,
adequacy of security measures, instruction of authorized persons, determination of responsible
persons, obligations related to the exercise of the rights of data subjects, cross-border transmission
personal data and the obligation to specifically register, notify or record information
systems. The purpose of the inspection was to identify the state of compliance with selected provisions of the law
when processing personal data about the bank's clients.
The inspection in question found an error consisting in non-compliance with the notification
obligations incurred by the operator in connection with the information system aimed at
to obtain information about business partners and potential clients. Mistake
of the operator was also found in connection with the transitional provision of § 76 par. 2 of the Act,
according to which (each) operator was obliged to give a contractual relationship with the intermediary

in accordance with this Act within two years from the date of entry into force of this Act. In relationship
no deficiencies were found in the other parts of the inspection, which the Office acknowledged in particular
in connection with the adoption of appropriate security measures and their regular updating
focused on innovative technical possibilities of personal data processing.

7.1.3 Insurance company

The control of the insurance company operating in the territory of the Slovak Republic (operator) was
based on the plan of inspections focused in the same way as the inspection of a branch of a foreign bank. The purpose
control was the identification of the state of compliance with selected provisions of the law during processing
personal data on the insurance company's clients.
The inspection in question found an error in the method of obtaining consent
data subject for the processing of personal data (consent did not contain
all the requirements laid down by the Personal Data Protection Act). Mistake
operator was also found in relation to the lack of information

notified to the data subject before obtaining his or her personal data for marketing purposes.

No deficiencies were found in relation to the other parts of the inspection.

7.1.4 Leasing company

Control of a leasing company operating in the territory of the Slovak Republic (operator)

based on the inspection plan, it was focused in the same way as the inspection of a foreign bank branch

and control of the insurance company. The purpose of the inspection was to identify the compliance status of the selected

provisions of the law in the processing of personal data on clients of non-bank creditors and others

non - bank creditors, consumer credit providers (without restriction or

to a limited extent) and other non-bank creditors.

The inspection in question found an error consisting in non-compliance with the notification

obligations incurred by the operator in connection with the information system aimed at

on its marketing activities, an error in the manner of obtaining the consent of the persons concerned

with the processing of their personal data for marketing purposes (the data subject did not have the

freely express their consent or disagreement with the processing of her personal data), as well as

error relating to the content of the contracts concluded by the operator with its

intermediaries (contracts did not contain all the requirements laid down by the Protection Act

personal data). No findings were found in relation to the other parts of the inspection

shortcomings.

7.1.5 Telecommunications Service Provider

Control of the television broadcaster, access to the Internet and public telephone

service operating in the territory of the Slovak Republic (operator) was on the basis of the plan

controls focused on the principles of personal data processing, existence and application

appropriate legal basis for the processing, the means of obtaining the consent of the persons concerned,

fulfillment of information obligation towards the persons concerned, liquidation of personal data, relations

between the operator and the intermediary, the adequacy of security measures,

instruction of authorized persons, appointment of a responsible person, related obligations

with the exercise of the rights of data subjects, the cross-border transfer of personal data and the obligation

specifically register, notify or record information systems. The purpose of the inspection was

identification of the state of compliance with selected provisions of the Act on Client Clients

providing telecommunications services.

The inspection in question found an error consisting in the incompleteness and incorrectness of the data

listed in the records of the information system focused on the records of clients, error

consisting in the absence of registration of the camera system, the mistake consisting in omission

the obligation to instruct authorized persons, errors in the field of security measures,

their documentation, updates and applications, as well as errors in obtaining consent

data subjects with the processing of their personal data for marketing purposes (data subject

did not have the opportunity to freely express her consent or disagreement with the processing of her personal

data). The operator's mistake was also found in relation to the storage of personal

data after the purpose of their processing and in relation to the scope and designation of the space

accessible to the public monitored by a camera system.

7.1.6 Cities and municipalities

On the basis of a plan of inspections and random selection taking into account the nationwide scope of the Office

eight checks on the processing of personal data by the authorities were carried out during the period under review

local government (operators), of which five inspections focused on municipalities and three inspections

focused on cities.

The inspections focused on the principles of personal data processing, existence and application

appropriate legal basis for the processing of personal data, the controller's procedure

in the processing of personal data without the consent of the data subject and in obtaining the consent of the data subject

persons, fulfillment of information obligation, liquidation of personal data, relations between

operators and intermediaries, the adoption of appropriate technical and organizational

measures, instructions of the authorized person, appointment of the responsible person, related obligations

exercising the rights of the data subject, as well as the obligation to register, notify or register personal data information systems.

The purpose of these inspections was to identify the state of compliance with the law during processing personal data by operators.

They resonated among the operators' errors identified by these inspections especially mistakes

- in the area of adopted security measures (a total of 6 cases of violation of § 19 par. 1 Act),
- associated with the conditions of delegation of the responsible person and related obligations operator (a total of 5 cases of violation of the provisions of Sections 23 to 25 of the Act),
- related to the conditions for monitoring premises accessible to the public (a total of 4 cases of violation of § 15 par. 7 of the Act),
- associated with the obligation to register IS that are not subject to special registration or notification obligation (a total of 4 cases of violation of § 43 paragraph 1 of the Act),
- associated with the obligation to instruct authorized persons before carrying out the first processing operations with personal data (a total of 4 cases of violation of § 21 paragraph 2 of the Act).

Of the results of those inspections, none of which were concluded by a finding of compliance with the requirements of the law, there is a justified obligation of the supervisory body to focus its attention to local authorities in the position of IS operators, by all available methods (ie not just control activities). From the performed inspections at the same time concludes that cities comply with legal requirements to a much greater extent, which is undoubtedly related to the human and financial resources which (unlike municipalities)

have. The Office finds the situation to be alarming, but not because of the cities and towns process the personal data of residents (data subjects) for different purposes, but because cities and municipalities in the position of local self-government bodies (except for specific exceptions) process

personal data on the entire population of the Slovak Republic.

7.2 Extraordinary inspections

In the period under review, extraordinary inspections were carried out to a decisive extent on the basis of

at the request of the persons concerned, possibly on the basis of suggestions other than those

the persons concerned. A significant part of extraordinary inspections was (traditionally) focused

for camera systems.

7.2.1 Resocialization center

Control of the processing of personal data by a non-profit organization that as accredited

the entity provides services in the field of social protection of children and social guardianship

(resocialization center - operator), was motivated by an initiative other than the one concerned

persons, the content of which suspected a violation of several provisions of the law

when processing the personal data of the Centre's clients.

The control focused on the principles of personal data processing, existence and application

adequate legal basis for the processing of personal data, the controller's procedure

in the processing of personal data without the consent of the data subject and in obtaining the consent of the data subject

persons, fulfillment of information obligations and liquidation of personal data, fulfillment of obligations

resulting from the relationship between the operator and the intermediary, the adoption of

technical and organizational measures corresponding to the way personal data are processed,

instruction of the authorized person, fulfillment of the operator's obligations related to supervision

on the protection of personal data (responsible person), as well as to verify compliance with the notification

obligations, special registration and the obligation to keep records of the information system.

In addition to the personal data of employees, the operator also processes the personal data of the data subjects

persons as clients of the Center. The clients of the resocialization center are understood as drugs

a dependent or otherwise dependent natural person or child to whom assistance is provided

usually associated with their long-term stay (eight months or more) in this center.

The client's stay in the resocialization center is based on a court decision

(interim measure or substantive decision) or in agreement with the client or his client
authorized representative (child), the conclusion of which is subject to the recommendation of an addictologist or
psychiatrist. Costs associated with the client 's stay in the resocialization center on the basis of
court decisions are borne by the state (through the Center for Labor, Social Affairs and the Family
Of the Slovak Republic), the client 's stay in the resocialization center on the basis of the agreement is
financed from contributions from the Higher Territorial Unit, as well as the client himself.
In relation to the lawfulness of the processing of personal data of the clients of the resocialization center was
found that the operator processes personal data on the basis of Act no. 305/2005 Coll., Which
sets out the purpose of the processing of personal data, the circle of data subjects and the scope of personal data
data, as a result of which it acquires the nature of a special law in the sense of § 10 par. 2 of the Act.
The inspection did not confirm any of the suspicions formulated in the complaint and was not
found or any other error of the operator. The Office (among other things) found personal data
clients processed in a magazine issued by the operator are published
in an anonymised form, as a result of which no personal data is processed

by publishing them. Photos of clients on the notice board in the main building of the resocialization
resorts, videos posted through YouTube, and accounts set up in
Facebook social networks are not part of any information system of the inspected person.
At the same time, the Office stated that the inspected person's procedures for acquisition and further processing
personal data correspond to the requirements of § 6 par. 2 of the Act (principles of processing
personal data) as well as that in relation to the security of personal data processing
in the information systems of the inspected person did not find a conflict with the requirements of § 19 par. 1
of the law. The inspection in question was completed by signing the inspection record.

7.2.2 Foreign bank branch

Control of a branch of a foreign bank operating in the territory of the Slovak Republic
(operator), which took place at the initiative of the data subject, was aimed at

the controller 's procedure for processing the personal data of the data subject through
contracts under which several financial services have been provided to the data subject. Touched
the person exercised his rights against the operator in writing, but was not satisfied
with content, resp. the extent of the operator's response. The person concerned in the complaint
addressed to the Office in particular that it had not provided its information to the operator
the address to which the operator has sent several documents or the telephone number
to work.

The operator processes the personal data of clients to the extent of the data specified in the contract
documentation for the purpose of establishing pre-contractual relations, the provision of consumer credit
and credit relationship management, reporting and archiving of unusual operations reports, identification
and client verifications in accordance with the Act on Protection against Money Laundering
and protection against terrorist financing, reception, handling and archiving of complaints,
protection and enforcement of the operator's rights against clients. Provided personal data of clients
are not published.

The performance of the inspection was focused on compliance with selected provisions of the law during processing
personal data of clients of a foreign bank branch with emphasis on communication between
the controller and the data subject, as well as the processing procedure of the controller
personal data of the data subject in relation to the contracts concluded with the controller since
2010, on the basis of which the person concerned was granted loans, a credit card,
installment sales, and the like. The Office requested complete documentation from the operator
concerning all the contractual relations of the person concerned with the operator and subsequently
entered the personal data information systems in which the controller processed
personal data of clients. The Office focused on credibly proving the source of obtaining personal
data (correspondence address other than permanent residence address, employment telephone number
and the name of the employer) and the lawfulness of their processing.

The inspection did not confirm any of the suspicions formulated in the complaint and was not

found or any other error of the operator. By looking at the client folder

the person concerned was found to have the person concerned in the questionnaire which was part of the contract

on consumer credit, itself provided details concerning the employer (including the telephone number)

employment numbers). By verifying the stored communication records of the call center employee

with the data subject, it was found at the same time that the data subject could prove himself / herself by telephone

asked the operator to change the correspondence address, while the address of permanent residence

remained unchanged. The inspection in question was completed by signing the inspection record.

34

7.2.3 Camera systems

Monitoring of areas accessible to the public by camera systems is generally

considered a highly effective way of protecting health, property and crime prevention.

Related proposals and incentives for monitoring system operators

they also have a significant effect on the focus of the Office's control activities. In the evaluated

During this period, the Office checked the compliance of the processing of personal data with the principles of personal

processing

data with an emphasis on compliance with the basic obligations of the controller and the existence

appropriate legal basis, the adoption of adequate security (technical

and organizational) measures corresponding to the way personal data are processed, compliance

the obligation to instruct the entitled person, the fulfillment of the obligation to entrust the responsible person, as well as

fulfillment of the obligation to notify, the obligation of special registration and the obligation to keep records

IS.

In the evaluated period, the Office performed and completed 16 extraordinary inspections focused on

for processing personal data through a camera system. Of the total number

6 inspections were carried out on operators who are legal entities or

self-employed persons and 10 checks on operators who are natural

persons.

In carrying out these inspections, the Office placed emphasis on the adequacy of the scope monitored space, resp. the risk of undue interference with the rights and freedoms of the persons concerned, as well as on the legal basis and security of personal data processing. Of the total number performed

In the evaluated period, there were 11 inspections completed by the inspection record (of which 8 control records were based on the fact that monitoring is not subject to the regime of the Act) and 5 inspections were completed by the inspection protocol.

Operators whose inspection was completed by the inspection record duly complied with notification or registration obligation and have duly informed authorized persons.

The monitoring itself was approached by all operators in accordance with the principle proportionality, as they monitored the area only to the extent necessary to achieving the purpose of processing. The monitored area was in all cases marked as to inform the persons concerned of the monitoring before entering the monitored area.

The Office found a breach of the operator's obligations under the law in five cases.

The breach of the operator 's legal obligations consisted in particular in the fact that operators monitored an area inaccessible to the public without a legal basis, monitor the area accessible to the public to the extent that it was not necessary to achieve for the purpose of processing, records made by monitoring the area accessible to the public kept for more than 15 days, did not clearly mark the monitored area, did not have properly instructed authorized persons and did not fulfill the obligation to register the IS. In relation to security processing office in two cases, found that the operator had not adopted adequate technical and organizational measures, and in two other cases found that the operators in their conditions, they have taken security measures in accordance with the requirements of the law, but the documentation proceeded in violation of the provisions of Decree no. 164/2013 Coll., In particular in the information system security analysis section.

Based on the identified violations of the law, it is necessary to continue to pay increased attention operators who process personal data by monitoring the accessible area

public, including with regard to the fulfillment of the information obligation.

35

7.3 Conclusions arising from the Office's control activities

In general, from the results of regular and extraordinary inspections performed in the evaluated
period, the obvious efforts of operators to ensure compliance with the provisions of the law, at the same time are
however, some categories of operators also need to be addressed
increased attention in the coming period. The control activity of the Office, the basic
the mission is to act preventively on the protection of personal data processed
IS operators, it is therefore desirable to support the Office's other activities at this time,
mainly due to a fundamental change in the legal regulation of the conditions of processing represented
Regulation and Act no. 18/2018 Coll., Which apply in the territory of the Slovak Republic
from 25.05.2018. The basic precondition for compliance with the requirements of the Regulation
and Act no. 18/2018 Coll. is a general identification with the intent of this legislation
formalize.

36

8 PERSONAL DATA PROTECTION PROCEDURE

The purpose of personal data protection proceedings is to determine whether the conduct of the controller or
the rights of natural persons in the processing of their personal data have been violated by the intermediary
and, if deficiencies are identified, impose remedial action. For personal protection proceedings
data, the provisions of the Administrative Procedure Code shall apply. Substantive decision in protection proceedings
personal data is usually the basis for fine proceedings, which is a separate administrative
proceedings.

If there is no competence of the Office to act and decide the case, most often because
the case in question does not fall within the scope of the law, the Office is obliged to forward the application
competent administrative authority. In 2017, the Office forwarded 8 submissions to the relevant court
administrative authority for action and decision. In 2018, a total of 3 submissions were submitted.

The Office may, in the exhaustively determined cases referred to in the third chapter of Part Three of the Act
postpone the proposal or initiative. The most common case of postponement is its unfoundedness when
it is already clear from the evidence provided, in particular by the person concerned, that there has been no breach of the law.
In 2017, the Office postponed 213 submissions and in 2018 141 submissions were postponed.
The Office, in the framework of supervisory activities, conducts proceedings on the protection of personal data with the aim of
protection
the rights of natural persons against unauthorized interference with their private life during processing
their personal data, while also examining compliance with legal obligations.
If it finds a violation of the rights of the data subject or a breach of personal processing obligations
by a decision, if justified and expedient, impose on the controller or
the intermediary to take remedial action within a specified period
and the causes of their occurrence. Otherwise, it will stop the personal data protection proceedings. Proceedings
on the protection of personal data begins on the proposal of the petitioner or on the Office's own initiative.
Proceedings on the Office's own initiative are initiated on the basis of an initiative pursuant to § 63 para. 5 of the Act,
on the basis of the results of the inspection according to § 60 par. 2 in connection with § 63 par. 7 of the law, which they were
identified deficiencies or on the basis of the Office's own finding of a suspected infringement
of the law, as proceedings instituted without a petition.
In the monitored period of 2017 and 2018, the Office initiated 230 administrative proceedings, of which 96 were
initiated at the request of the person concerned, 50 initiated on the basis of an initiative, 26 initiated on the basis of
the results of the inspection, which identified deficiencies and 58 proceedings were conducted by the Office on its own initiative
on suspicion of a breach of the law.
In 2017, the Office initiated administrative proceedings on the basis of a proposal in 59 cases, on the basis of a complaint
in 42 cases, based on the results of inspections in 10 cases and on its own initiative in 20
cases.
In 2018, the Office initiated administrative proceedings on the basis of a motion in 37 cases, on the basis of an initiative
in 8 cases, based on the results of inspections in 16 cases and on its own initiative in 38

cases.

37

Overview of the methods of initiating proceedings under the law

Year

Based on

proposal

Based on

initiative

Based on

inspection results

From my own

initiatives of the Office

2017

59

42

10

20

to 24.5.2018

37

8

16

38

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

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

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

Between 2017 and 2018, the Office requested cooperation a total of 1,055 times. In protection proceedings

personal data, there were five cases where the entity from which the co - operation was requested
did not react to it and the Office even after the call to fulfill its obligations under § 74 par. 1 of the Act
co - operation was not provided (in the given cases proceedings were initiated against the subjects
on fines).
The Institute of Legal Representation was used in a significant number of cases during the period under review,
except that all parties to the proceedings were represented by legal persons
representatives. The most common subject of personal data protection proceedings was the review
or by processing the personal data of the data subjects in the IS, which included the cameras,
there was a violation of the provisions of the law. One of the most common violations of the law was
processing of personal data without a legal basis, resp. contrary to law
unauthorized disclosure of a universally applicable identifier (birth number)
provided for by a special law, insufficient security of personal data processing.
8.1 Knowledge of personal data protection based on personal data protection proceedings
In the proceedings on personal data protection, several pieces of evidence were used in the evaluated period
the means by which the true state of affairs can be ascertained and, for that purpose,
more complicated matters, in addition to the consideration, used the possibility of performing extraordinary
controls directly at the operator or intermediary. The inspection proved to be
an effective means of ascertaining the true situation, in particular when checking camera IS on
where it has made it possible to determine reliably the method and individual aspects of monitoring and on the basis of
assess the intrusion of the monitored persons. In order to find out the real state of affairs
there is also a relatively high number of requests for cooperation through which they were made
secured in the file materials, especially documentary evidence. The persons concerned served
mostly precise proposals containing all the requisites required by law, while only
to a minimum, they had to be called upon to remedy the shortcomings of the administration. Len
sporadically, the petitioner did not complete his motion to initiate proceedings after the summons.
Personal data protection proceedings, as a type of administrative procedure, are characterized by sensitivity

the issue under consideration, which concerns the observance and protection of fundamental rights and freedoms in the field of personal data processing. The personal data protection proceedings are not public proceedings, which includes several peculiarities that complement, resp. extend the legislation Act no. 71/1967 Coll., Or where necessary exclude the application of Act no. 71/1967 Zb. These specificities are important for the correct application of personal data protection, the Office in the first instance proceedings where appropriate and necessary, taken into account. Such a special institute in personal data protection proceedings is e.g.

38

secrecy of the petitioner's identity in cases where his rights could be violated and legally protected interests (as the person concerned), or negative action by operator. The secrecy of the petitioner's identity found its justification and the persons concerned in the interest of their protection, they used it in the evaluated period, for example, in proposals by which sought the protection of their rights and the interests protected by law in the exercise of their rights jobs.

During the period under review, operators often in the course of personal protection proceedings data before attempting a substantive decision, they tried to dispose of the findings voluntarily shortcomings in the processing of personal data, as well as to adopt effective safeguards lawful processing of the personal data of the persons concerned. About received and executed measures to remedy the deficiencies found by the parties to the Office within the prescribed time limits as a general rule, there was no reason to initiate proceedings for a disciplinary fine on the grounds of negligence.

39

9 PENALTIES FOR BREACH OF THE LAW

Sanctions for violations of the law are fines and disciplinary fines. Sanctions are adjusted in the fourth the title of Part Three of the Act.

9.1 Penalties

The procedure for imposing a fine, as a separate administrative procedure, is conducted by the Office on the basis of a finding breaches of the law ex officio. When imposing a fine and determining its amount the Office shall take into account, in particular, the gravity, duration and consequences of the infringement, the repetition such a course of action and the extent of the risk to private and family life and the number of persons concerned persons. In addition to the operator and the intermediary, the Office may impose a fine on another entity (eg for failure to cooperate, breach of confidentiality, provision of false personal data). Especially in terms of the gravity of the infringement law defines the cases when the Office obliges to impose the obligation and when it has the possibility not to impose a fine, taking into account other facts.

In 2017, the Office legally imposed 20 fines in the total amount of EUR 27,800 and collected a total of EUR 36,860.47 (fines imposed in 2016 and paid in 2017). Average fine per year 2017 amounted to approx. EUR 1,390. The Office imposed the lowest fine in the amount of EUR 300 for breach of the obligation to act in accordance with technical, organizational and personnel measures taken by the operator. The highest fine in the amount of EUR 5,000 was imposed by the Office operator for unauthorized disclosure of a generally applicable identifier of a larger number of persons concerned.

In 2018, the Office legally imposed 37 fines in the total amount of EUR 89,800 for violating the law. In 2018, the Office collected a total of EUR 93,000.07 on fines as of the closing date of the report (September 17, 2018), until May 24, 2018, the Office collected EUR 22,450.00 in fines. Average fine per year 2018 amounted to EUR 2,427. The Office imposed the lowest fine in the amount of EUR 150 operator for failing to cooperate. The Office legally imposed the highest fine in the amount of EUR 40,000 to the operator for violating the security of personal processing data. In one case, the operator requested the possibility to pay the fine imposed in installments. Taking into account the justification, the Office granted the operator's request.

Overview of fines imposed and collected in the monitored period

Year

Count

fines

Total height

legally imposed

fines in Euros

Average height

fines rounded

for the whole Euro up

Total selected on

fines in Euros

2017

20

27,800

1390

36,860.47

2 427

to 24.5.2018 was

collected on fines

22,450.00

as of the closing date

reports (17.9.2018) to

was 93,000.07

2018

37

89 800 CZK

40

The fine, as a type of sanction, was mainly repressive and preventive in the period under review
function. In imposing it, the Office took into account, inter alia, the status of the entity and its activities, such as
also the impact of the amount of the fine on its continued existence. In connection with the imposition of fines during
during the evaluated period for violation of the law, it can be stated that they did not impose fines
liquidation effects.

9.2 Ordinary fine

The Office may impose a disciplinary fine exclusively on the operator or intermediary.

A disciplinary fine, which serves to ensure a dignified and undisturbed course of supervision
activities of the office, resp. as a sanction for non-compliance with certain obligations imposed in the proceedings
on personal data protection did not need to be imposed in 2017, while in 2018 they were
imposed two disciplinary fines in the amount of EUR 200 and EUR 1,000 for failure to cooperate
required by the inspection body.

9.3 Selected cases from the supervisory activities of the Office

9.3.1 Postponements

9.3.1.1 Disposal of personal data of the data subject

In 2017, the Office received a proposal from the person concerned against the operator,
who was to violate the provisions of the law by processing the personal data of the data subject
in connection with the conclusion of the injunction, did not liquidate without undue delay, but imposed
to the archive.

According to the provisions of § 17 par. 1 of the Act, the operator is obliged to fulfill the purpose of processing
ensure the destruction of personal data without undue delay. Paragraph 1 according to § 17 par. 2
law does not apply if personal data are part of the registration record. In that case
the operator ensures the liquidation of the registration record according to a special regulation.

After examining the documents and evidence gathered in the examination of the case in question, the Office found that
that the operator has entered into an injunction with the person concerned pursuant to Section 724 et seq. of the law
no. 40/1964 Coll. The Civil Code, as amended, the subject of which was

taking the necessary steps to enforce the data subject's claims for compensation

damage resulting from the loss event. The operator thus disposes of personal data

the person concerned processed for that purpose in accordance with a special regulation. Office at

postponed the motion to initiate proceedings on the basis of the findings.

9.3.1.2 Disclosure of personal data in the notice of the place where the document is filed

In the first half of 2018, the Office received the submission of the person concerned, who found out through

Google's Internet search engine that gives her personal information in the range of first name, last name, year

birth, permanent residence are publicly available on the Internet in the published city name

about the place where the document is stored, where he can pick up the addressed document in person.

By monitoring the internet links found, the office found that the document in question

The notice of the place of storage of the document was published by the city on its official website

page in the official notice board section and it was a notice to be posted for the 15th

days. The data published in the notification were assessed as personal physical data

persons in accordance with the provisions of § 4 par. 1 of the Act. The Office evaluated the submission of a natural person as

proposal to initiate proceedings on personal data protection against the city as an operator.

In relation to the subject matter of the proposal, the city was obliged to have a legal basis

disclosure of personal data, respect the principles of personal data processing,

especially after the end of the purpose of disclosure of personal data to destroy them.

In order to assess the matter in question, the Office called on the city to cooperate. From the city's answer

it was established and it was also proved that the city was requested by the bailiff to provide it

cooperation in accordance with a special law, which is Act no. 233/1995 Coll. on bailiffs

and Execution Activities (Execution Rules) and on Amendments to Certain Acts (hereinafter referred to as the Execution

Rules)

"Enforcement Act"), which regulates the obligation of third parties to cooperate with the courts

to the executor to the extent necessary. The bailiff asked the city to serve the document

to the liable person - natural person, as he did not stay in his place of permanent residence.

The document addressed to the natural person was placed in an envelope delivered to his own hands. The city

on the basis of the above and the obligation to cooperate with the bailiff

notified the natural person of the deposit of the bailiff's document by posting the notice on his

online official whiteboard. For the purposes of notification of the deposit and delivery of the official consignment,

city authorized to process, ie. disclose personal data of a natural person within the scope of identification

the consignee of the official consignment to be delivered. After the end of the purpose of personal processing

data, the city was obliged to stop publishing personal data in the posted notice.

The Office checked whether the notice was posted from the online official board and thus terminated

disclosure of personal data of a natural person for that purpose.

Based on the evaluation of the collected documents and the assessment of the matter in relation to

to the law, the Office assessed the person concerned's proposal as manifestly unfounded, as the city

was entitled to disclose the personal data of the data subject to the extent necessary,

surname, year of birth, address of permanent residence for the purposes of notification of place of storage

official postal item due to its delivery to the obligor in the enforcement proceedings. Office

therefore suspended the application.

9.3.1.3 Information obligation in the exercise of the right of petition

In 2018, the Office assessed the complaint according to which the organizer of the petition obtained personal information

data of the persons supporting the petition did not fulfill the obligation to communicate the information to the persons

concerned

according to § 15 par. 1 of the Act. The Office found that the personal data of the petitioners were

processed according to § 10 par. 2 of the Act, ie on the basis of a special law, which was in the given

in the case of Act no. 85/1990 Coll. on the right of petition, as amended, to the extent

and in the manner provided for by the Law on the Law of Petitions. Since according to § 15 par. 3 of the Act

the obligation to notify the data subject of information pursuant to § 15 par. 1 of the Act does not apply to

processing of personal data according to § 10 par. 2 of the Act, the Office assessed the complaint as obvious

unfounded and put it aside.

9.3.1.4 Sending marketing offers

In 2018, the data subject made an oral motion to initiate proceedings on the protection of personal data, which contained a suspicion that the operator who is the provider of cash loans, processes the petitioner's personal data for marketing purposes without a legal basis. The petitioner stated that he had been a client of the operator in the past and that he was already one several years, the operator sends him a repeat offer to his postal address to grant a loan. The petitioner further claimed to have applied to the operator several times by telephone and e-mail with a request to terminate the processing of his personal data for marketing purposes, but to no avail.

42

The Office, by examining the documents and evidence gathered in the examination of the present case, found that that the operator processed the applicant 's personal data for marketing purposes on the basis of consent of the petitioner, who provided in the Statement on instructions on personal data protection of 2012, which was part of the Consumer Credit Agreement concluded by the petitioner with the operator in 2012. The submitted copy of the statement in question showed that that the operator has obtained a separate, separate, from the agreement to the consumer credit agreement separate consent of the petitioner with the processing of his personal data for a predetermined purpose. The proposer has given the controller consent to the processing of his personal data for the purposes of information about the products and services provided by the addresses for a period of 10 years from fulfillment of obligations towards the operator. Due to the date of conclusion of the Contract on consumer credit, it was clear that the consent granted could expire at the earliest in 2022. The operator therefore processed the personal data of the petitioner for the purpose of sending offers for the provision of a loan in accordance with § 9 par. 1 of the Act, with the legal basis of this processing of personal data was the consent of the petitioner according to § 11 par. 1 of the Act. Pursuant to § 28 par. 6 and § 29 par. 3 of the Act, the petitioner was obliged to request his blocking,

resp. liquidation of personal data after revocation of consent, resp. termination of the purpose of processing

addressed to the operator in a certain form - in writing or orally in the minutes, whereby

he was obliged to complete the request made by electronic means within three days. Draftsman

addressed his request to terminate the processing of personal data to the controller

by phone and e-mail. The operator was not obliged by law to comply with the request

in such a form. Therefore, the operator when processing the applicant's request for termination

sending marketing offers proceeded in accordance with the law. The operator stated that

that it registers the petitioner's request to delete and revoke the consent to the processing of his / her

personal data, on the basis of which he has already canceled the sending of advertising offers to the applicant, namely

despite the fact that the application was not submitted in the form prescribed by law. The office did not find out

violation of the law, the submitted proposal as manifestly unfounded therefore postponed.

9.3.2 Procedures

9.3.2.1 Breach of personal data protection when donating a discarded computer to another person

In the first half of 2017, the Office received a petition from the petitioner, who learned that she was a schoolgirl

discovered documents concerning pedagogical staff in a donated computer from the municipality,

in particular, the appellant's salary assessment. The petitioner suspected that she had obtained

information about her salary and her personal data were processed unjustifiably, and so it was

damaged her reputation. Relevant evidence that he had been discarded was also attached to the application

and the donated computer to the schoolchild contains her personal data in the salary assessment. The submission was

evaluated as content as a proposal to initiate proceedings on personal data protection. Office for

reasonable violation of the law initiated proceedings on a motion against the municipality and the school. Office in the

beginning

proceedings issued a preliminary measure pursuant to § 43 par. 1 letter (b) the administrative procedure by which he has

imposed

the municipality's obligation to keep the data contained in the computer donated by the municipality to the schoolchild,

who was already in the school's computer room at the time. Evidence needed for

examination of the subject matter of the proceedings were, inter alia, the data contained in the record

computer devices. The Office considered that the purpose of the conduct should not be undermined

for the necessary recording equipment of the computer in question, in particular to avoid

to liquidation, loss or other impairment of its contents. To find out the real situation

The Office requested the cooperation of the municipality and the school.

43

The controller is responsible for the security of personal data. The operator is obliged

protect processed personal data from damage, destruction, loss, alteration,

unauthorized access and disclosure, provision or disclosure, as well as prior

any other impermissible processing methods. To this end, it shall take appropriate

technical, organizational and personnel measures corresponding to the way personal data are processed

data, taking into account in particular the technical means available, confidentiality and relevance

personal data processed, as well as the range of possible risks that they are capable of

security or IS functionality.

From the collected documents, the office had found and proved that the municipality provided the school to the pupil

computer for the purpose of practicing computer skills. It was supposed to be an old unnecessary one

the computer in the archive has already been scrapped, and the municipality should have checked it

discarded computers and in good faith that all data is deleted from the computer, this computer was

handed over to the student. The Office had proved from documentary evidence that the recording equipment

discarded computer contained working documents of the school with personal data.

On the basis of the documents collected in the proceedings, the Office stated that the municipality had violated § 19 par. 1

by failing to comply with the obligation to protect the petitioner's personal data processed

in the school documents located in the discarded computer of the municipality handed over to the pupil

schools, prior to their unauthorized access and disclosure to third parties by non-acceptance

appropriate security measures appropriate to the way these personal data are processed

data. In view of the mistake found, the Office imposed protection measures on the municipality

personal data of natural persons found in the discarded computer until their disposal.

The proceedings against the school were stopped by the office, as it was proved that the computer with documents, the content of which was also personal data, owned, used, excluded from the register of the municipality, which at the same time, it has not taken adequate measures to ensure the protection of the personal data of the data subjects persons.

9.3.2.2 Processing of personal data after withdrawal of consent

In 2017, the Office conducted proceedings on the protection of personal data at the proposal of the petitioner, who argued that the controller did not stop processing his personal data despite that the applicant has withdrawn his consent to the processing. The Office found that in the present case processing of personal data necessary for the performance of the contract in which the claimant acts as one of the contracting parties, therefore the operator could not meet the request of the proposer due to the fact that he processed the objected personal data on the basis of § 10 par. 3 letter b) of the Act without consent of the person concerned and, in this sense, the petitioner's rights have not been infringed. Office at the same time found that the controller determined the conditions for the processing of personal data by default obtained consent to the processing of personal data also in relation to such processing, which carried out on a different legal basis than the consent of the person concerned, as was the case also in the case of a proposer who has given the operator consent to personal work data for which the law did not require consent and for which the controller could not provide the exercise of the rights which the law confers on the data subject in relation to the processing of personal data data on the basis of consent.

The Office found that the operator had misled the persons concerned in this way and restricted their right to transparent processing of personal data, thus violating § 6 para. 2 letter b) of the Act. By decision, the Authority imposed remedial measures on the operator identified shortcomings.

9.3.2.3 Delivery of documents containing a special category of personal data

In 2017, the Office conducted proceedings on the protection of personal data on the basis of a proposal from the data subject

persons suspected of a personal data breach

by sending a letter containing a specific category of personal data to the data subject

persons by ordinary letter. In order to find out the complete and real objective

state of affairs, the operator underwent an extraordinary inspection of personal processing

data.

The operator assumed that each letter item was from its moment

handover at the collection point is protected by postal secrecy in accordance with § 32 par. 2 letter g)

Act no. 324/2011 Coll. on Postal Services and on Amendments to Certain Acts

as amended (hereinafter referred to as the "Postal Services Act") and at the same time postal

secret in terms of its definition in § 10 of the Postal Services Act, Art. 22 of the Act

no. 460/1992 Coll. The Constitution of the Slovak Republic, as amended, and Section 196 of the Act

no. 300/2005 Coll. Criminal Code as amended.

Postal conditions of the entity providing postal services according to the Postal Postal Act

provide that the entity is not responsible for the leakage of information and data on consignments

and the contents of the consignments, if they can be read, reproduced or otherwise directly

unprotected acquisition before they are submitted by the sender or after they have been delivered to the addressee.

It follows that it is up to the sender to assess the confidentiality of the content

transported consignment and chose the appropriate type of postal item accordingly,

i.e. the corresponding service provided by the postal service provider under the law

on postal services.

When processing personal data, the controller is obliged to proceed in such a way as to protect

personal data processed and, inter alia, prevent unauthorized access, disclosure or

provision of personal data. For this purpose, he is obliged to adopt adequate security

measures covering all areas which have or may have an impact on the processed

personal data and their security. Security measures must take specific account

the conditions under which the controller processes personal data, including in this case
secure delivery of consignments containing a specific category of personal data, and which
delivery is related to the activity of the operator.
In the proceedings, it was found that the operator had not taken adequate safety measures
in connection with the processing of a special category of personal data of the persons concerned (clients)
when delivered by letter, and thus when taking appropriate security measures
proceeded in violation of the provisions of § 19 par. 1 of the Act because it was mandatory for protection purposes
personal data processed before their damage, destruction, loss, alteration,
unauthorized access and disclosure, provision or disclosure
technical, organizational and personnel measures corresponding to the way personal data are processed
data, taking into account the technical means available, the confidentiality and the importance of the data processed
personal data as well as the extent of possible risks.
The Office imposed measures on the operator to remedy the identified deficiencies and the causes of their occurrence
and ordered the operator to take appropriate technical, organizational and personnel measures
corresponding to the way personal data are processed in connection with the processing of the special
categories of personal data of the persons concerned upon delivery, document the measures taken
and inform the entitled persons about the measures taken.
45
9.3.2.4 Making e-shop purchasing conditional on marketing approval
In 2017, the Office conducted proceedings on the protection of personal data on the basis of a complaint in the case
suspicions of violating the provisions of the law in the operation of the e-shop. The content of the complaint was
a statement that the operator makes the purchase conditional on registration on its website,
whereas in order to successfully complete this registration, the buyer must give consent to processing
your personal data for marketing purposes.
On the basis of information, documents and evidence gathered during the protection proceedings
The personal data office found that if the buyer registered on the website

the operator fills in all the required information, but does not tick the box

gives the controller consent to the processing of personal data within the scope of registration

for marketing purposes, clicking on the "Register" button will clear the verification that the buyer

"Is not a robot" and the buyer remains on the registration form page. Registration that is

condition of purchase on the operator's website is so successful only if

the buyer indicates consent to the processing of his personal data for marketing purposes.

At the request of the Authority, the operator stated that registration should have been possible without consent

with the processing of personal data for the purposes of further marketing processing, whereby

the wrong registration system should have been set due to an incorrect setting

services (technical error).

According to § 11 par. 3 of the Act, the operator may not enforce the consent of the person concerned, nor

conditional on the threat of denial of the contractual relationship, service, goods or obligation

established by the operator by a legally binding act of the European Union, international

the treaty by which the Slovak Republic is bound or by law. The operator violated

provision of § 11 par. 3 of the Act, when in order to successfully complete the registration required from

buyers indicate consent to the processing of personal data for marketing purposes, thereby

there was the enforcement or conditional of the consent of the persons concerned by the threat

rejection of the contractual relationship, as the inability to register on the website

the operator ultimately made the purchase impossible

at the operator. It does not matter whether it was an intentional act or a technical error.

The operator during the personal data protection procedure registration settings system

therefore, the Office imposed on him a measure to correct the identified deficiencies and the causes of their occurrence

and ordered him to ensure that registration on his website was possible

even without indicating consent to the processing of personal data for marketing purposes.

9.3.2.5 Disclosure of personal data in draft employment contracts in bulk

sent by e-mail

The Office accepted the submission of the data subject in the matter of unauthorized disclosure of personal data in the draft employment contracts to be circulated by the operator's staff in bulk to their work email addresses. The proposal stated that they had been sent out en masse draft contracts by e-mail contained personal data of the operator's employees including salary data. The submission was assessed as a motion to initiate protection proceedings personal data. The petitioner requested the Office pursuant to § 63 para. 4 of the Act on the Secrecy of Its identity.

To find out the real state of affairs, the office called on the operator to cooperate. Operator processed personal data of employees for the purposes of personnel and payroll and personal data the persons concerned were processed through natural persons who had, in accordance with the law

status of beneficiaries. In this particular case, they had access to personal data processed for the given purposes by two authorized persons of the operator, which were demonstrably instructed in the rights, obligations and responsibilities under the law in execution processing operations with the personal data of the data subjects processed for the purposes of personnel and payroll.

The Office had proved that one of the authorized persons had sent it electronically from his e-mail through the WORD annex to the employment contract document of the 53 persons concerned, including their personal data name, surname, residence, birth number, basic salary valid at the time of signing unauthorized disclosure of the personal data of the persons concerned, including a special category of personal data (birth number) for a larger group of employees operator.

The Office found that the rights of the persons concerned whose employment contracts were sent in e-mail communication have not been violated by the systematic procedure of the operator at processing of their personal data or as a result of breach or negligence of obligations of the operator in the field of personnel security. The procedure that occurred

to unauthorized disclosure of personal data of the persons (employees) concerned, was limited to the individual processing operation carried out by the authorized person in breach with instructions on its rights and obligations in the processing of personal data and in conflict with it with the operator's internal regulations. The Office also found that the operator evaluated the case, registered it as a security incident and investigated. The fact that the employee of the operator in the given case acted contrary to the instructions of the authorized person does not relieve the operator of the strict responsibility to guarantee the safety of those processed personal data according to § 19 par. 1 of the Act. Responsible for the security of personal data operator.

On the basis of the collected documents, the Office found a violation of the provisions of Section 19 para. 1 of the Act by sending its employee - the authorized person, electronically to the group employees of the operator as part of the e-mail attachment on employment contracts and employment contracts of the 53 data subjects with their personal data, thereby breaching the obligation protect the processed personal data from unauthorized disclosure. Based on the findings imposed an action on the operator to remedy the identified deficiencies and causes as well as the obligation to inform the Office in writing of their fulfillment. Following on from the stated violation of the provisions of § 19 par. 1 of the Act, the Office initiated proceedings in the second half of 2017 on the imposition of a fine in which the operator was fined for the detected error.

9.3.2.6 Publication of a universally applicable identifier

In 2017, based on the received complaint, the Office conducted proceedings on the protection of personal data in the matter of suspicion of violation of the provisions of the law in the publication of compulsorily published orders on the website of the operator - the municipality. The complaint contained an allegation that that the operator, in the context of the data on the four mandatory published orders, as well as within the text of the orders themselves in the .pdf format, he published the birth number of the person concerned as the ID number natural person who acted as a supplier.

On the basis of information, documents and evidence gathered during the protection proceedings

personal data, the office found that the birth number of the person concerned was published by the operator as an ID number

on the grounds that in the information system used by the operator for publication

orders, it was necessary to enter the ID number or birth certificate when entering a new supplier into the database

number. Without entering this information, the system did not allow the registration to complete. The operator therefore

asked persons who did not have an assigned ID number to provide consent to processing and publication

their personal data (including birth number) on the website. Operator

after notifying the authorities checked the capabilities of the information system and found that the system administrator

did not instruct the operator's staff to use a slash when entering their personal identification number,

birth number would not be published.

The operator, the municipality, was based on § 5b of Act no. 211/2000 Coll. obliged to publish

exhaustively defined data on completed orders, including name, surname,

the permanent residence address of the supplier - natural person and the identification number of the supplier, if any

assigned. Act no. 211/2000 Coll. however, no other regulation provided for an obligation

publish the operator within the data on completed orders and suppliers

also the birth numbers of the supplier. The legal basis for the publication of the person 's birth number

in accordance with the provisions of § 9 par. 1 of the Act, the consent of the person concerned could not be

that the operator even had the consent of the person concerned to the disclosure of his birth

numbers. According to § 13 par. 2 second sentence of the law to publish a generally applicable identifier, t. j.

birth number is prohibited. This ban is absolute and cannot be broken even by granting

consent of the person concerned to the publication of his or her birth number. The law does not provide for such an exception.

The operator violated the provision of § 13 par. 2 of the Act when on its website

published the birth number of the person concerned. Operator during personal protection proceedings

data published birth number deleted. The Authority therefore imposed a measure on the operator

to remedy the identified shortcomings and their causes only in the part concerning others

shortcomings identified during the personal data protection proceedings which constituted the breach
obligations to instruct the entitled persons who published data on mandatory disclosures
orders on the operator's website, the obligation to anonymize the birth number
before the publication of the relevant documents.

9.3.2.7 Disclosure of personal data in copies of documents by sending an incorrect one
address

In the first half of 2018, the Office accepted the filing of the affected person against the bank, resp. her
branch, which he evaluated according to the content as a proposal to initiate proceedings on the protection of personal data
data. The petitioner requested a written warrant for her son
an application at a bank branch for changes in the disposition of her son's account, and shall be attached to the application
were copies of documents containing her personal data and the personal data of her son. Draftswoman
subsequently found that her application, including the documents with personal data attached to the application
were sent unjustifiably to another company, which therefore contacted it by telephone for the purpose of
ascertaining the reason for their delivery. A company employee had it during a phone call
announce that the company's documents do not belong and subsequently to the petitioner at her address
returned.

The Office initiated proceedings against the bank regarding the verification of its branch's processing process
personal data of the petitioner and her son. In the present proceedings, the Office called on the bank as well as
the company to which the petitioner's documents were to have been wrongly sent by the bank's branch,
for synergy. The bank processed the personal data of the petitioner and her son as clients in its own
ISOU for the purpose of providing banking services in accordance with a special law. Personal information
the persons concerned were processed at the bank's branch through the bank's employees,
and thus the entitled persons who the bank, as the operator, has demonstrably instructed about the rights
and obligations in the processing of personal data. The authorized persons also confirmed with their signature

that they have been informed of the obligation to protect personal data against misuse or disclosure

unauthorized persons. However, the Office found that when sending a copy of the appellant 's application, including annexes, there was an error by the authorized person of the bank's branch, which in the internal list contacts bank incorrectly traced the delivery address and copies of documents with personal data the appellant and her son were subsequently mistakenly sent to another subsidiary company of the bank, but did not process the personal data of the bank's clients. In connection with the mistake the beneficiary was found in the proceedings that the operator had breached the obligation to protect the personal data of the data subjects processed prior to their unauthorized disclosure in § 19 par. 1 of the Act. Following the findings and proven facts, the Office imposed measures to eliminate the identified deficiencies and the causes of their occurrence.

49

10 REMEDIES AND DECISION-MAKING

Against the decision of the Office in the matter of personal data protection proceedings, against the decision on the imposition of a fine as well as against a decision not to disclose information resp. decision an appeal may be lodged on the non-disclosure of the information - an appeal, whereby the provisions on remedies set out in the Administrative Procedure Code shall apply in the alternative of order. The President of the Office shall decide on the appeals lodged on the basis of recommendations of the Appeals Committee.

In 2017, the President of the Office, as the appellate body, decided on 29 appeals filed against decisions issued in personal data protection proceedings and 8 appeals against decisions imposing a fine. In proceedings on personal data protection, the President of the Office upheld 12 decisions, annulled 15 decisions and referred them back for further proceedings and 2 decisions has changed. In the fine proceedings, it upheld all 8 decisions. In 2017, the President of the Office also decided on one interim measure in the personal data protection procedure, which she confirmed. In 2017, the President of the Office reviewed the out-of-appeal body proceedings 6 final decisions, the reason for initiating an out-of-appeal review proceedings in only two cases where it decided to amend the first-instance decision.

In the period from 01.01.2018 to 24.05.2018 (inclusive), the chairwoman was the first-instance body
the Office, as an appellate body, referred for review and decision of 15 appeals,
whereas by 24.05.2018 it legally decided on five. In personal data protection proceedings
1 appeal was validly decided during this period, which was rejected
and the decision of the first instance body was upheld. The fine was the subject of the present proceedings
period validly decided on 4 appeals, while 3 decisions were confirmed
and 1 changed. During this period, the President of the Office also preliminarily examined one valid one
decision. The grounds for an extraordinary appeal were not identified.
During this period, 1 appeal was lodged against the decision imposing a fine, which was withdrawn.
Decision-making in the second instance also affects the decision-making activity of the Office as a liable person
according to law no. 211/2000 Coll., In which the Office either makes the required information available or
issue a decision not to disclose information resp. decision not to disclose the information
partly. In 2017, the President of the Office received 4 such appeals. In two cases
confirmed the decision of the first instance body and in two cases annulled and returned the decision
for further proceedings. In 2018, in the period defined above, the Office was not in the matter of applications
about the information delivered no decomposition.
50
11 RIGHTS OF THE PERSONS CONCERNED AND THEIR LIMITATIONS
The person concerned is defined by law as a natural person to whom personal data relate to
that it also grants it certain rights in the processing of personal data. Rights of data subjects
belong without distinction to any natural person and are addressed to each operator, as appropriate
to his intermediary.
Upon written request, the person concerned shall have the right, in particular, to access from the operator
to the personal data processed and the right to object to the processing of personal data. The purpose
The provisions of Section 28 of the Act governing the rights of the persons concerned are to be provided to the persons
concerned

in particular, the necessary protection and guarantee them the rights they enjoy as data subjects in the processing their personal data belong. For example, the person concerned has the right to request confirmation whether or not personal data about her are processed, information about the processing of her personal data data in IS in the range of so-called information obligation, information on the source from which the controller has obtained her personal data for processing, a list of her personal data which are destruction of personal data whose purpose of processing has ended and i. The operator is obliged to process the request of the person concerned in writing in law specified 30-day period.

The operator may restrict the right of the data subject (not to comply with his request) only if if it has exercised its right to rectification or liquidation of its incorrect, incomplete or outdated personal data that are being processed and their right to liquidation personal data whose purpose of processing has ended. Limitation of these rights concerned persons is possible only if it follows from a special law or its application would be violated protection of the person concerned or the rights and freedoms of others would be infringed. Restriction the operator is obliged to notify the rights of the person concerned in writing without undue delay the person concerned and the Office.

The Office registers received written notifications of operators about restrictions of rights (non - compliance requests) of the persons concerned. Any notification of a restriction of the rights of the person concerned by the Office examine and assess in relation to whether the operator has restricted the right of the person concerned according to law.

In 2017, the Office registered 262 notifications on the restriction of the rights of data subjects and in 2018 registered 86 notifications of restrictions on the rights of data subjects.

The rights of the persons concerned were most often restricted due to the application of the provisions special laws, such as Act no. 483/2001 Coll. about banks, according to which the bank must keep the data and copies of the client's identity documents for at least five years since the end of the trade. If the persons concerned exercise the right to liquidate their personal

data because, for example, they have ceased to be a bank client and the purpose of the processing has ended, the bank cannot comply with such a request of the data subject and must limit his rights (personal data cannot be destroyed due to the five-year archiving obligation). Affected persons banking institutions most often requested the deletion of personal data on the grounds that clients have duly paid receivables from the bank as an IS operator as well as cancellations all contracts. The persons concerned also request non-contacting the bank, which banks consider as a revocation of the granted consent to the processing of personal data for the purposes of marketing and, in accordance with this applicable requirement, inform the data subject that the appeal consent and take into account the personal data of the data subject for this purpose they will not.

51

The persons concerned also exercised their rights more frequently under the law, who are providers of consumer finance (credit products), installment sales, but also with insurance companies.

52

12 EUROPEAN AND INTERNATIONAL LEGISLATIVE PACKAGE PROTECTION OF PERSONAL DATA

12.1 European level

Following the adoption of Regulation and Directive 2016/680, the European Commission submitted on 10 January 2017 draft of two legislative acts - draft regulation 45/2001 and decision no. 1247/2002 / EC (hereinafter "the Regulation for the Union institutions, bodies, offices and agencies") and the draft Regulation e - privacy in order to ensure compliance with a uniform approach to personal data protection throughout the European Union. These regulations will be lex in relation to the Regulation special.

The Regulation directly contains a provision requiring Regulation 45/2001 to be amended adapted to the principles and rules laid down in the Regulation. On May 23, 2018, representatives

The Council and Parliament have agreed on the text of a regulation for the Union institutions, bodies, offices and agencies and will apply from autumn 2018.

As in the Regulation, the Regulation provides for Union institutions, bodies, offices and agencies several principles to be followed in data processing and several rights guaranteed individuals whose data are collected. In accordance with the Regulation, institutions and others must authorities to ensure that they provide transparent and easily accessible information on how use personal data, and to envisage clear mechanisms for individuals to apply their rights. The new legal instrument also reaffirms, clarifies and strengthens the role responsible persons within each EU institution and the Supervisor. The goal is also an effort to simplify procedures in this area. For the processing of personal data by EU agencies in the field of law enforcement and judicial cooperation (eg Eurojust), the Regulation applies through a separate chapter. The rules in this chapter are in line with Directive 2016/680 on law enforcement. More specific provisions may be laid down in the founding acts of these agencies rules that take into account their specific circumstances. Europol and the European Public Prosecutor's Office are still excluded from this Regulation. By 30 April 2022 at the latest and every five years thereafter The EC shall report to the European Parliament and the Council on the application of this Regulation appropriate legislative proposals are attached if necessary.

The forthcoming e-privacy regulation will cover electronic data processing communications and information related to end-user end-devices.

Electronic communications data means their content, such as the content of private messages, but also metadata, which include e.g. numbers called, websites visited, geographical location, time of the call or message.

The aim of the draft e-privacy regulation is to ensure strict privacy rules for users of electronic communications services and a level playing field market participants. At the same time, an effective e-privacy directive does not reflect changes in the digital environment and is therefore no longer a sufficient tool for regulation in this area. This is, for example, the Internet

over-the-top communication services not covered by the e-privacy directive. Current
the e-privacy directive also does not apply to electronic communications services offered
providers operating over the Internet, even though they offer functionally equivalent
service. However, these providers will fall within the scope of the proposed
e-privacy regulations. Providers of these services will be able to adopt the e-privacy regulation
process data from electronic communications only for exhaustively defined reasons, and only if
this will be necessary for the purpose of fulfilling the services they provide, maintaining the quality of services,
fulfillment of legal obligations or the protection of vital interests. Otherwise they will be able to

service providers to process electronic communications data only with the consent of the terminal
user. The legislative process for the e-privacy regulation is still ongoing.

12.1.1 Article 29 Working Party of Directive 95/46

WP29 established under Article 29 of Directive 95/46. The members of the working group are leading
representatives of the supervisory authorities for personal data protection of the EU and EEA Member States,
EC representative and supervisor.

WP29 (until May 24, 2018)

 is the official advisory body of the EC in the field of personal data protection and the main one
an EU-wide forum;

 issues opinions on EU legal acts and international treaties that concern them
processing of personal data;

 adopts expert opinions and recommendations if situations arise during data processing,
which the national legislation of the EU Member States does not provide for, if any
to infringe the rights of data subjects in the processing of their personal data;

 issues recommendations to national supervisory authorities for the protection of personal data
uniform implementation of the articles of Directive 95/46 and already of the Regulation and the Directive
2016/680.

During the evaluated period, nine specialized subgroups were active within WP29

for the interpretation of key institutes and definitions (Key Provisions), specifically a subgroup for:

 coordination of activities of individual subgroups (Future of Privacy),

 cooperation between the supervisory authorities of the European Union and international cooperation

(Cooperation),

 issues related to new technologies and technical aspects of processing

(Technology),

 transfer of personal data to third countries (International Transfers),

 processing of personal data for the purposes of border and public order protection (Borders,

Travel and Law Enforcement),

 processing of personal data by financial institutions (Financial Matters),

 processing of personal data in the public sector (E-government),

 Enforcement cooperation.

Prior to the entry into force of the Regulation, a new group dealing with social media was set up

(Social Media Working Group), the creation of which was conditioned by a significant increase in infringements

protection of personal data by social media.

The role of these subgroups is to prepare opinions and working documents for each

areas of personal data processing. The Office actively participated in the meetings of the first five

the above subgroups; he participated in the activities of the remaining subgroups by sending written papers

documents or by written procedure.

During the period under review, WP29 adopted documents, guidelines, which were to help not only

supervisory authorities, but also operators and intermediaries in preparation for the Regulation

and Directive 2016/680; for example:

 Guidelines on reporting personal data breaches under the Regulation;

 Guidance on consent under the Regulation;

 Guidelines on the right to data portability;

Transparency Guidelines under the Regulation;

Guidelines for responsible persons;

Guidance on data protection impact assessment and determining whether

for the purposes of the Regulation, processing "is likely to lead to high risk";

Guidelines on the use and setting of administrative penalties for

Regulations and more.

7 WP29 plenary sessions were held during the period under review. The Office is in the evaluated

participated in 2 plenary sessions.

12.1.2 Committee set up under Article 31 of Directive 95/46

The Committee 31 for the Protection of Individuals with regard to the Processing of Personal Data is set up under

Art. 31 of Directive 95/46. The Committee is an advisory body to the EC and is composed of representatives of the Member

States

EU countries. Its function is to assist the EC in implementing its measures. Committee 31 shall approve or

gives reservations on draft EC documents, in particular those related to them

with cross-border transfer of personal data. Committee 31 shall meet on an ad hoc basis,

usually once a year. The committee did not meet during the period under review.

12.1.3 European Data Protection Supervisor

The Supervisor is an independent EU data protection authority established by Regulation 45/2001.

The role of the Supervisor is

 monitoring and ensuring the protection of personal data and privacy when institutions

and EU institutions process personal data of individuals

 advisory work for the EU institutions and bodies on all matters concerning

processing of personal information,

 monitoring new technologies that may affect the protection of personal data;

the possibility of referring the matter to the Court of Justice under the conditions laid down in the Treaty

European Communities,

 the possibility of intervening in actions brought before the Court of Justice of the European Communities;

 cooperation with national supervisory authorities and other supervisory authorities with a view to

improve consistency in privacy and more.

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

data protection authorities and supervisors. In order to ensure high

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

official in the coordination of supervision.

The following IT systems are currently subject to this oversight model:

• Eurodac,

• Visa Information System (VIS),

• Schengen Information System (SIS),

• Customs Information System (CIS),

• Internal Market Information System (IMI).

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

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

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

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

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

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

did not attend these meetings.

12.2 International level

12.2.1 Convention Consultative Committee 108

The Consultative Committee established by the Council of Europe on Convention 108 is composed of representatives Contracting Parties to the Convention, supplemented by observers from other States (Members or non-members) and international organizations; is responsible for interpreting the provisions and for improving the implementation of Convention 108 and for drawing up reports, guidelines and guidelines in areas such as contractual provisions governing protection data in the transfer of personal data to third parties which did not guarantee an adequate level data protection or data protection with regard to biometrics.

12.2.2 Council of Europe Ad Hoc Committee on Personal Data Protection (CAHDATA)

Ad hoc Committee established by the Council of Europe in 2013, as an ad hoc committee on the protection of individuals the purpose of which was to end the discussion on the modernization of Convention 108 and to final proposal of the Committee of Ministers.

Three plenary sessions of the committee took place during the period under review. The Office attended two plenary sessions. The last, third plenary session approved the modernization proposal Convention 108, which has now been submitted to the Committee of Ministers of the Council of Europe for approval. The modernization of Convention 108 took place simultaneously on EU soil as well as on soil Council of Europe. As for the Slovak Republic, the Ministry was also involved in the modernization of the Interior of the Slovak Republic, Ministry of Foreign Affairs and European Affairs Of the Slovak Republic and the Office.

The Office participated in the modernization through continuous comment fulfillment also play a role vis-à-vis the EU in the framework of the Permanent Representation of its delegates in Brussels, as well as vis-à-vis the Council Europe in the framework of the Permanent Representation of its delegates in Strasbourg. The Office assessed the consistency of the text Convention 108 with the forthcoming new Slovak legislation under the law

no. 18/2018, as well as compliance with the Regulation.

The three-year effort to modernize Convention 108 resulted in the adoption of the Protocol

Committee of Ministers of the Council of Europe at its 128th session. The adoption of this Protocol was a process

modernization of Convention 108 was completed and the Protocol was submitted on 15-16 June 2018

Parliamentary Assembly of the Council of Europe. This Protocol shall be open for signature at

October 10, 2018 in Strasbourg.

12.3 Law enforcement agencies

Due to the deepening of mutual cooperation and exchange of information between the active authorities

several specific institutions have been set up at EU level in criminal proceedings. The basis for

their establishment was mainly international legal instruments such as the Europol Convention, the Convention

on the Schengen Information System, Convention on the use of information technology at

customs purposes and others.

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

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

supervisory coordination set up by the supervisor.

Representatives of the Office represented the Slovak Republic in joint supervisory bodies

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

Visa Information System (SCG VIS), Customs Information System (JSA Custom, SCG CIS),

Europol (JSB Europol), Eurodac (SCG Eurodac).

12.3.1 Europol Joint Supervisory Body (Europol JSB)

Europol was established by Council Decision No 2009/371 / JHA in order to provide assistance

and support the competent authorities of the Member States and facilitate their cooperation in

prevention of organized crime, terrorism and other forms of serious crime

activities involving two or more Member States and in combating such forms

crime. Council Decision No 2009/371 / JHA replaced the Convention establishing the European

police authority established on the basis of Article 3 of the Treaty on European Union. From May 1
2017, the new Europol Regulation no. 2016/794.

In order to ensure the supervision of the processing of personal data by Europol,
Article 34 of Council Decision no. 2009/371 / JHA on the establishment of a European Police Office
the Joint Supervisory Body (JSB Europol). In order to establish a joint supervisory body
was to provide a platform for cooperation between Member States' supervisory authorities,
communication and coordination of their activities. The Joint Supervisory Body shall be responsible for matters
concerning the performance and interpretation of Europol's processing activities
and the use of personal data, in matters relating to controls carried out independently
national supervisory authorities of the Member States or the exercise of the right of access
and on issues related to the development of harmonized proposals for common solutions
existing problems.

During the period under review, the Office participated in a total of three meetings at which they were discussed
Europol issues. Since the entry into force of the new Europol Regulation, the so-called
Cooperation Board and in April 2017 the last meeting of the supervisory body over
Europol. During this Europol JSB meeting, the following topics were discussed: inspection report,
a report on the transfer of knowledge to the new supervisory authority and an exchange of experience concerning
trafficking in human beings.

The processing of applications was discussed within the Europol Joint Supervisory Body
citizens in exercising their rights, deciding that the persons concerned may be contacted
directly by the Supervisor and he is able to process applications in all languages.

Europol's representatives submitted their comments and suggestions on the revision of Regulation 45/2001,
noting in particular that some Europol operations could become illegal.

12.3.2 Joint Supervisory Body of the Customs Information System

The Office also oversees the CIS. The legal basis for the CIS, laid down in particular in Council Regulation (EC)
no. 515/1997 was amended in 2015 by Regulation (EU) of the European Parliament and of the Council

2015/1525. Relevant changes include data retention periods (5 years plus 2 years

57

instead of an annual review of up to 10 years) and the introduction of the option

limit the visibility of new cases to the competent authorities of selected Member States.

The Office is part of the Joint Supervisory Body CIS ("JSA Customs"), which was established

on the basis of Art. 18 of the Convention on the use of information technology for customs purposes as an institution

authorized to supervise the processing of personal data in the CIS. The role of JSA Customs is

in particular the monitoring and application of the provisions of personal data protection legislation,

examining problems which may arise in the operation of the CIS, drawing up proposals for

joint problem-solving as well as opinions on the adequacy of personal data protection measures

data.

The Supervisory Coordination Group is also active in the area of CIS protection

over the Customs Information System (SCG CIS). It is made up of representatives of JSA Customs

and the Supervisor. In order to promote good cooperation with JSA Customs for Customs

its chairman is usually elected chairman of the CIS oversight coordination group, as

it is still the case today. Working meetings of both subgroups are usually coordinated and follow-up

one on top of the other.

One SCG CIS meeting took place in 2017; the content was a presentation on

to-do list and a common framework for controls. He participated in the preparation of the to-do list

and the office.

12.3.3 SCG SIS II Supervision Coordination Working Group

Schengen Information System II, established by Council Decision 2007/533 / JHA

allows members of the designated security forces of the Member States to access

to data on searches for persons and objects that have entered the Schengen Information System

imposed by any Member State and, in specific cases, adequately

records respond.

Schengen Information System II Surveillance Coordination Working Group II (SCG SIS

II) belongs to a group of working groups set up by the Supervisor. Intention

is subject to the supervision of the protection of personal data processed by the European institutions

responsible authority, ie the supervisory officer.

The SCG SIS II was established in accordance with Article 46 of the Regulation of the European Parliament and of the Council

1987/2006 of 20 December 2006 on the establishment, operation and use of the Schengen acquis

second generation information system (SIS II) and Article 62 of Council Decision 2007/533 / JHA

of 12 June 2007 on the establishment, operation and use of the second Schengen Information System

generation (SIS II). SSG SIS II met twice during the period under review. The subject of the meeting

were, in particular, new proposals for the Schengen Information System II, recommendations,

issues of logging and interoperability of systems, as well as the election of a new President and Vice-President,

Schengen Information System II report and national alert criteria.

12.3.4 Visa Coordination Coordination Working Group for the Visa Information System

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

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

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

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

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

Supervision

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

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

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

with Regulation 1987/2006, and whether it also carries out regular audits of personal processing activities

data.

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

at national level. The SCG VIS was set up in accordance with Article 43 of Regulation (EC) No
Parliament and of the Council 767/2008 of 9 July 2008 concerning the Visa Information System (VIS)
and the exchange of data between Member States on short stay-visas (VIS Regulation).
During the period under review, the Office participated in two SCG VIS meetings.
An implementation report was presented at the first SCG VIS meeting
Art. 41 of the VIS Regulation, which governs the supervision of the VIS. The message was sent to everyone
members of the Schengen area, reflecting the experience of the supervisory authorities
Member States with controls at national level. The second meeting of the SCG VIS was focused on
in particular to discuss with the Commission and eu-LISA on current developments, security training
and data protection for the staff of those authorities which have access to the VIS, an activity report
VIS group for the years 2015-2016.

12.3.5 Eurodac Supervisory Coordination Working Group

Eurodac was established by Council Regulation (EC) No 2725/2000, which concerns the establishment
the "Eurodac" fingerprint comparison system for the effective application of the Dublin
Convention, but in 2013 a Regulation of the European Parliament and of the Council (EU) was
no. 603/2013 on the establishment of Eurodac for the comparison of fingerprints with effect
repealed the original 2000 Regulation as of 20 July 2015. Pursuant to this Regulation 603/2013
The purpose of the system, which has been in operation since January 2003, is to assist EU Member States in
determining which Member State should be responsible for examining a particular application for asylum.
Meetings of the Eurodac SKD are in charge of the Supervisor, who also according to the Regulation
45/2001 supervises the central part of the system and coordinates the activities of national ones
supervisory authorities.
During the period under review, the Authority participated in two SCG Eurodac meetings. At the first meeting
the Commission's presentation on Eurodac 2016 was presented and the Vice-President was elected
groups. The second session focused on current developments (presentation and discussion
with eu-LISA), draft questionnaire on the rights of data subjects, deletion of alerts in the system

Eurodac, a special search in Eurodac, access options for group members

information as well as issues related to the development of the situation at national levels.

12.3.6 Supervisory Coordination Working Group for the Internal Market Information System

The purpose of the Supervisory Coordination Working Group for the Internal Market Information System (hereinafter only “SKD IMI”) is the coordination and supervision of the processing of personal data in the IS for internal market. This processing is carried out on the basis of Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49 / EC. Regulation 2012/1024 allows for an exchange

information in administrative areas, such as the recognition of professional qualifications, or in exercising patients ’rights in cross-border healthcare.

12.3.7 European Commission Expert Working Group on Regulation and Directive 2016/680

The expert group set up by the EC on the Regulation and Directive 2016/680 was established in the second mid-2016 in order to assist the EC in the implementation of newly adopted legal acts EU. In the context of the Regulation, the agenda of the subgroup focuses on clarifying the conditions as possible at national level in the framework of personal data protection legislation to achieve an effective and uniform application of the Regulation. Regarding the implementation of the Directive 2016/680, the work of the group is aimed at ensuring a high level of implementation protection of the rights of individuals with regard to the processing of personal data for the purpose of criminal proceedings, uninterrupted data exchange and effective police and judicial cooperation.

The members of the expert working group are experts from EU Member States as well as country representatives EEA (Iceland, Liechtenstein, Norway) and Switzerland. This platform enables efficient exchange of information between Member States on ongoing legislative changes with the application of the Regulation and provides a space for sharing experience with the solution individual legal issues.

The expert working group met 10 times in the evaluated period. The Office participated in 2 meetings.

The Office participated in the work of the expert group by participating in meetings devoted to the topic Regulation applications. The agenda of the meetings focused mainly on the issue preparation of the application of the Regulation, conditions applicable to the consent of the child in connection with information society services, processing of personal data relating to the admission of guilt for criminal offenses and offenses, notification of personal data breaches, processing personal data in the framework of activities outside the scope of EU law, restrictions on rights the person concerned and others.

13 INTERNATIONAL MEETINGS WITH PARTNER BODIES SUPERVISION

13.1 Meeting of representatives of supervisory authorities for personal data protection Vyšehrad group

In March 2017, a Meeting of Representatives of the Supervisory Authorities for Protection was held in Cracow personal data of the Visegrad Group. It was the second meeting in a row.

The subject of the meeting was mutual information on the current state of the legislative process implementation of the Regulation, reorganization of supervisory authorities in connection with the application Regulations and there was also a detailed discussion on specific issues related to the selected the institutes of the Regulation. A conference organized by the Polish side was also discussed due to a public debate on the independence of the supervisor Polish professional and political public. The issues were also discussed together supervisory action, issues of practical solutions in reporting breaches of protection as well as the choice of data protection impact assessment methodology (eg use of ISO standards). The meeting also included a seminar on the practical implementation of cooperation between supervisory authorities.

13.2 II. International Conference of Municipal Police of the Visegrad Four

In Brno in May 2017 II. International Conference of Vyšehrad Municipal Police

fours. A representative of the Office spoke on the new Data Protection Regulation in context

cyber security. The conference focused on data protection issues

and the duties of the Municipal Police in relation to the protection of the state's cyberspace.

13.3 E-Volution of Data Protection Conference

In September 2017, the E-Volution of Data Protection Conference took place in Estonia. The entire

the conference was held in the spirit of the Regulation. On the protection and balancing of fundamental human rights

therefore, the reform of personal data protection in Europe, as well as the ruling of the Court of Justice, are also worthwhile

European Union. The court even assessed the application for the first time from a personal data protection perspective

EU-Canada PNR international agreement (Directive of the European Parliament and of the

(EU) 2016/681 of 27 April 2016 on the use of Passenger Name Record (PNR) data for purposes

prevention, detection, investigation and prosecution of terrorist offenses and serious

crime).

13.4 Bilateral meeting with representatives of the Japanese supervisory authority

At the beginning of December 2017, the Office welcomed representatives from Personal Information Protection

Commission of Japan (hereinafter referred to as "the Commission"). The main purpose of the meeting was to inform

representatives of the Office's activities and activities and to provide them with information on the proceedings

and inspections carried out by the Office, as the commission set up in January 2016 is authorized

exercise control over private sector businesses

in Japan. Personal data protection supervision has so far been divided and managed in Japan

16 relevant ministries, but is currently centralized to the commission along with the full

enforcing the amended Personal Data Protection Act of May this year.

13.5 IT between paragraphs

An inter-paragraph IT conference was held in Prague in February and October 2017 and in April 2018.

The conference in February 2017 focused on the protection of personal data in the light

Regulations in the IT environment, on the subject of a single digital Europe and the directive on payments

services. The conference provided a comprehensive view of the issue of personal data protection
and data management in the IT environment, with an emphasis on design solutions for implementation and procedures
whether in the field of law, technology, including practical demonstrations.
The conference in October 2017 focused on the area of personal data protection in context
Regulations in the IT environment, on the topic
practical implications of the new legislation
to the business environment.
The conference in April 2018 focused on the national regulation of the Czech Republic in the field of protection
personal data, in particular the rights of data subjects and the effects of the Regulation on internal processes
controller and the related personal data protection policy.

13.6 QuBit Conference

In April 2017 and April 2018, the QuBit conference was held in Prague. The conference in 2017 was
focused primarily on cyber security and was attended by 175 security
cybersecurity experts from 21 countries around the world. Conference
in April 2018 it focused on cyber security, on new cyber attacks,
options for defense and private sector practices, applying the latest knowledge in this field
areas in the development of new technologies. A representative of the Office led a workshop on GDPR in practice.
The workshop focused on the practical application of the impact assessment that was presented at
documents of the decree on the procedure for impact assessment, which is the responsibility of the Office.

13.7 III. International Conference of Municipal Police

In April 2018, the III. International Conference of Municipal Police.
A representative of the Office also spoke at the conference on "New legislation in the field of protection
personal data / selected aspects ". The conference was focused on building cooperation
between institutions and commercial entities, promoting meetings and exchanges of experience between
representatives of municipal and city police, representatives of state administration and local governments,
partner organizations, the integrated rescue system and academia.

ASSESSMENT OF THE PROTECTION STATUS OF PERSONAL PROTECTION

IN THE PERIOD FROM 1 JANUARY 2017 TO MAY 24, 2018

DATA

In the period under review, the interest in the protection of personal data can be assessed as more than positive, mainly due to the approaching deadline for the application of the Regulation and the law no. 18/2018 Coll. For this reason, both operators, intermediaries and the general public and the professional public were much more interested in this issue.

Regarding information and awareness of the general public about personal data and their protection to see a drastic shift towards informing the general public; people are interested in their personal data, protect them and operators ask how and why their personal data process. This trend is also confirmed by the operators, who also in various common forums and platforms inform participants on behalf of the Office that they are increasingly confronted with people's questions and that they must be able to justify on the basis of which they process the person's personal data.

People are much more aware of their rights and are not afraid to demand their fulfillment in practice.

Personal data is becoming an important business item and is the focus of many companies, the more care must be taken to ensure their rigorous protection and lawful processing.

From these findings, the following can be formulated for some sectors and areas of life recommendations:

Parents and children as affected persons

Children and their personal data are increasingly coming to the forefront of companies' interests, and with that hand in hand in the digital age and the processing of their personal data, it is therefore extremely important already in the family, before starting school, the children were guided by their parents to take care of protection their personal data so as not to provide information about themselves and their parents or siblings to someone they don't know. Until a child enters school, the parent is primarily the one who the child is can and should learn the right habits, not only to be able to ask and thank, but also to

knew that his data were his and that a stranger has no right to require them to know

that he can turn to his parents in this area of life as well, so that he knows how to deal with such a situation

preserve.

School

Children spend a lot of time at school, school is their second home, it is essential that they also go to school

children also received information on the protection of personal data in various subjects, about what kind

may have consequences if they recklessly provide personal data. It is necessary to make this

more attention was paid to the issue within appropriately selected subjects.

Development and research

The protection of personal data is gradually reaching all areas of life, it is no longer just about

that the person provides his personal data to the bank, school, office. Privacy has

be in the spotlight the moment we download a mobile application to our phone when

we decide to use smart technologies available to individuals at home

elements of the household, but for the household as a whole, when we decide to have a smart watch,

in which we enter data about our health. The protection of personal data is gradually overlapping

many activities of everyday life, so it is also appropriate for companies to take action

followed the principles of privacy by design and privacy by default when developing applications and programs.

On the other hand, it is also up to smart technology users as they let them steal

privacy, or whether they make an effort and read the terms of personal data processing before

by entering them into the application.