REPUBLIC OF BULGARIA

COMMISSION FOR PERSONAL DATA PROTECTION

ANNUAL ACTIVITY REPORT

of the Commission for Personal Data Protection

for 2018

pursuant to Article 7(6) of the Personal Data Protection Act

TABLE OF CONTENTS

List of the Acronyms Used in This Document

PDC	–	Personal data controller
APC	–	Administrative Procedure Code
SAA	–	Social Assistance Agency
SCAC	–	Sofia City Administrative Court
SEAV	–	Statement establishing an administrative violation
BACR	–	Bulgarian Association of Clinical Research
SAC	–	Supreme Administrative Code
SJC	–	Supreme Judicial Council
SACP	–	State Agency for Child Protection
Directive 95/46/EC	–	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Directive (EU) 2016/680	–	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
Directive (EU) 2016/681	–	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
DPO	–	Data protection officer
PIN	–	Personal Identification Number
EDPB	–	European Data Protection Board
EDPS	–	European Data Protection Supervisor
eRALD	–	CPDP's electronic system for registration of personal data controllers

AVP Act	–	Administrative Violations and Penalties Act
CReg Act	–	Civil Registration Act
API Act	–	Access to Public Information Act
EC Act	–	Electronic Communications Act
Health Act	–	Health Act
PDP Act	–	Personal Data Protection Act
HI Act	–	Health Insurance Act
AASPDP Act	–	Act Amending and Supplementing the Personal Data Protection Act
MoI Act	–	Ministry of Interior Act
CI	–	Compulsory instruction
CCFIAA Act	–	Counter-Corruption and Forfeiture of Illegally Acquired Assets Act
JS Act	–	Judicial System Act
PEA Act	–	Private Enforcement Agents Act
SJC Inspectorate	–	Inspectorate with the Supreme Judicial Council
IMIS	–	Internal Market Information System
QES	–	Qualified electronic signature
CPDP	–	Commission for Personal Data Protection
CCFIAA Commission	–	Counter-Corruption and Forfeiture of Illegally Acquired Assets Commission
CRC	–	Communications Regulation Commission
MoI	–	Ministry of Interior
MFA	–	Ministry of Foreign Affairs
MoES	–	Ministry of Education and Science
MoRDPW	–	Ministry of Regional Development and Public Works
SME	–	Small and medium-sized enterprise
MoTITC	–	Ministry of Transport, Information Technology and Communications
NRA	–	National Revenue Agency

NDB ‘Population’	–	National Database ‘Population’
NHIF	–	National Health Insurance Fund
ME Ordinance	–	Ordinance on Medical Expertise
PD	–	Penal decree
CrPC	–	Criminal Procedure Code
DP	–	Data Processor
RAC	–	Rules of Administration in the Courts
RACPDPA	–	Rules on the activity of the CPDP and its administration
PR Brussels	–	Permanent Representation of the Republic of Bulgaria to the EU in Brussels
PORB	–	Prosecutor’s Office of the Republic of Bulgaria
RSAD	–	Regional Social Assistance Directorate
Regulation (EU) 2016/679	–	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
NP	–	Natural Person
LE	–	Legal Entity

I. Introduction

This Annual Report of the Commission for Personal Data Protection (CPDP) is drawn up in accordance with Article 7(6) of the Personal Data Protection Act (PDP Act) and covers the period from 1 January 2018 to 31 December 2018.

This report contains information on the main directions of the CPDP activity during the period mentioned above. The fact that a new legal framework in the area of personal data protection is in place in the European Union since 25 May 2018 led to a change in the Commission's individual activities. These changes are discussed in this report to the National Assembly of the Republic of Bulgaria. Special attention is paid to the activities of the Bulgarian Presidency of the Council of the EU and to the conduct of a national information and awareness campaign covering the new European legal framework in the area of personal data protection. The report presents summarised information on issues raised by citizens' inquiries or as a result of the consultations conducted by the CPDP. The degree of achievement of the objectives and priorities set for year 2018 is analysed and the administrative capacity and financial position of the CPDP are reported.

II. ANALYSIS OF AND REPORT ON THE DEGREE OF ACHIEVEMENT OF THE OBJECTIVES AND PRIORITIES OF THE CPDP SET IN THE 2017 ANNUAL REPORT AND OF THE CPDP STRATEGY FOR DEVELOPMENT IN THE FIELD OF PERSONAL DATA PROTECTION (HORIZON 2022)

Year 2018 was characterised by two significant challenges facing the CPDP which it successfully managed: the first **Bulgarian Presidency of the Council of the European Union** and the launch of the **practical implementation of the new legal framework in the field of personal data protection**, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Regulation (EU) 2016/679, General Data Protection Regulation).

The participation of the CPDP in the first Bulgarian Presidency of the Council of the EU in 2018 can be assessed as extremely successful. First of all, all legislative dossiers taken over from the previous Estonian Presidency were closed successfully and in a timely manner despite the political, legal and practical difficulties. Secondly, through the CPDP team, Bulgaria gained the considerable respect and trust of the European Commission, the European Parliament, the General Secretariat of the Council, Eurojust, Europol and Frontex, as well as of the other Member States. Last, but not least, during the Presidency the CPDP representatives acquired significant professional experience which will contribute to the development of the Commission internationally and to the professional development of its experts.

On 25 May 2018, Regulation (EU) 2016/679 (the General Data Protection Regulation) entered into force. The uniform application of these rules in Europe is the most significant reform in the area of personal data and privacy in the past two decades. When preparing the information and awareness campaign, the CPDP took into account the horizontal nature of the reform that covers both the public and the private sector (over 350 000 personal data controllers) and the need for a broad information and awareness campaign in an accessible language. Taking into account the profundity of the changes and the complexity of the matter, despite its limited financial and human resources during the reporting period the CPDP organised over 60 separate events with over 6 000 participants from the public and private sectors, the academia and the non-governmental sector.

In addition, the CPDP prepared two information brochures aimed at clarifying key issues to support the implementation of the General Data Protection Regulation. The brochures' titles were

‘**10 practical steps for implementing the General Data Protection Regulation**’ and ‘**Practical Issues relating to Personal Data Protection after 25 May 2018**’. The brochures were printed in 24 000 copies and copies were sent to all ministries and agencies. They were published on the institutional website of CPDP and distributed both in the CPDP building and at events in which the CPDP participated, as well as through the assistance of public and industry organisations.

In order to raise public awareness of key issues of the General Data Protection Regulation, a special section devoted to the Regulation was created on the institution’s website. Explanatory materials and recommendations on the implementation of the Regulation were published there: guidelines of the CPDP, of the European Commission, of the Working Party under Article 29 of Directive 95/46 (whose successor is the European Data Protection Board established by said Regulation). In order to facilitate the fulfilment of the obligation of personal data controllers (PDCs) and data processors (DPs) to designate a data protection officer (DPO), the CPDP published on its website instructions on the manner and form of notification of designated DPOs to the CPDP.

The CPDP’s efforts for developing a national training centre in the field of personal data protection continued in 2018. Unfortunately, the Commission did not receive the financial support required by the end of the reporting period and this was an objective obstacle to the implementation of the initiative.

During the reporting period, together with the Ministry of the Interior, the CPDP initiated the process of public discussion of the draft Act Amending and Supplementing the Personal Data Protection Act (AASPDP Act) in order to introduce measures for the implementation of Regulation (EU) 2016/679 and to transpose Directive 2016/680 in national law. At the end of 2018 CPDP representatives participated actively in a working group with the Committee on the Internal Security and Public Order at the National Assembly to finalise the draft Act and reach a reasonable compromise on its texts with relevant stakeholders.

In addition to the successful presidency of the Council of the EU, the international activity of the CPDP continued and increased at different levels in 2018. The fact that the Chairperson of the CPDP Mr Ventsislav Karadjov was elected as the President of the newly established European Data Protection Board (EDPB) — a completely new body of the EU with legal personality and broad powers — for the next five years is compelling evidence of the reputation on the Bulgarian data protection supervisor.

Following intensive preparations completed entirely by the Bulgarian supervisory authority, in October 2018 the CPDP hosted a series of events within the 40th International Conference of

Data Protection and Privacy Commissioners. In parallel with the events in Brussels, more than 200 delegates and 50 moderators and lecturers from many Bulgarian, European and international institutions as well as from leading national and foreign companies participated in the plenary discussions and accompanying seminars in Sofia. A specific aspect of the forum in Sofia was the increased attention devoted to the data protection supervisors of the Western Balkan countries and the Commonwealth of Independent States (CIS) as part of the CPDP's policy to provide assistance and share experience.

The work of the CPDP aimed at contributing to the achievement of the strategic goal of full accession of the Republic of Bulgaria to the Schengen area continued in 2018. Taking into account the fact that the process is largely political, CPDP representatives continued to participate in Schengen evaluation missions, including in the capacity as leading experts, thus further strengthening the reputation of Bulgaria in the field of personal data protection. The information bulletin issued by the CPDP reported regularly on the participation of CPDP representatives in Schengen evaluation missions.

In pursuance of the requirements of Regulation (EU) 2016/679 of the European Union and of the Council, in 2018 the Commission created the organisation required and developed the information system that maintains the following registers:

- Register of personal data controllers and processors which have designated data protection officers;
- Register of accredited certifying bodies;
- Register of approved codes of conduct;
- Register of infringements of Regulation 2016/679 and of the law, as well as of the measures taken in pursuance of the exercising of corrective powers (Register of infringements and the measures taken).

The significant change in the legal framework in the field of personal data protection and the protection of individuals with regard to the processing of their personal data after 25 May 2018 affected and impeded significantly the implementation of the goals and priorities set for 2018 regarding the control activities of the CPDP. Regardless of the direct applicability of Regulation (EU) 2016/679, an up-to-date and comprehensive national legal framework was not yet available in 2018 and internal CPDP instruments regulating control activities were not in place. Nevertheless, by prioritising certain tasks and competencies of the CPDP under the new European legislation, a

‘Methodology for the actions to be taken by the CPDP in cases of receiving notifications of personal data breaches in accordance with Article 33 of Regulation (EU) 2016/679’ was developed during the reporting period.

In 2017, the CPDP developed and adopted a Strategy for Development in the Field of Personal Data Protection (Horizon 2022). The Strategy is in line with the new EU legal framework for personal data protection (Regulation (EU) 2016/679, Directive (EU) 2016/680 and Directive (EU) 2016/681), as well as with fundamental initiatives at national level – National Reform Programme ‘Bulgaria 2020’ and Strategy for the Development of the Public Administration (2014–2020). The availability of a strategic document enables a sustainable development in the area of personal data protection. The Strategy underlies the Commission’s long-term operation. Its development has also taken into account the experience accumulated by the CPDP over 15 years, the possibilities for further development as well as the main challenge for the protection of personal data — the creation of a digital environment and the functioning of the digital society.

The Strategy contains an analysis of the current condition in the sector and elaborates on the results achieved, the strengths and weaknesses to date, describes the opportunities for development and the threats and risks in the sector. The strategic goals for the period 2017–2022 and the targeted policies of the CPDP are defined.

The strategic goals of the CPDP for the 2017–2022 period include:

– system implemented for the prevention and containment of the unlawful forms of personal data processing and violations of natural persons’ rights;

– supervision mechanism effectively applied;

– comprehensive system in place for training in personal data protection, public awareness raising events and initiatives;

– sustainable administrative services provided to citizens and data controllers;

– proactive approach applied to international cooperation;

– system of initiatives in place for upgrading the professional qualification of the CPDP and its administration;

– advanced openness and transparency processes.

For the attainment of its strategic objectives, the CPDP has endorsed a set of policies which comply with European standards and good practices:

– European coherence policy;

– Quality management policy;

– Prevention policy;

– Control and accountability policy;

– Partnership policy;

– Publicity and inclusion policy;

– Accessibility policy;

– Monitoring policy;

– Sustainable-development and management-of-change policy.

The Strategy contains a performance monitoring and evaluation mechanism. The purpose of this mechanism is to initiate corrective action so that the expected results and strategic objectives can be achieved as effectively as possible.

In pursuance of the Strategy, the individual work plans of the officials in the administration for 2018 took into account the strategic goals and specific objectives set out in the annual work plans of the administrative units that correspond to the tasks set out in the Action Plan for the Implementation of the Strategy, including specific actions, indicators and officials responsible for their implementation.

The full text of the Strategy ‘Horizon 2020’ and of the Action Plan for its implementation are accessible on the CPDP website.

III. CPDP ACTIVITIES THAT ARE NO LONGER CARRIED OUT AS OF THE EFFECTIVE DATE OF REGULATION (EU) 2016/679 (25 MAY 2018)

1. Registration of Personal Data Controllers and of Registers of Personal Data Maintained Thereby

The implementation of Regulation (EU) 2016/679 removed the basis for registration of personal data controllers (PDCs). In this connection, as of 25 May 2018, the CPDP suspended all proceedings initiated in accordance with Chapter 3 of the PDP Act and not completed by 25 May 2018, such as:

- registering PDCs in the register referred to in Article 10(1)(2) of the PDP Act;
- exemption from the registration requirement;
- deregistering PDCs from the register referred to in Article 10(1)(2) of the PDP Act, including all assigned and unfinished preliminary inspections in accordance with Article 17b of the PDP Act.

During the period from 1 January to 25 May 2018, 5 997 user profiles of PDCs were created in the electronic system for registration of PDCs (eRALD). Of these, 5 767 were profiles of PDCs requesting entry in the register referred to in Article 10(1)(2) of the PDP Act and 230 were profiles of PDCs wishing to be exempted from registration in this register.

Between the inception of eRALD in 2009 and 25 May 2018, the total number of system users was 377 044, of which 345 082 applied for PDC registration and 31 959 requested an exemption from the registration requirement (Figure 1).

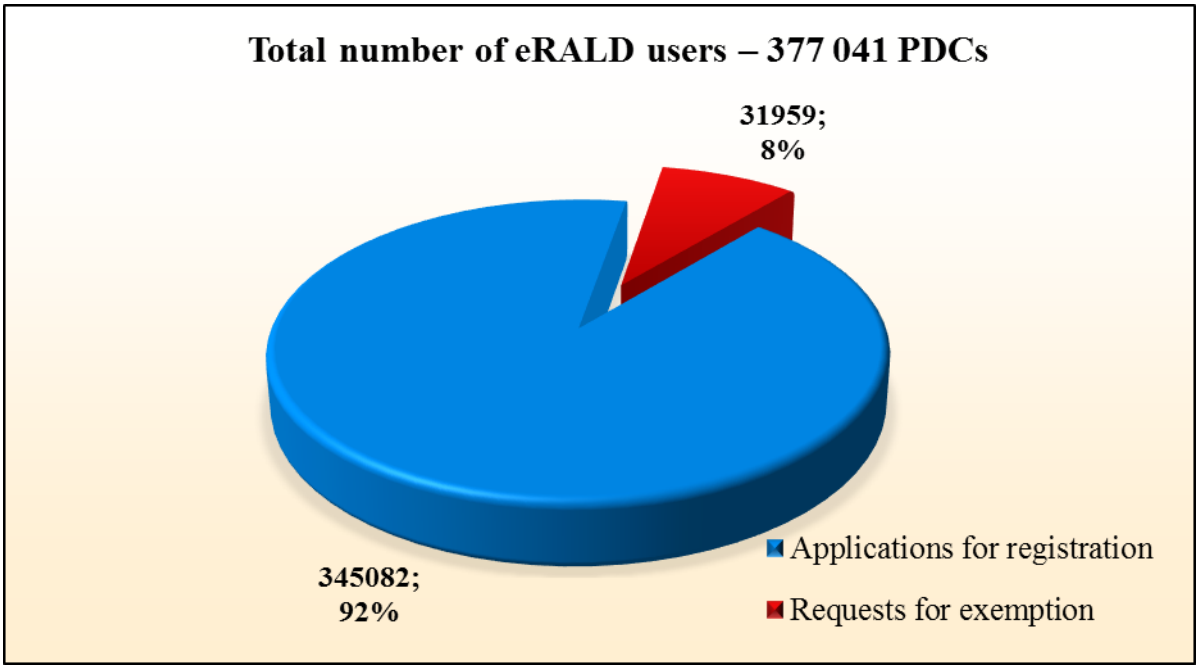

Figure 1

During the period from 1 January to 25 May 2018 the CPDP registered 4 327 new PDCs. Thus, the overall number of registered PDCs became 297 751 (Figure 2).

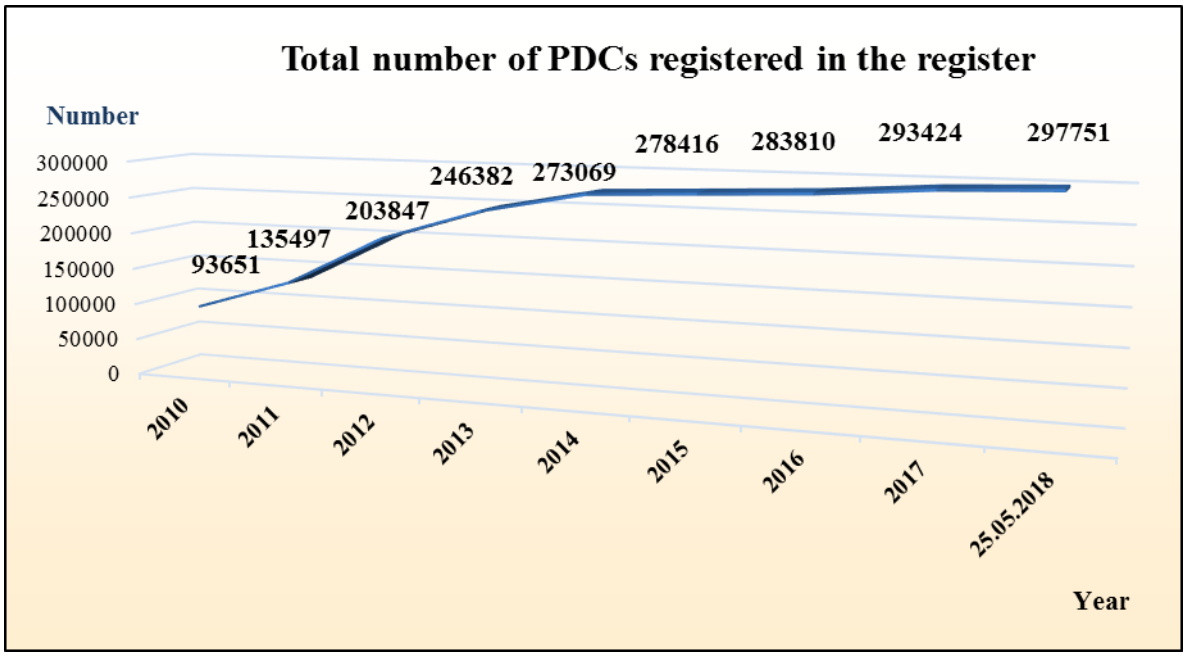

Figure 2

During the reporting period the CPDP exempted from the obligation to register 177 PDCs, whereby the total number of PDCs exempted from that obligation as of 25 May 2018 reached 28 641 (Figure 3).

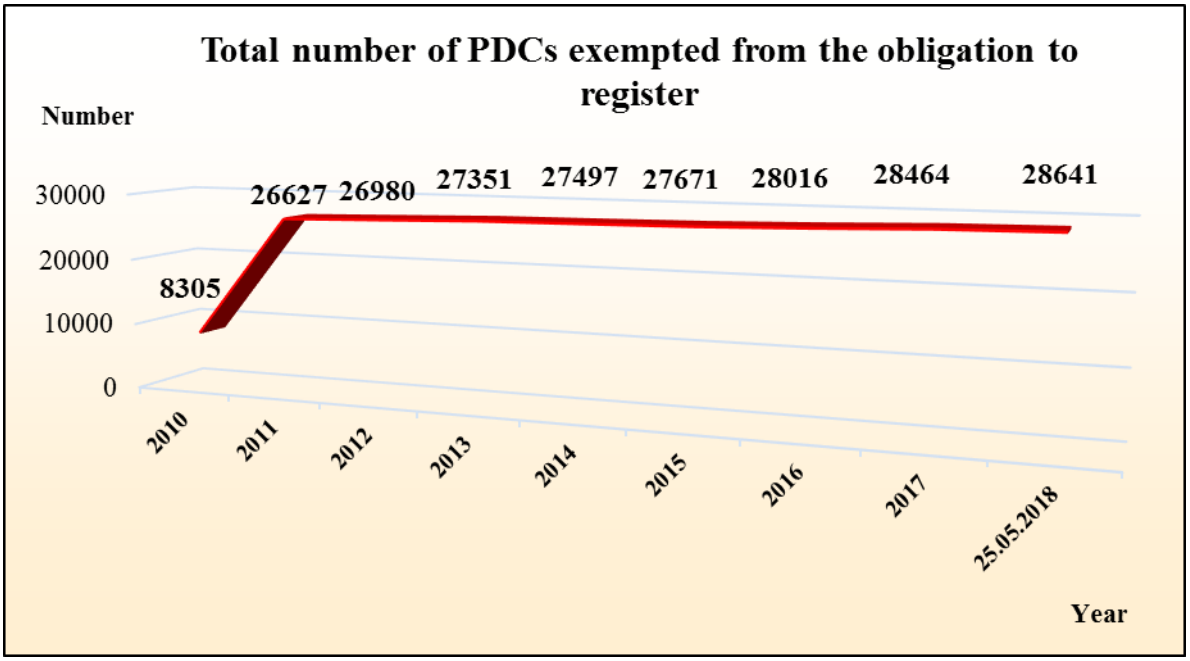

Figure 3

Between 1 January and 25 May 2018 the CPDP deregistered from the register referred to in Article 10(1)(2) of the PDP Act 27 PDCs, whereby the total number of deregistered PDCs reached 466.

Where a PDC applies for processing of data falling within the scope Article 5(1) of the PDP Act or in the case of data the processing of which according to a CPDP decision endangers the rights and lawful interests of individuals, the CPDP always performs an ex ante inspection in accordance with Article 17b of the PDP Act before entering the applicant in the PDC Register. During the period from 1 January to 25 May 2018, 279 PDCs were subjected to ex ante inspections before being registered in the register referred to in Article 10(1)(2) of the PDP Act.

2. Provision of Personal Data to Third Countries — Overview and Statistics as of 25 May 2018

By 25 May 2018, the CPDP expressed opinions on **3** notifications for provision of personal data to third countries on the grounds of standard contractual clauses.

The CPDP position in the cases where personal data is transferred on the grounds of Article 36a(5)(2) of the PDP Act is that the PDC shall not request authorisation for such transfers but shall notify the CPDP of the planned transfer and enclose evidence of the existence of standard contractual clauses.

When considering the notifications, the CPDP monitors the implementation of and the provision of evidence if the transfer agreement reproduces in full the text of the standard contract clauses, if the requirements envisaged in Article 19 and Article 20 of the PDP Act have been complied with, and the applicable legal grounds for transfer of data under Article 4(1) of the PDP Act.

IV. PROTECTION OF THE RIGHTS OF INDIVIDUALS IN RELATION TO THE PROCESSING OF THEIR PERSONAL DATA

1. Proceedings Related to the Examination of Complaints and Requests. Statistics and Analysis of the Complaints and Requests Received by the CPDP

As part of its supervisory remit in the area of personal data protection, the CPDP has the power to examine complaints lodged by natural persons against PDCs over alleged violations of their rights laid down in the PDP Act. Complaints or requests for protection of violated rights can be lodged within one year after the applicant obtains knowledge of the violation, but not more than five years after the occurrence of the violation. Missing these deadlines results in an inability of the CPDP to exercise its powers and makes the complaints inadmissible.

Pursuant to the requirements set out in the Rules on the Activity of the Commission for Personal Data Protection and its Administration (RACPDPA), a complaint can be filed in person, in a hard copy; via a letter addressed to the administrative address of CPDP; by fax; by e-mail at the CPDP e-mail address, and in this case the complaint shall be in the form of an electronic document signed with a qualified electronic signature (QES); or via the CPDP website, and in this case the complaint shall also be in the form of an electronic document signed with a QES.

The CPDP has created an organisation to provide individuals with the opportunity to lodge complaints with it in five different ways and the requirements regarding the content of the complaint are as follows: it shall contain information about the complainant – names, address, telephone number, e-mail address (if available); the nature of the complaint or the alleged specific infringement of the complainant's rights; other information and documents that the individual considers relevant to the complaint; date and signature (for electronic documents – electronic, for paper documents – authentic handwritten signature). The absence of any of the requisites of the complaint leads to its irregularity. It shall be noted that when a complaint is received, the exact identification of the complainant is required, as the nature of the proceedings concerns infringements involving the personal data of the complainant.

The proceedings relating to complaints are regulated by the Administrative Procedure Code (APC) and are provided for in Article 38 of the PDP Act. They are closed with an administrative act of the CPDP which is an individual administrative act subject to two-instance judicial review.

With its decision on the merits of a complaint, the CPDP may refuse to honour the complaint because it is unfounded where no infringements of the complainant's rights are established, and in

the case of a well-founded complaint the CPDP may issue compulsory instructions, set a time limit for correcting the infringement or impose an administrative penalty.

When requests are received which do not contain information regarding infringed rights of the sender, but report violated rights of a third party or other violations in the processing of personal data, an inspection may be carried out in accordance with the procedure laid down in Article 12 of the PDP Act.

We would like to draw attention to the fact that an individual can refer the case to the relevant competent court, but this right cannot be exercised if there is a pending proceeding before the CPDP for the same offence or if the Commission's decision on the same violation has been appealed and no enforceable court ruling exists.

It is necessary to point out that while the possibility to refer a case to the CPDP is limited to up to one year of becoming aware of, but not later than five years after the alleged infringement, the competent court may be approached within 14 days of becoming aware of the infringement. Furthermore, no fees are payable for considering complaints by the CPDP and thus the ability to protect the rights, provided for in the PDP Act, is available to all individuals.

From 25 May 2018, the date from which Regulation (EU) 2016/679 applies, the CPDP has the tasks and powers specified in Articles 57 and 58 of the Regulation when examining complaints received. These provisions extend the scope for administrative intervention when infringement of the data subject's rights is established or for influencing the PDC in the event of a possible infringement. When imposing financial penalties, the CPDP complies with the requirements of Article 83 of Regulation (EU) 2016/679 which introduces a more detailed assessment when determining the amount of the administrative fine.

2. Statistics and Analysis of the Complaints Received by the CPDP

In 2018 the CPDP received over 784 complaints filed by individuals who claim that their rights have been infringed when their personal data were processed. For comparison, it should be noted that for the entire 2017 the complaints received were no more than 480.

The complaints submitted in 2018 and 2017 are compared graphically as shown below:

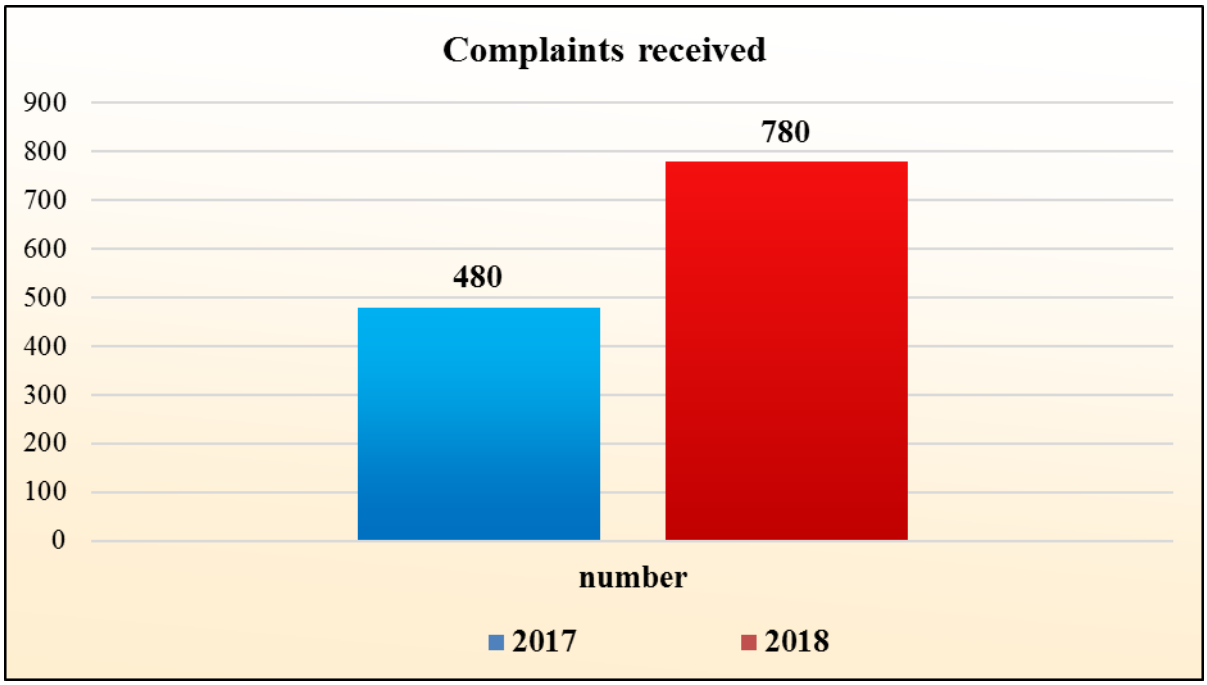

Figure 4

The number of complaints received after 25 May 2018, the application date of the General Data Protection Regulation, increased. More than 531 complaints were received after that date.

However, the increase in citizens' complaints activity cannot be linked to an increase in the number of violations in the processing of personal data. Such statistics can only be made after the closure of the proceedings initiated before the CPDP in respect of the complaints received. The Commission believes that the citizens' activity to protect their rights in the processing of personal data results from the great number of comments, analyses, interviews and other journalistic material in the media. It is necessary to point out here that through constant communication with the media and multiple events, valuable and practical information reaches the population. This is part of the overall policy of the CPDP to achieve publicity, transparency and open dialogue with the Bulgarian society.

Depending on the final decision of the CPDP, the rulings were as follows:

1. on whether the complaints are founded – 176 decisions;

2. for suspending the administrative proceedings due to the existence of a parallel procedure at the MoI or the prosecution authorities – 4 decisions;

3. on inadmissibility of complaints – 71 decisions;

4. on irregularity of complaints and requests – 40 decisions.

In 12 of the administrative proceedings closed due to inadmissibility, the complainants withdrew their complaints; in practical terms this means that the CPDP was de-seized.

Eighty-nine complaints were rejected as unjustified since the CPDP did not find violations of personal data processing rules or infringements of complainants' rights.

The CPDP found 87 complaints to be justified. Of these, the CPDP pronounced decisions regarding 36 complaints before the entry into force of the General Data Protection Regulation and regarding 51 complaints after 25 May 2018. The proceedings closed by imposition of the administrative sanction fine/financial penalty were 37, and the financial penalties and fines imposed amounted to BGN 365 300. Twelve compulsory instructions were issued.

It is necessary to point out that after the entry into force of the General Data Protection Regulation the CPDP has the power to issue warnings or orders in cases of breaches in personal data processing or infringement of data subjects' rights.

In this connection, the CPDP exercised these powers in connection with 42 justified complaints.

The ratio of justified vs. unjustified complaints can be expressed graphically as shown below (Figure 5).

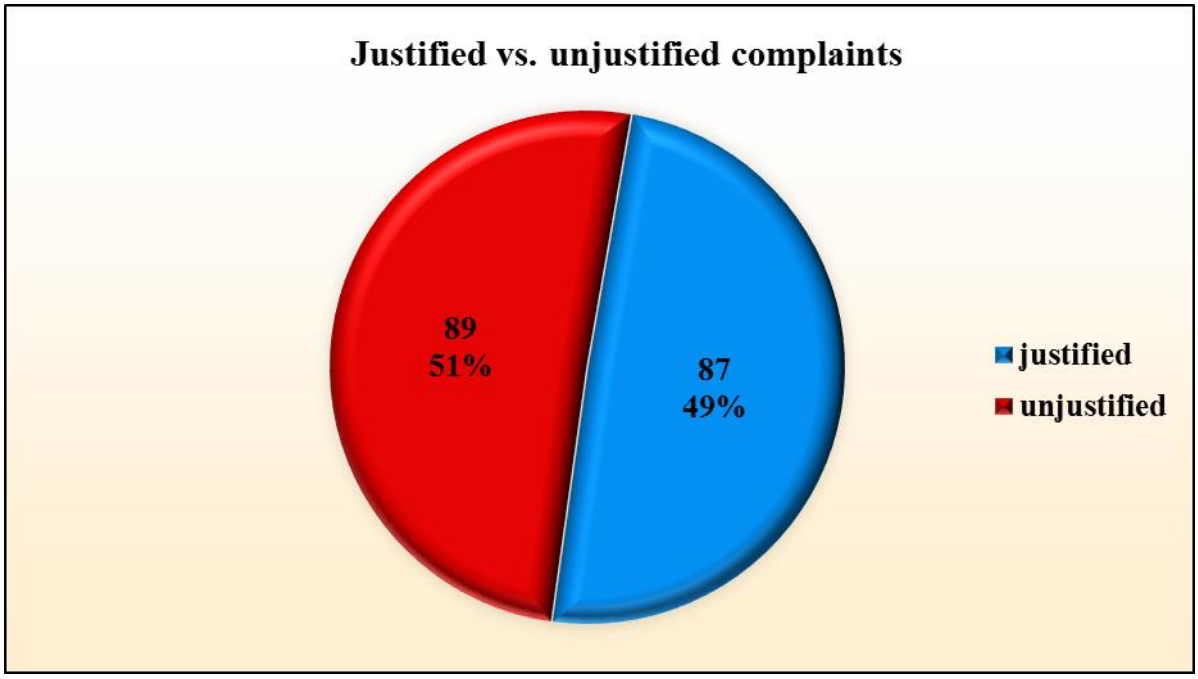

Figure 5

It is necessary to point out that in 2018 the CPDP's practice of ruling on justified complaints changed in view of the application of Article 58(2) of Regulation (EU) 2016/679, which gives the competent authority corrective powers where PDCs infringe on data subjects' rights. In this connection, in 20 % of the cases concerning justified complaints the CPDP imposed corrective measures with respect to PDCs.

The ratio of corrective measures imposed vs. the compulsory instructions given and administrative penalties imposed before 25 May 2018 is presented in the following figure (Figure 6)

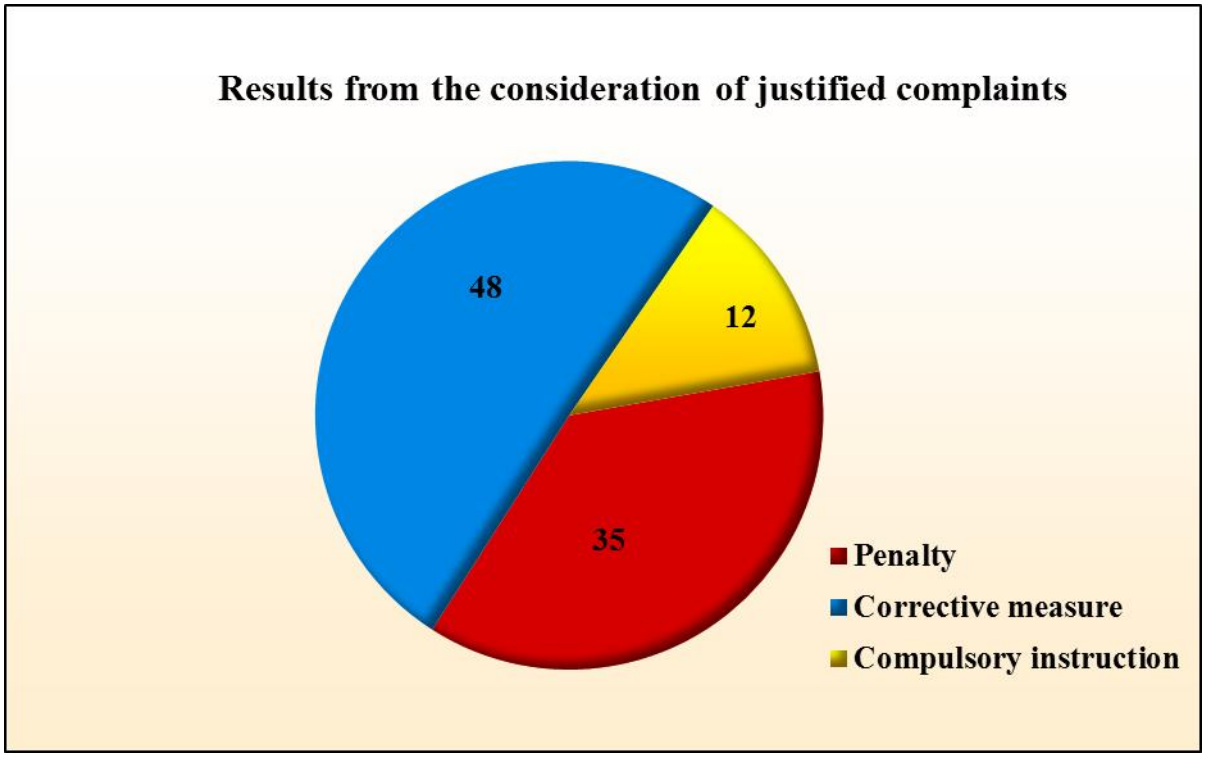

Figure 6

The established violations committed by PDCs can be grouped into the following categories:

– processing of personal data in the absence of a lawful reason for the data processing operation (Article 4 of the PDP Act): 9 violations in respect of which the CPDP imposed financial penalties in the total amount of BGN 95 600;

– processing of personal data, wherein the PDCs had failed to apply technical and organisational measures to protect the data against accidental or illegal destruction, or against accidental loss, unauthorised access, modification or dissemination, or against other illegal

processing (Article 23 of the PDP Act): 18 violations in respect of which the CPDP imposed financial penalties in the total amount of BGN 22 700;

– failure of the PDCs to assist the CPDP in exercising its supervisory powers (Article 22(5) of the PDP Act): one violation in respect of which the CPDP imposed a financial penalty of BGN 1 000;

– infringement of the right of access to personal data: the CPDP established one violation in respect of which it imposed a financial penalty of BGN 1 000.

Following the entry into force of Regulation (EU) 2016/679, in 37 cases corrective powers were exercised in accordance with the procedure for considering complaints:

– 25 reprimands were issued to PDCs where processing operations have infringed provisions of the Regulation – Article 58 (2) (b) of Regulation (EU) 2016/679;

– in one case the controller was ordered to comply with the data subject's requests to exercise his or her rights pursuant to the Regulation – Article 58 (2) (c) of Regulation (EU) 2016/679;

– in 15 cases the controller was ordered to bring processing operations into compliance with the provisions of the Regulation – Article 58 (2) (d) of Regulation (EU) 2016/679;

– in one case the controller was ordered to rectify personal data or restrict processing pursuant to Articles 16, 17 and 18 of the Regulation – Article 58 (2) (g) of Regulation (EU) 2016/679.

The Commission imposed financial penalties with a total amount of BGN 246 500 for the 13 infringements in personal data processing found.

3. Comparative analysis of complaints

According to the type of the PDC and with respect to the subject of the complaints filed against PDCs before the CPDP, the following main sectors are differentiated:

- Telecommunications. Although fewer complaints (91) were received in 2017 compared to 2016, in 2018 there is a trend of increase in the number of complaints. To date the CPDP has received more than 135 complaints filed against companies in the telecommunications sector. Complaints are related to the provision of personal data for collecting claims arising out of concluded contracts for electronic communications. In such cases, personal data are provided on the basis of a contract for collecting of claims or as a result of an assignment agreement. One fact raises

serious concerns: individuals file complaints containing allegations of unauthorised registration of SIM cards that are subsequently used for committing crimes – telephone fraud.

- Video surveillance. This sector maintains the trend of increase in the number of complaints observed in the past few years. In 2017 the complaints to the CPDP that contain allegations of unlawful processing of personal data through video surveillance system were 32, while in 2018 their number is close to 84. With regard to the subject of complaints to the CPDP containing allegations of illegal processing of personal data of individuals through video surveillance, the following two factual situations can be distinguished: video surveillance carried out in condominiums and video surveillance carried out by an individual for personal and household activities.

- Banks and credit institutions. Next come the complaints against banks and companies that offer lending services. Complaints in this category, in addition to allegations of unauthorised disclosure of personal data for the collection of claims from natural persons, also include allegations related to the use of personal data for granting loans without such loans being requested. The number of such complaints increased from 23 in 2017 to 67 in 2018.

- Electronic media. In 2018 the CPDP received 35 complaints from individuals who claim that their personal data are distributed through the media. For comparison, the complaints in this sector in 2017 were 12. Making the public aware of important and significant events and issues is also due to the electronic media which, because of their accessibility, reach an extremely wide group of users. This helps increase the sensitivity of individuals to information disseminated through electronic media, in particular their personal data. It needs to be pointed out that the personal data processed need to be relevant, proportionate to the purposes for which they are being processed and not exceeding their scope. The practice of the CPDP shows that personal data is distributed through the publication of copies of documents.

- Education. This sector has always been the subject of special monitoring by the CPDP insofar as data controllers mainly process personal data of children. The fact that 23 complaints were received this year while there were 6 (six) complaints in 2017 cannot remain unnoticed. The increased number of complaints is due to the introduction by the educational establishments of the so-called ‘statement of consent’ for the processing of personal data. The reverse hypothesis is also observed: bank accounts are opened to pupils for scholarships or other payments without the consent of a parent or another person representing the child.

It should be noted that most of penalties for established violations were imposed on PDCs in the telecommunications sector as well as on controllers providing utilities and banks.

Most of the infringements are related to the processing of personal data without the legal basis for such processing (such as a contract or consent).

The sectors of operation of PDCs against which complaints from individuals were most frequently received in 2017 were as follows:

Telecommunications – 135 complaints

Video surveillance – 84 complaints

Banks and credit institutions – 67 complaints

Executive branch – 41 complaints

Media – 35 complaints

Employment and social security services – 25 complaints

Education – 23 complaints

Judicial authorities – 16 complaints

Local authorities – 4 complaints

4. Practice for Dealing with Complaints

As far as the specific cases under complaints received or considered during the reporting period are concerned, the following cases can be identified:

1. The CPDP was notified of an infringement on the rights of a minor – a pupil in connection with the provision of the minor's personal data by the educational establishment in which he/she studies to a credit institution for the opening of a bank account in which a scholarship for high success is to be transferred. The evidence gathered in the administrative proceedings revealed that the PDC has not undertaken clear and specific organisational measures in respect of the collecting, use and providing a copy of the identity cards of the pupils eligible to receive scholarships from the educational establishment and that, as a result, the personal data of the person who complained to the CPDP were used (through the provision of a copy of his/her personal card by the educational establishment to the bank) unlawfully by the bank to open a bank account without said person giving an informed consent and without the consent of a legal representative in view of the fact that the person was a minor. The administrative-penal liability of the educational establishment was confirmed and the minimum penalty was imposed.

The proceedings also established beyond dispute the unlawful processing of the personal data of the pupil by the bank for opening an account and for issuing a special debit card without the existence of contractual relations between the parties and without a consent – explicit and informed statement of the pupil for processing of his/her personal data for the purpose of opening a bank account, respectively a consent of the parent or a trustee of the person. The administrative-penal liability of the credit institution was confirmed and a financial penalty was imposed.

2. The CPDP received a complaint containing allegations of unlawful processing of personal data of an individual by a mobile operator for the purpose of ten prepaid cards registered in the individual's name and used for committing crimes – telephone fraud. The evidence gathered in connection with the complaint demonstrated that the controller has not kept registration forms whereby the prepaid cards have been registered and cannot prove the existence of contractual relations with the individual and the individual's consent for the processing of his personal data for the stated purposes. Given the fact that the data of the individual who filed a complaint with the CPDP were processed unlawfully — without existence of any condition of admissibility of the processing — and in view of the high degree of public danger of the act and the passive behaviour of the controller in respect of which the violation is not the first one, a fine was imposed on the controller in an amount that corresponds to the infringement found.

3. The CPDP was approached by an individual practising a medical profession with a complaint about the unlawful processing of his personal data by a municipal medical treatment facility in connection with a contract registered with the NRA and a social security declaration submitted by the medical treatment facility in respect of the individual for June 2017. The complaint also contains allegations of unlawful processing of the individual's personal data in the case of their provision by a private medical treatment facility to a municipal medical treatment facility for the purposes of the contract.

The evidence gathered in connection with the complaint showed that the complainant had employment relations with the private medical treatment facility from 5 January 2016 to 25 May 2017 and in connection with this provided to the medical treatment facility his personal data (names, PIN, address) and copies of documents relating to the specifics of the position he occupied (a diploma for completed higher education in Medicine, a certificate for a recognised specialty in Gastroenterology and a certificate for membership in the Bulgarian Medical Union).

The CPDP found that the medical treatment facility provided by electronic channels to the municipal medical treatment facility copies of documents issued to the complainant and containing

his personal data (a diploma for completed higher education in Medicine, a certificate for a recognised specialty in Gastroenterology and a certificate for membership in the Bulgarian Medical Union), as well as a copy of the complainant's identity card. A penalty was imposed on the company for violation of Article 23(1) of the PDP Act, namely for processing personal data without having taken technical and organisational measures for the protection of the complainant's personal data, as a result of which the rights of the individual who filed a complaint with the CPDP were infringed.

In the course of the proceedings, the CPDP found another violation of the provisions of the PDP Act by the private medical treatment facility: keeping of a copy of the complainant's identity document in relation to the employment relations between the parties. This was done in breach of the principles on which the processing of personal data should be based and in particular the principle of proportionality of the data according to which the data processed should be relevant, proportionate to the purposes for which they are being processed and not exceeding their scope. In this regard, the CPDP gave instructions to the company, as appropriate, to destroy the copy of the complainant's identity card, given that the collecting by the employer and keeping a copy of an identity document in the workers' files are not proportionate to and exceeds the purposes for which the workers' data are processed, in particular in relation to the employment relationship between the parties.

The evidence gathered in connection with the complaint also showed that the complainant's rights were infringed by the municipal medical treatment facility. The complainant's personal data — three names, PIN, address and identity card number — were processed for drawing up a service contract between the municipal medical treatment facility as the appointing authority and the complainant as the contractor with the subject 'provision of consultations as a Gastroenterologist'. Said contract has not been signed by the individual. It was also established beyond doubt that in connection with the contract of 7 August 2017 the company has provided to the NRA personal data (names and personal identification number) in order to pay social security and health insurance contributions in connection with the contract. The CPDP decided that the processing of personal data of the complainant in the case described above (using said data to prepare a service contract, keeping and providing the data to the NRA) has been done in breach of Article 4(1) of the PDP Act insofar as said data have been processed without the complainant's consent and none of the other conditions for admissibility of processing as specified in items 1, 3, 4, 5, 6 and 7 of Article 4(1) of the PDP Act exist.

In view of the fact that this is the first violation of the PDC and given that the data have been provided by a state body to the NRA which already has them in relation to other contracts concluded with the individual, the CPDP issued a compulsory instruction, as appropriate, to the municipal medical treatment facility.

4. The parties to the administrative proceedings, in particular PDCs, are obliged to assist the CPDP when the latter exercises the powers vested in it with the PDP Act and the General Data Protection Regulation. The legislator has provided for the possibility of invoking the administrative penal liability of obligated entities for their refusal to assist the CPDP, respectively their failure to act on instructions and orders given by the CPDP in relation to the proceedings, failure to provide access to personal data and information and failure to provide access to premises, any equipment and means of data processing.

It is exactly for such violations that in 2018, in accordance with the procedure laid down in Article 83(5)(e) of Regulation (EU) 2016/679, that penalties were imposed on two PDCs. Despite having received instructions to assist the supervisory authority and provide relevant explicitly specified evidence, the PDCs did not provide assistance to the CPDP in exercising the powers conferred thereon by the law and did not clarify the facts surrounding the cases brought before the supervisory authority.

5. Case Law Relating to Appealed Decisions of the CPDP

In 2018, the Sofia City Administrative Court (SCAC) initiated 44 cases on appeals against administrative instruments issued by the CPDP. The cases before the Supreme Administrative Court (SAC) in the capacity of appellate court were forty-two (42), and 16 of them were initiated in 2016 and 20 were initiated in 2017.

Of all cases considered by the SCAC, 27 were concluded with decisions, and 17 are pending the decision of the corresponding panels. In addition, in 2018 the CPDP was notified of the decisions in 9 court cases which had to be delivered during the previous year. The information available shows that 21 decisions confirmed the appealed administrative instruments of the CPDP. In one of them the CPDP decisions were partially repealed, and in 14 decisions the instruments issued by the Commission were rescinded.

The figure (Figure 7) shows the number of confirmed and repealed decisions of the CPDP:

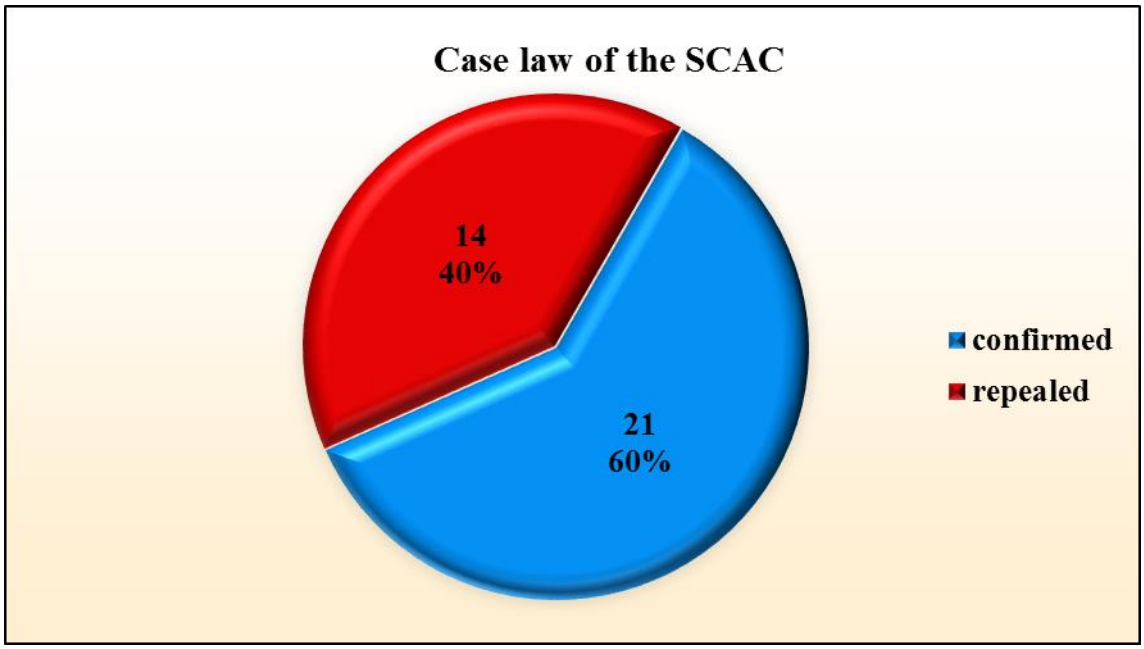

Figure 7

In 2018, the SAC held sessions on 42 cases, of which **19** cases initiated in 2016, 21 cases initiated in 2017 and 2 cases initiated in 2018. In 2018 the SAC notified the CPDP of the decisions in 50 court cases, 12 of which had to be delivered during the previous year.

The SAC confirmed 37 decisions of the SCAC that confirm the instruments issued by the CPDP and rescinded 4 decisions of the SCAC thus confirming the corresponding instrument issued by the CPDP. By 4 decisions the SAC overruled the decision of the SCAC, in two cases also repealing the decision of the CPDP, and the rest of the cases were returned to the SCAC for re-examination. In 5 decisions the SAC upheld the corresponding decision of the SCAC that revoked the decision of the CPDP. In conclusion, it can be said that following a two-instance judicial control of 50 cases related to appeals against decisions of the CPDP, 40 decisions of CPDP were enforced and 10 were rescinded.

In view of the final result, the practice of the SAC with regard to instruments issued by the CPDP can be expressed graphically as shown below (Figure 8).

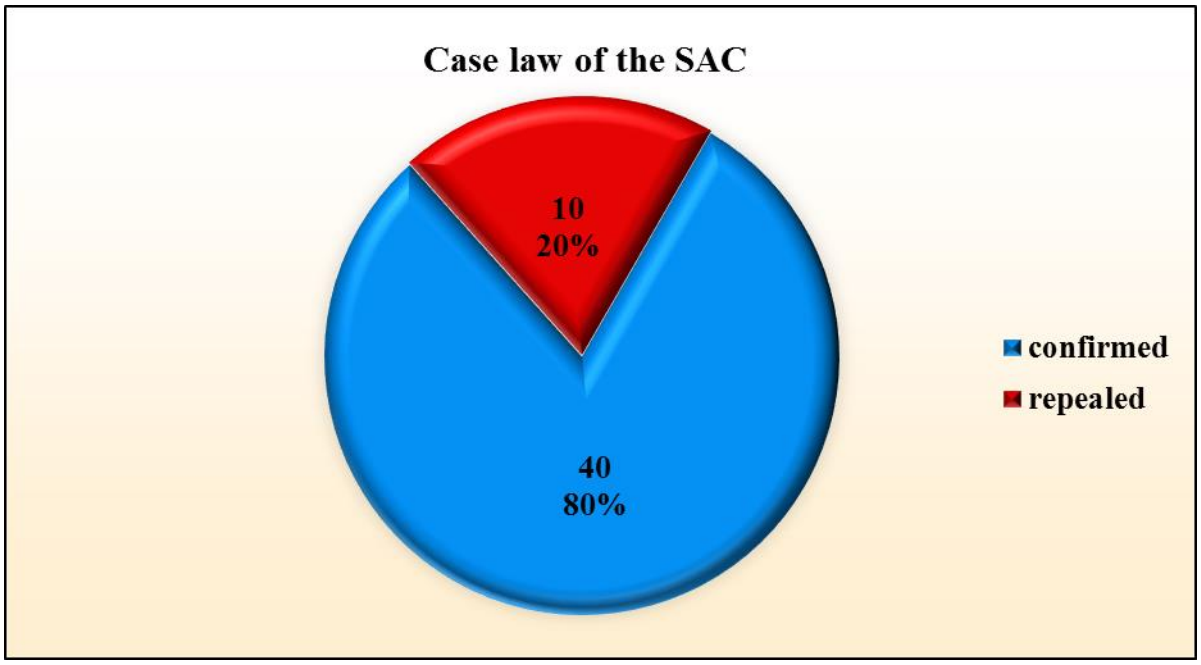

Figure 8

6. Statistics of the Imposed and Collected Public Receivables Stemming from CPDP Decisions

The total amount of the penalties imposed by CPDP administrative instruments in 2018 was BGN 365 300. The amounts collected pursuant to CPDP decisions in 2018 came to BGN 165 200, of which BGN 74 500 were collected coercively by the NRA.

7. Advice Provided to Citizens

7.1. Statistics and aggregated information on matters relating to personal data processing and protection and on inquiries from citizens and information and consultations related thereto

The questions received by the CPDP in 2018 were many and of diverse nature. With the adoption and introduction of the General Data Protection Regulation on 25 May 2018, an extended body of rights of individuals was introduced and additional obligations were imposed on data controllers. As a result, citizens started actively seeking assistance and clarification on the application of the new legal framework. This is also reflected in the statistical analysis of the inquiries received in the CPDP after 25 May 2018, notably over 2 000. Some general questions or issues of public interest brought to the attention of the CPDP during the reporting period are discussed below.

7.1.1. Personal data processing by the MoI authorities

During the reporting period, the CPDP was addressed with a number of questions concerning the provision of personal data (identity card) and whether it constitutes personal data processing. The answers in principle are that according to the provisions of Article 6(1)(c) of Regulation (EU) 2016/679 personal data processing is lawful where it is necessary for compliance with a legal obligation to which the controller is subject. The Ministry of Interior Act (MoI Act) which defines the main tasks and the main activities of the Ministry of Interior authorities is given as an example. Article 7 of this Act provides for the obtaining, analysis and storage of information, including processing of personal data, and provision of personal data in the cases provided by law.

The General Data Protection Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It also protects fundamental rights and freedoms of natural persons and in particular their right to protection of personal data. According to Article 2(2)(d) of the Regulation, it does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It is these goals listed in the Regulation that overlap with the main tasks of the MoI authorities. Therefore, police authorities have the right to process (in the form of recording) personal data of citizens.

7.1.2. Photocopying documents containing personal data (identity cards, driver's licences, passports, title deeds, etc.) by copying centres

In these cases, the personal data of individuals are not processed by copying, scanning and sending the identity documents but their media is processed. These actions do not result in storage and processing of personal data according to the provisions of the General Data Protection Regulation. Therefore the CPDP is of the opinion that copying centres are not PDCs, but they need to undertake appropriate technical and organisational measures in order to protect the data against accidental or unlawful destruction, or against accidental loss, unauthorised access, alteration or dissemination, or against other unlawful processing.

7.1.3. Personal data processing by courier companies

Due to repeated requests from citizens, intensified correspondence between the CPDP and various courier companies took place during the reporting period. In certain cases employees of the

courier company require personal data (three names and Personal Identification Number (PIN)), namely when postal money transfers are paid and when cash is paid on delivery of a consignment, where primary accounting documents (receipts) are issued on the basis of Article 6 and Article 7 of the Accountancy Act of the Republic of Bulgaria and Article 84 of the Tax and Social Insurance Procedure Code. This is regulated in the Instructions on Paying and Reporting of Cash on Delivery and the Instruction for Payment of Postal Money Transfers.

The actions relating to providing to the courier company of names, PIN and ID card number upon receipt of a cash on delivery consignment, as well as the comparing by the courier of these data with the person's identity card constitutes 'processing of personal data' by the data controller (the corresponding courier company). The actions relating to payment of cash on delivery are described in detail in the instructions. Upon payment of the cash on delivery, the employee prints out from the system a receipt and then checks the personal documents of the payee (the authorised person) and **provides the client with the receipt so that the client can write his or her PIN and full names and sign**. The employee writes his or her full names (this is not necessary if they are automatically printed by the system) and also signs the receipt in the 'person who paid the amount' field. The employee photographs the already completed receipt and uploads the digital image in the system for storage. The paper receipt is sent to the headquarters of the company.

7.1.4. Personal data processed by the Bulgarian Posts

The position which the CPDP has expressed on many occasions in connection with inquiries relating to the processing of data by Bulgarian Posts EAD is that the latter has the right and the legal obligation to process personal data. According to the provisions, the volume of personal data that is capable of identifying natural persons who issue and receive an accounting document for accounting and taxation purposes comprises the name, address and PIN. It should be taken into account that the postal operators are obligated persons within the meaning of the Measures against Money Laundering Act and, according to its provisions, are also required to collect data that allow the individualisation of the senders and recipients, including PIN.

7.1.5. Data protection officer. Need, requirements

The new General Data Protection Regulation introduces the figure of the so-called 'Data protection officer' (DPO). The data protection officer is a staff member of the PDC or a natural person outside the controller's organisation who has the task to provide advice in the area of personal data protection, to monitor compliance with the Regulation in the controller's operations and to raise awareness of staff and train staff.

The DPO can be a member of staff but can also be an external person who performs his or her obligations on the grounds of a concluded service contract. Therefore PDCs are not obliged to appoint such a member on their staff. They are only obliged to designate a person who will perform the functions of a data protection officer. The employee appointed as a DPO is not precluded from performing other functions within the organisation as long as these functions do not lead to a conflict of interest. The conditions under which a DPO is designated or appointed are entirely within the discretion of the PDC.

The position of the CPDP remains that the decision on whether to appoint a DPO needs to be taken by the PDC after assessing the controller's activity and the personal data of individuals processed. The conditions laid down in Article 37 of the General Data Protection Regulation need to be taken into account when said decision is made. In principle, it is desirable to make an assessment of the volume of data, their nature, respectively the risk to persons in the event of data security breaches, the means by which data will be collected and processed and the objectives set.

PDCs can benefit from the guidance of the Article 29 Working Party (which as of 25 May 2018 became the European Data Protection Board) regarding DPOs. Except in legally regulated cases, PDCs can voluntarily appoint DPOs and this will be considered a good practice.

The DPO may be recruited on an employment or on a service contract and can be an employee of the administration (without any conflict of interest) or an external expert. A single DPO can be appointed for several PDCs as long as they operate in the same field. Detailed information regarding DPOs can be found on the CPDP website.

7.2. Analysis of the nature of the inquiries received through the Centre for Information and Contacts maintained by 1 August 2018

The Centre for Information and Contacts (Call Centre) of the CPDP as an important communication channel for direct communication with citizens and improving the quality of services was maintained until 1 August 2018. Its goal was to deal with inquiries by providing as full information as possible from the very first call. Among the most frequently asked questions were those regarding the registration of PDCs (which were topical before 25 May 2018) as well as questions relating to filing complaints in cases of misuse of personal data of citizens and complaints about the misuse of personal data by social networks, institutions and the so-called collection companies. Following the entry into force of the new European legal framework as of 25 May 2018, the number of questions relating to training in the field of personal data protection in relation to the new requirements of Regulation (EU) 2016/679 increased.

The questions asked most frequently resulted from the fact that PDCs find it difficult to determine the scope of personal data registers processed by them, respectively their number and the statutory grounds for keeping such registers. Applicants were usually not familiar with the statutory regulations in the field of personal data protection and therefore needed to get support from the call centre operators.

Many of the questions asked when registering companies with online e-commerce were related to the provision of personal data in non-EU and EEA countries. In such cases inquiries were referred to the experts in the specialised CPDP administration.

The Centre for Information and Contacts received calls relating to difficulties in the drafting of the instructions of PDCs under Article 23(5) of the PDP Act. PDCs also encounter difficulties with regard to the criteria applicable to the defining of different levels of protection of personal data.

Complaints/reports and questions were also sent via the standard forms for filing on the CPDP website. Access to standardised forms of communication and interaction with the institution was provided, clear guidelines were developed for individuals on how they can exercise their rights in a complaint procedure should they believe that PDCs have failed to fulfil their obligations.

The complaints and questions were numerous and varied in nature, and those reporting misuse of personal data in social networks, fast-track lenders and government institutions prevailed.

The trend of increase in violations relating to the misuse of personal data by mobile operators and fast-track lenders and to providing personal data to the so-called collector companies, and to the misuse by employers of personal data of employees who have terminated employment relationships continued.

Many reports from citizens were related to the placing of video cameras in residential buildings without the consent of residents under the Condominium Management Act, as well as to the improper directing of these cameras for tracking objects and spaces beyond their intended purpose.

The number of questions regarding to the new Regulation (EU) 2016/679, the extent of its implementation and the planned training by the CPDP was extremely high.

Through the form for submission of questions via the CPDP website, inquiries were made by foreign individuals regarding the interpretation of the new Regulation (EU) 2016/679 and questions were sent relating to the Schengen visa and the tax obligations of Bulgarian citizens living abroad.

There were numerous requests for meetings in connection with the implementation of Regulation (EU) 2016/679, as well as questions relating to PDC training, queries regarding seminars and certification of companies falling within the scope of Regulation (EU) 2016/679. Requests for training were received from banks, mobile operators and law firms. Some of the questions were related to the new obligations of PDCs and processors to appoint a DPO pursuant to the requirements of Regulation (EU) 2016/679.

The CPDP received questions concerning the definition of data processing 'on a large-scale' according to Regulation (EU) 2016/679 and requests for clarifications on the 10 practical steps for implementing the Regulation, published on the CPDP website to raise public awareness.

PDCs were interested in the amendments to be made in the PDP Act as a result of Regulation (EU) 2016/679 and in the possible adoption of model codes of conduct.

The number of questions regarding to the new Regulation (EU) 2016/679, the extent of its implementation, the interpretation of individual considerations and regulations was extremely high.

A significant part of the questions concerned forthcoming planned training by the CPDP in relation to the implementation of the General Data Protection Regulation.

The new requirements of Regulation (EU) 2016/679 relate to the legal grounds for the processing of personal data, including on the basis of the consent of the persons, the time limit for storing the consent and the right to be forgotten which is a new focus in the relationship between the data subject and the data controller.

Frequently, questions were asked regarding the certification of PDCs, the issuing of ISO 27001:2013 certificates, the certification body in the Republic of Bulgaria and the statutory requirements that PDCs must fulfil in order to obtain a certificate.

A large group of questions related to the fact that courier companies require information about PIN in relation to the sending or receiving of cash on delivery (CoD) consignments.

Complaints and questions outside the competence of the CPDP were also received in 2018. They were forwarded to the relevant competent government institutions.

V. CONTROL AND ADMINISTRATIVE-PENAL ACTIVITY

1. Control activity before 25 May 2018

The procedure and methods for carrying out the overall control activity are governed by the provisions of the PDP Act, the RACPDPA, Ordinance No 1 of 30.01.2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection (the Ordinance), the Instruction on the control activities, the Methodology for Carrying out Sectoral Inspections and other internal regulations.

The Commission exercises control in the following areas:

- direct control on PDCs in the public and in the private sector;
- assisting PDCs with consultations and guidance on the compliance with the regulations, and on measures taken to protect the personal data processed;
- ongoing assessment of PDCs' work to ensure compliance with the legislation in the field of personal data protection;
- establishment of violations and imposition of sanctions on the grounds of and in accordance with the procedures laid down in the PDP Act and in the Administrative Violations and Penalties Act (AVP Act).

The controls laid down in Article 12 of the PDP Act are exercised directly by the Chairperson and the members of the CPDP and specially authorised officials from the specialised administration – Control and Administrative-Penal Proceedings Department of the Legal Proceedings and Supervision Directorate. Where necessary and depending on the subject and the tasks of the inspection, employees from other departments/directorates of the Commission are additionally authorised and take part. The activity relating to this type of control includes inspections of PDCs to establish facts and circumstances and collect the necessary evidence.

The purpose of these inspections is to establish:

- the legal basis on which personal data is processed;
- the procedures for keeping the personal data register;
- the purposes for which the personal data is processed;
- the proportionality, accuracy and updating of the data;

• the compliance of the extent of the protection of the personal data processed with the Ordinance.

Control is exercised by carrying out three types (ex-ante, ongoing and ex-post) inspections as provided for in Article 12 of the PDP Act. To clarify facts and circumstances relating to submitted complaints and reports and in pursuance of CPDP decisions, on-the-spot inspections are carried out. This in most cases is related to business trips of the inspecting teams in the country and, on more rare occasions, abroad.

The activities relating to the consideration of different requests, in connection with which no inspection within the meaning of the PDP Act is required, is also a form of control. This activity includes review of the relevant legislation, requesting the PDCs concerned to provide written replies and/or opinions, prescribing certain measures, consultations, etc., as well as mandatory notification of the person submitting the request.

Inspections end by the issuance of a statement of findings and, depending on the findings therein, a proposal for issuing a compulsory instruction can be made. In the event that an administrative violation of the provisions of the PDP Act is established, the Commission initiates administrative penal proceedings pursuant to the AVP Act.

Between the beginning of 2018 and 25 May 2018, 316 inspections were initiated, of which:

– 291 ex-ante inspections;

– 7 ongoing inspections;

– 18 ex-post inspections.

The total number of inspections carried out between the beginning of 2018 and 25 May 2018 (Figure 9), including inspections initiated in 2017, was 243. Of these:

– 204 ex-ante inspections;

– 14 ongoing inspections;

– 25 ex-post inspections.

During the same period, 159 requests were received and 189 requests were closed, including inspections initiated in 2017.

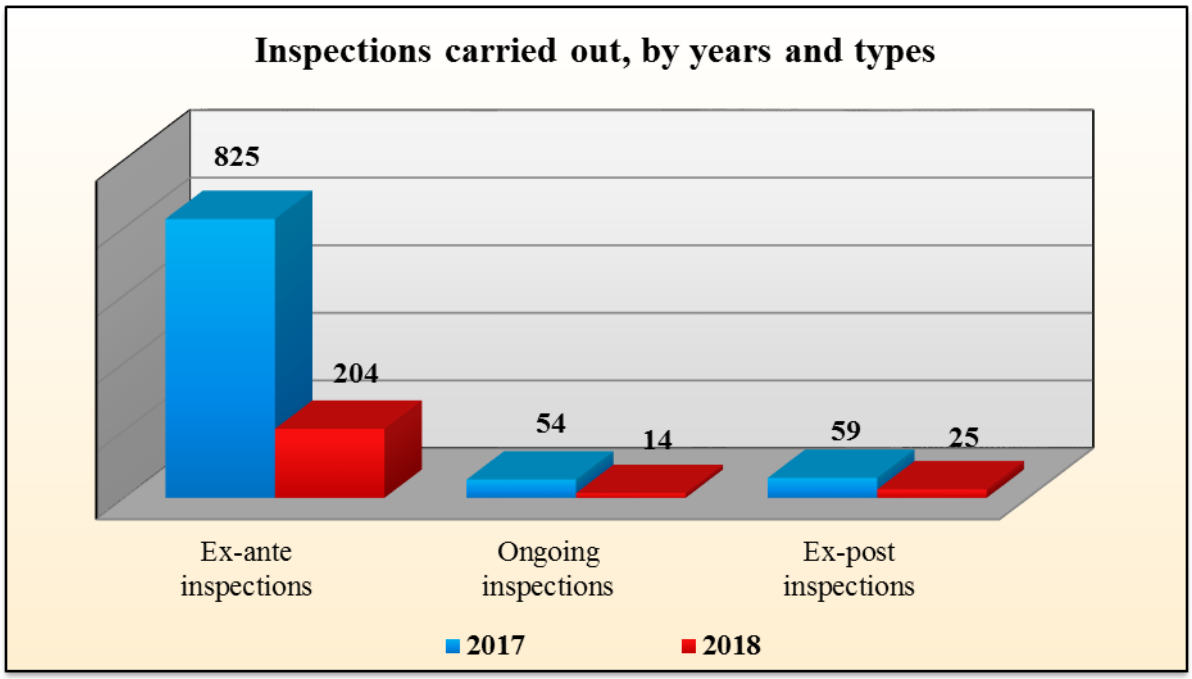

Figure 9

The control activity resulted in the drawing up of 239 statements of findings and the issuance of 4 compulsory instructions and 7 statements establishing administrative violations.

The comparative statistics show a considerable decrease in all types of inspections. This is due both to the shorter reporting period (almost 5 months) and to the fact that one of the types of inspections (ex-ante inspections) is no longer carried out.

The specific environments in which personal data is processed mean that there is a need to differentiate the inspections. In pursuance of its activities during the first 5 months of 2018, the CPDP carried out the largest number of inspections in the following sectors and areas:

- health care – 115 inspections;
- education and training – 30 inspections;
- video surveillance – 20 inspections;
- trade and services – 20 inspections; and
- non-profit organisations – 12 inspections.

1.1. Ex-ante Inspections

Pursuant to Article 17b of the PDP Act, these inspections are required prior to the PDC registration in the register referred to in Article 10(1)(2) of the PDP Act in the cases where the data controller has declared processing of data subject to special protection as per Article 5(1) of the PDP Act (related to health, sexual live or human genome, data revealing the person's race or ethnicity, or the person's political, religious, philosophic beliefs or membership in related organisations) or data the processing of which, according to a CPDP decision, endangers the individuals' rights and lawful interests.

The ex-ante inspections aim at establishing the technical and organisational measures undertaken in the context of personal data processing operations and the admissible type of protection provided by data controllers and their compliance with the requirements of the Ordinance.

Ex-ante inspections end with the registration of PDCs in the register referred to in Article 10(1)(2) of the PDP Act, issuing of compulsory instructions regarding the conditions of personal data processing and the keeping of a personal data register, or refusal of registration.

Between the beginning of 2018 and 25 May 2018, a total of 204 ex-ante inspections were carried out, including 3 inspections initiated in previous years in which a refusal of registration of personal data controllers and registers kept thereby was ruled.

The main problem with these inspections, similar to previous years, was the communication with the PDCs for provision of the documents required to finalise the inspection. The most frequent difficulties included uncollected correspondence, change of address, inaccuracies in the applications submitted and failure of the PDC to submit the required documents requested by a letter duly received thereby.

Another important issue in these inspections was the often poor quality of the personal data protection instructions that PDCs are obliged to adopt in accordance with the requirements of Article 23(4) of the PDP Act and Article 19(2) of the Ordinance. This resulted from the insufficient knowledge or lack of knowledge of the relevant legislation and personal data protection issues in their activities.

1.2. Ongoing Inspections

Although the number of ongoing inspections in accordance with Article 12(3) of the PDP Act is much lower than the number of ex-ante inspections, these inspections present larger factual and legal complexity.

According to the PDP Act, these inspections are carried out at the request of interested persons or at the initiative of the CPDP on the basis of the control plans adopted thereby for the corresponding year.

Fourteen ongoing inspections were carried out during the reporting period (Figure 9). They resulted in the issuance of 2 statements establishing administrative violations (SEAVs) and 3 compulsory instructions (CIs).

Ongoing inspections of more significant public interest which continued from 2017 are the inspections relating to inquiries received in the CPDP from the Registry Agency as to whether applicants – legal entities and natural persons (individuals) satisfy the requirements for technical and organisational measures taken for 'high level of impact – high level of protection' within the meaning of CPDP Ordinance No 1 of 30.01.2013. The inquiries were sent with a view to concluding a contract for the provision, for consideration, of the entire database of the Commercial Register and the National Database of the BULSTAT register with updating of the data. In the course of these inspections and in the context of the opinion of the CPDP issued in 2015, it is established whether the required necessary technical and organisational measures corresponding to a 'high level of protection' are undertaken in the activity of the respective legal entity or individual in accordance with Article 17(3) of the Ordinance. The Registry Agency and the applicant for the service are notified of the results in order to take follow-up actions according to their competence.

In 2018 the CPDP received 14 such requests. During the period the CPDP carried out 2 inspections of PDCs to establish the existence of measures for 'high level of protection'. The rest of the inspections were terminated because on 25 May 2018 the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 started and Ordinance No 1 of 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection was repealed. In this case, the legal grounds for carrying out inspections and for the existence of measures for 'high level of impact – high level of protection' within the meaning of the repealed provisions, on which the CPDP's original opinion was based, have lapsed and as of 25 May 2018 the CPDP cannot and should not perform any actions and certify these circumstances.

1.3. Ex-post Inspections

The third type of inspections are those in accordance with Article 12(4) of the PDP Act, notably ex-post inspections carried out to verify compliance with CPDP's decisions or compulsory instructions as well as inspections undertaken at CPDP's own initiative upon receipt of irregularity reports (alerts).

Twenty-five ex-post inspections were carried out during the first five months of 2018 (Figure 9). The subject matter and the methodology employed in these inspections are similar to the ones in the ongoing inspections, as described above, the only difference being the legal grounds on which they are carried out. The inspections ended with the issuance of 2 SEAVs and 1 compulsory instruction.

The 16 ex-post inspections carried out following the decision of the CPDP in connection with video surveillance were of significant public interest. The cases of complaints about the installation of video surveillance systems in condominiums and neighbouring low-rise buildings are most frequent. The main objective of these inspections is to establish the lawfulness of the installed video surveillance systems, the location of the installed cameras and the angle of capture, the number of cameras, the resolution of the images and their quality, the special functions of the camera, the storage of recordings/images and the periods before their deletion, the provision of information to individuals, etc.

1.4. Consideration of Requests

Pursuant to Article 36(2) of the RACPDPA, when a request does not contain details about violations of the applicant's right, action can be taken in accordance with Items 3, 5 and 6 of Article 10(1) and Article 43 of the PDP Act. Between the beginning of 2018 and 25 May 2018 the Commission received 159 requests from individuals, including topical inquiries on personal data protection issues. As in 2017, most frequently reports referred to the attention of the CPDP unlawful actions relating to:

- publishing of personal data in websites and possibility for unregulated access to such data;
- creating false profiles in websites;
- reports against mobile operators;
- receiving unsolicited electronic communications and phone calls;

• processing of personal data for direct marketing purposes without the consent of the individual having been requested.

A total of 189 requests were considered during the first 5 months of 2018 and 3 statements establishing an administrative violation were drawn up. Answers regarding the actions taken by the CPDP were sent to the individuals concerned.

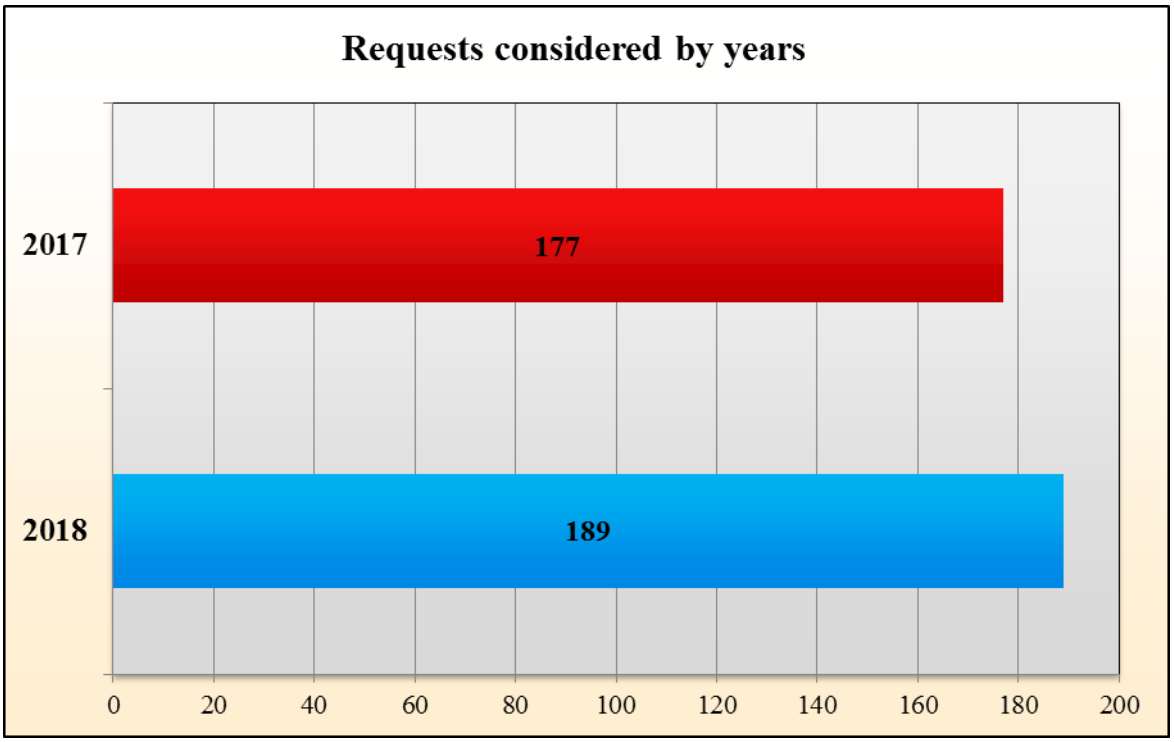

Figure 10

The comparative statistics from the previous year (Figure 9 and Figure 10) and the analysis of all types of inspections, including reports and various inquiries received by 25 May 2018 when the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council started, show a significant percentage increase both in size and in terms of quality and timeliness. These results were achieved due to the proper organisation of the work and the efforts of employees, especially taking into account the composition of the Control and Administrative Penal Procedures Department which was significantly reduced for objective reasons during the reporting period.

2. Administrative-penal activity before 25 May 2018

2.1. Compulsory Instructions

On the grounds of Article 10(1)(5) of the PDP Act and in connection with the control activity referred to in Article 12(1) of the PDP Act, the CPDP issues compulsory instructions (CIs) to PDCs regarding the protection of the personal data processed.

The CIs aim to afford adequate protection of the personal data in the personal data registers kept by maintaining the minimum scope of appropriate technical and organisational devices and protection measures as per the PDP Act and the Ordinance. Instructions put the PDC under the obligation to perform or suspend a specific action(s) based on omissions found in the course of the inspection, which are in breach of provisions of the PDP Act. The table below presents comparative information regarding the instructions issued during the first 5 months of 2018 and the previous reporting period (2017).

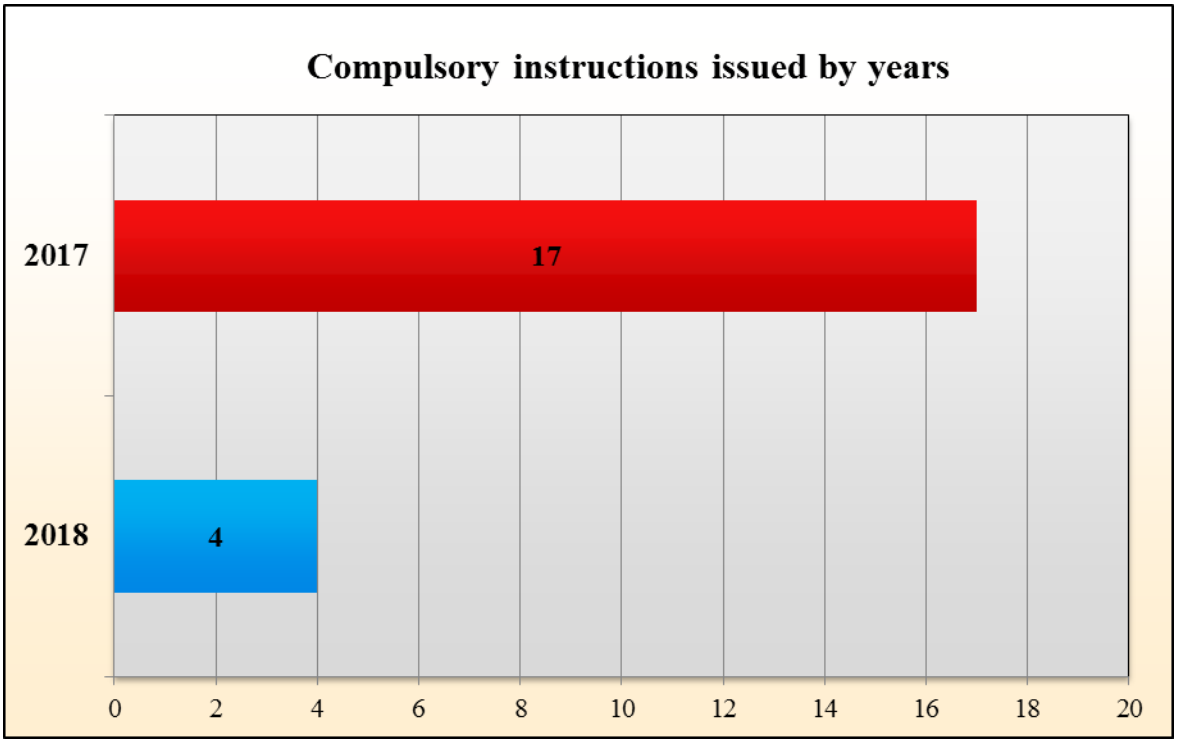

Figure 11

All compulsory instructions issued by the CPDP in 2018 were complied with within the time limits set. The compulsory instructions were issued in connection with:

- the processing of documents that contain personal data where the volume required is bigger than the volume necessary to identify the individual and thus the processing is not proportional to the objective of the processing of personal data;

- the defining of time periods for storage and the actions to be taken after the objectives of personal data processing are achieved, in accordance with the requirements of Article 25 of the PDP Act;

- the provision of information to individuals in relation to the processing of their personal data;

- the establishing of specific technical and organisational measures required to ensure adequate level of protection of personal data.

2.2. Administrative-penal Proceedings

Until the entry into force of the new Act to amend and supplement the PDP Act, according to the provisions of Article 43 of the PDP Act the legal grounds for establishing violations and initiating administrative penal proceedings, issuing, appealing and enforcement of penal decreed is the procedure laid down in the AVP Act. Statements establishing administrative violations (SEAVs) of provisions of the PDP Act are issued by a Commission member or by officials authorised by the institution and PDs are issued by the Chairperson of the Commission. These grounds and procedure remain unchanged in the new legal framework.

In connection with established violations of different provisions of the PDP Act, 7 SEAVs were issued in 2018. Based on these, the Chairperson of the CPDP issued 4 PDs. In view of the amendments to the legal framework and the direct application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 as of 25 May 2018, as well as in view of the amended legal regulation regarding the mandatory registration of PDCs following an assessment of the evidence collected, the administrative-penal authority decided that no penalty decrees should be issued because the said act is no longer a violation and terminated the proceedings as inadmissible according to Article 54 of the AVS Act. On these grounds, 2 (two) of the SEAVs drawn up in 2018 were terminated. On the grounds of Article 43(6) of the AVS Act (failure to find the offender), 1 SEAV was stayed.

Similar to previous years, in 2018 the Commission continued to encounter major difficulties in delivering the issued SEAVs to addressees via municipal administrations in various parts of the country as provided for in Article 43(4) of the PDP Act. Most often, municipalities do not observe the 7-day statutory time period for submitting, signing and returning the proceedings to the CPDP, which is sometimes explained by objective reasons – lack of sufficient staff, large volumes of proceedings, etc. In some cases SEAVs are served on persons without representative powers or the

receipt whereby the PDC certifies that it has been informed of its right to object to the statement within 3 days is not signed, or the documentary evidence is not served. These omissions make it necessary to return the file for new execution, which delays the closure of the proceedings. With a view to diligent search and service of the SEAVs and PDs, the CPDP seeks and receives assistance from the MoI authorities in the country. The distribution of the PDs by type of the violation to be remedied is presented on the next chart (Figure 12).

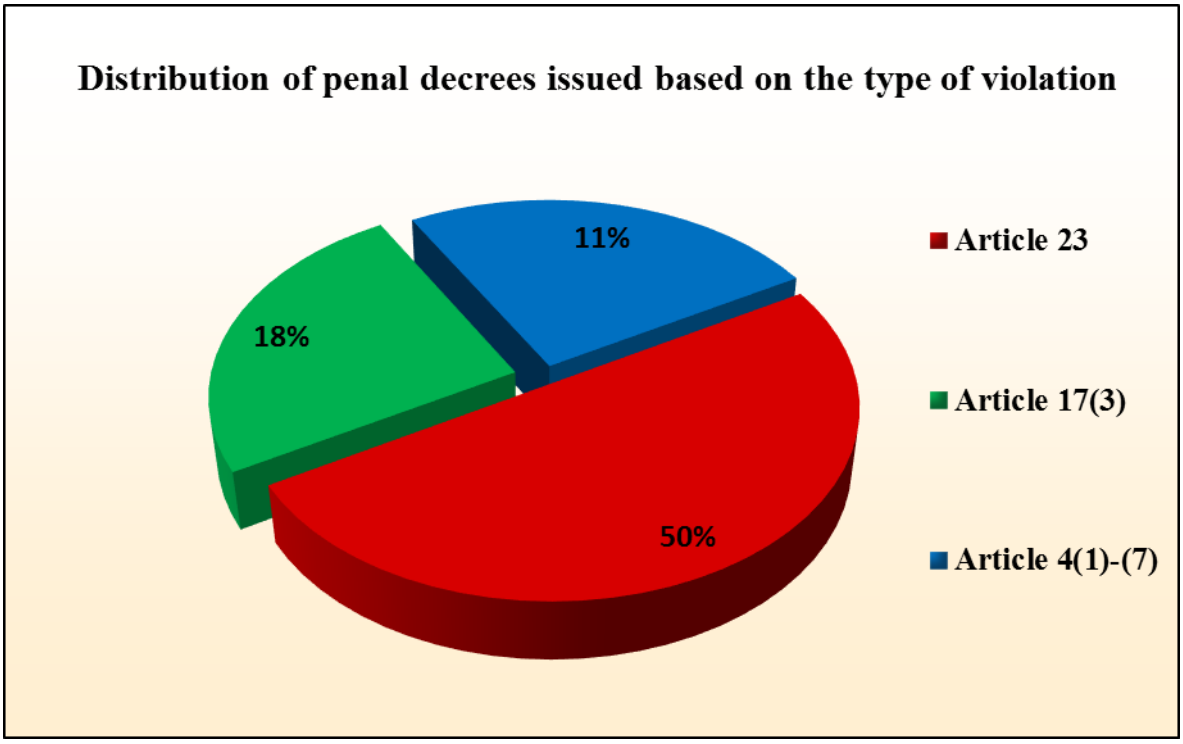

Figure 12

Two penal decrees were issued for violations of the provisions of Article 23 of the PDP Act. One of the offenders is a bank and the other offender is a commercial company. For violations of the provisions of Article 17(3) of the PDP Act and processing of personal data prior to submitting an application for registration, 1 PD was issued. For violations of the provisions on the admissibility of the processed personal data according to Article 4(1)-(7) of the PPD Act, one PD was issued to a private enforcement agent.

The small number of administrative-penal proceedings for this type of violations also results from the fact that they are frequently the subject of other types of proceedings initiated on complaints from individuals and are considered by the CPDP acting as a collective body.

The penalties imposed in 2018 amounted to BGN 12 000 (twelve thousand). The largest financial penalty – BGN 10 000 (ten thousand) – was imposed on a private enforcement agent for processing personal data without legal grounds. The revenues collected in connection with PDs

during the year amounted to a total of BGN 20 992.98, including BGN 17 592.98 collected by the NRA.

Eight PDs issued in prior years are in a trial phase.

The Tax and Social Insurance Procedure Code (TSIPC) is implemented for collecting the claims under PDs that have entered validly into force. If the offender does not pay a penalty under a penal decree/court ruling that has entered validly into force within the time period specified, the case is transferred to the NRA.

It is important to note that with effect from 31.03.2019 the NRA will no longer receive enforcement grounds via channels other than the electronic service 'Accepting instruments giving rise to a public claim by external creditors' introduced in a real environment as of 3.12.2018. In this way the activity of public creditors, such as the CPDP, will become much easier. This makes it necessary, together with the NRA and on their instructions, to complete the application and registration actions required for the use of the service and to train the respective CPDP officials to work with the service.

The analysis of the court decisions, including those from prior years, confirms the conclusion of the existence of diverse case law on identical cases.

In the court proceedings continuing in 2018, out of the 30 PDs issued against political entities registered in the CEC for participation in the election for members of the European Parliament from the Republic Bulgaria held on 25 May 2014, 1 PD issued against a coalition of political parties was rescinded, 5 PDs are still in a trial phase, and under 2 PDs the NRA is collecting the receivables.

In line with the ordinary practice, all court decisions and their reasons, especially the court decisions rescinding PDs, are analysed in depth with a view to integrating them in the lawful performance of control activities, but first and foremost with a view to resolve existing weaknesses and omissions in the activities relating to establishing violations of the PDP Act and to ensure that they are properly documented in accordance with the provisions of the AVS Act. The introduced good practice all court decisions to be sent in a timely manner by e-mail also to the Chairperson and Members of the CPDP contributed to this. As a result, it has been observed that the staff members authorised to prepare SEAVs, draft PDs and provide procedural representation have increased their legal competences. The conclusion regarding the excessively long period of considering the cases at the trial phase, from the initiation of the court proceedings till their completion with a legally enforceable judicial act, is confirmed. This reduces both the sanctioning and the educational effect of the punishments imposed by the PD for violation of the PDP Act.

A priority in the administrative-penal activity is to maintain a sustainable trend of sustained high quality of the prepared SEAVs and their strict compliance with the law and a relatively lower percentage of PDs cancelled by the court.

The analysis of the court judgements from the past two years shows that for the two most common violations, those of Article 17(1) and of Article 18(3) of the PDP Act, the PDs rescinded by courts register a growth; the difficulties in their practical application will be eliminated with the legislative changes initiated and in view of the implementation of the new legal framework in the field of personal data protection.

3. Control activity after 25 May 2018

As already mentioned, the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) started on 25 May 2018. The other important document applied as of 6 May 2018 is Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

These two documents impose the obligation to make the legislative amendments required to introduce the new legal framework in national law. After the Act to amend and supplement the PDP Act is adopted, it will be mandatory to issue new and/or update existing CPDP internal regulations concerning the procedures and methods for carrying out the control activities of the Commission, such as the RACPDPA, the Instruction on Control Activities, the Methodology for carrying out Sectoral Verifications, etc.

In connection with the new provisions of Regulation (EU) 2016/679 that introduce the so-called accountability principle, by a decision the CPDP repealed as of 25 May 2018 Ordinance No 1 of 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection adopted on the grounds of Article 23(5) of the PDP Act (repealed) (SG No 43 of 25.05.2018). It should be noted that long before the entry into force and application of the Regulation this Ordinance defined identical institutes and processes in relation to the protection and security of personal data, such as ‘impact assessment and levels’, ‘levels of

protection' and the obligation to take appropriate technical and organisational measures to protect personal data, etc. In addition to being highly assessed and recognised at European level, while it was effective it proved to be particularly important and useful in the practice both for exercising the control activities of the CPDP and for fulfilling legal obligations by data controllers and processors. It is therefore expedient, following appropriate adaptation, to retain it in the form of recommendations and to continue its use. This will be extremely useful for the practical implementation of the PDP Act and Regulation (EU) 2016/679.

With respect to the control activities of the CPDP, Article 58(1) of the Regulation specifies the different investigative powers, including in the form of data protection inspections (audits) to clarify facts and circumstances in relation to complaints, reports and in pursuance of CPDP decisions.

The purpose of the investigations is to establish the grounds and purposes for data processing, the data processing procedures, the compliance with data processing principles and the correspondence between data protection measures and risks to the rights and freedoms of natural persons.

Depending on the findings of the investigations and in order to achieve the objective of the law, Article 58(2) of Regulation (EU) 2016/679 provides for corrective powers of the CPDP which the supervisory authority can exercise and apply with respect to controlled entities. Depending on the circumstances in each particular case, the CPDP can issue 'warnings' or 'reprimands' respectively, as well as various orders to data controllers or data processors in relation to certain personal data processing operations, including to impose, instead of or in addition to such measures, an administrative fine or financial penalty in accordance with the procedure laid down in the Administrative Violations and Penalties Act.

Between 25 May 2018 and the end of the year, 611 investigations were assigned, of which:

– 77 inspections and

– 534 based on reports.

During the same period, 552 investigations (including investigations assigned before 25 May 2018) were completed, of which:

– 60 inspections and

– 492 based on reports.

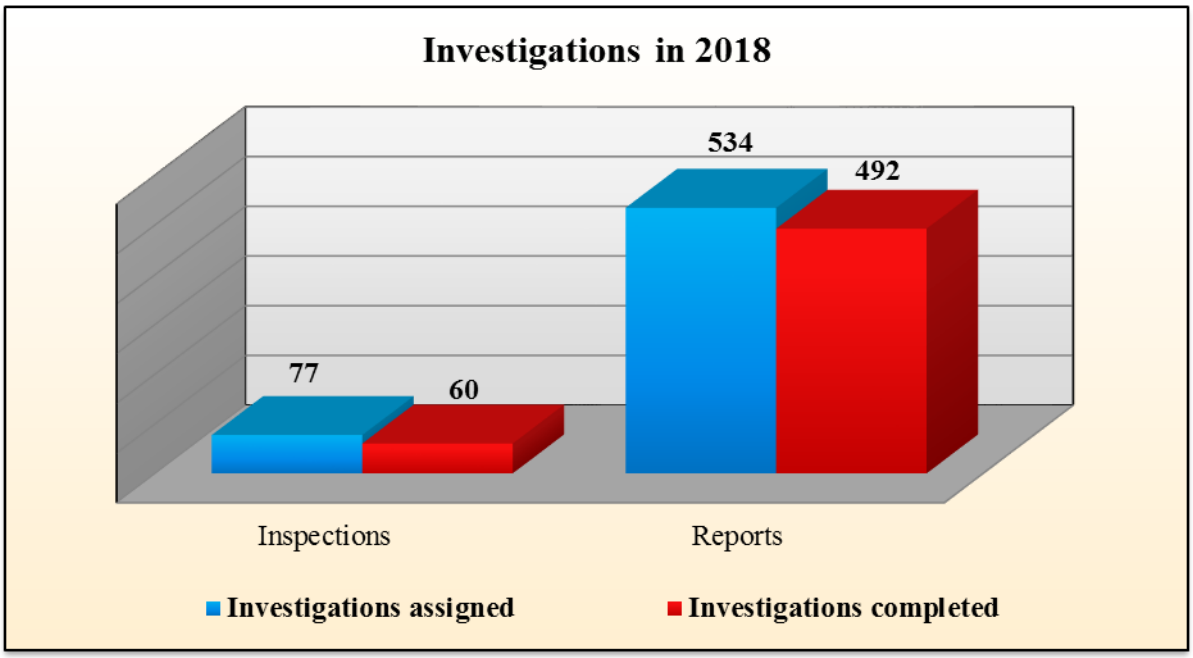

Figure 13

As a result of the investigations carried out, 58 statements of findings were drawn up, 9 reprimands were issued, 5 orders were issued to data controllers to bring processing operations into compliance with the provisions of Regulation (EU) 2016/679 and 1 statement establishing an administrative violation was drawn up. In 509 cases, no violation of the provisions of the Regulation was detected and responses were sent to the individuals concerned or the relevant reports were referred to the competent authorities.

The comparative statistics show a considerable decrease in the number of inspections due to the fact that ex-ante inspections are no longer carried out. There is a significant increase in the reports received by the CPDP for violated provisions of the Regulation and in the inquiries related to its application.

3.1. Investigations relating to data protection in accordance with Article 58(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council

- **Inspections/audits**

After 25 May 2018, investigations are carried out in the form of data protection inspections (audits) following a report of a breach of the provisions of the Regulation or following a decision of the CPDP in connection with a complaint or self-referral.

During the period under review, a total of 60 audits were carried out, 32 of which following a reported breach of the Regulation and 28 as a result of a decision of the CPDP. As a continuation of the existing practice, the largest number (36) of audits were carried out in connection with video surveillance and installation of video surveillance systems in condominiums and neighbouring low-rise buildings.

As a result of the audits carried out and the violations of the provisions of Regulation (EU) 2016/679 found (other than violations within the complaints procedures initiated in accordance with the CPDP's corrective powers under Article 58(2) of the same Regulation), 1 statement establishing an administrative violation was drawn up, 1 reprimand was issued and 5 orders were issued to the respective PDCs to bring processing operations into compliance with the relevant provisions.

- **Consideration of Requests**

Between the start of the application of Regulation (EU) 2016/679 and the end of 2018, 534 requests from individuals were received, including inquiries on topical issues related to the protection of personal data. The most frequently reported breaches were related to unlawful actions in relation to:

– receiving unsolicited commercial communications by e-mail and through phone calls;

– processing of personal data for direct marketing purposes without the consent of the individual having been provided;

– creating false profiles in social media;

– publishing of personal data in websites and possibility for unregulated access to such data; etc.

The CPDP addressed 492 requests by the end of the reporting period. As a result of established breaches of Regulation (EU) 2016/679, 8 reprimands were issued to the respective PDCs and in the remaining cases answers regarding the actions taken by the CPDP were sent to the individuals concerned.

3.2. Corrective powers under Article 58(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council

According to Article 58(2) of the Regulation, in the event of finding breaches the supervisory authority can exercise and apply different corrective actions with respect to the controlled entities. Depending on the circumstances in each particular case, the CPDP can issue 'warnings' or 'reprimands', as well as various 'orders' to data controllers or data processors in relation to certain personal data processing operations. These corrective powers are subject to appeal in accordance with the procedure laid down in the Administrative Procedure Code. The CPDP can impose, instead of or in addition to such measures, an administrative fine or financial penalty. In such cases administrative proceedings are initiated in accordance with the procedure laid down in the Administrative Violations and Penalties Act.

In 2018, following investigations carried out and violations of Regulation (EU) 2016/679 ascertained, the CPDP issued 9 reprimands and 5 orders to data controllers to bring processing operations into compliance with the provisions of the Regulation and drew up 1 statement establishing an administrative violation.

No reprimands and orders have been appealed to date.

Another important element the CPDP's activities is related to the fulfilment of the obligation of PDCs according to Article 33 of Regulation (EU) 2016/679 to notify the CPDP, respectively the individuals who are data subjects, of all personal data breaches. By the end of the reporting period, 33 such notifications were received from different PDCs located on the territory of the Republic of Bulgaria, EU Member States as well as non-EU countries. The notifications were registered in a special register.

Their analysis shows that incidents can be divided into two main groups – caused by human factors and caused by natural disasters.

The majority of incidents relates to the disclosure of data to third parties as a result of unintended technical errors caused by a human factor within the organisations and of the occurrence of technical problems in information systems. Another cause is the unauthorised access by unknown individuals external to the organisation through malicious attacks on the PDC's systems constituting different types of cybercrime, including theft of documents that contain personal data. The relevant law enforcement authorities have been notified as well. The CPDP was also notified of events relating to data security in Facebook and Google.

Another group of incidents is related to physical security breaches caused by natural disasters and elements such as the occurrence of fire in buildings, premises and systems of controllers where

personal data are processed. As a result of these events, documents containing personal data of individuals were partially and/or completely destroyed and significant material damage occurred.

Until the adoption of the new RACPDPA, whose draft contains allocation and description of the roles and responsibilities of directorates and departments and of actions involving the IMI system (taking into account the 'Methodology regarding the actions of the CPDP upon notifications of personal data breached in accordance with Article 33 of the General Data Protection Regulation'), by the end of 2018 the Control of APP Department had registered, reviewed and analysed the notifications received and orders are expected to be issued to relevant contractors for follow-up where required.

It is necessary to prepare and adopt a Risk Management Methodology and/or an audit questionnaire in these cases, including a standard form for notifications of data breaches. This is particularly important as all follow-up actions to be performed as set out in the above methodology are carried out based on and depending on the level of risk determined by the PDC. The CPDP needs to be able to verify beyond doubt the accuracy of this level based on clearly defined rules and not based on the subjective assessment by a particular employee.

VI. PROCEEDINGS FOR EXPRESSING OPINIONS AND PARTICIPATION IN COORDINATION PROCEDURES OF LEGISLATION ON MATTERS RELATING TO PERSONAL DATA PROTECTION

In 2018 the Commission for Personal Data Protection responded to 36 requests by issuing official opinions in accordance with Article 10(1)(4) of the PDP Act before 25 May 2018 and in accordance with Article 58(3)(b) of the General Data Protection Regulation after the latter came into force.

1. Opinions on issues relating to personal data protection

During the reporting year, a trend was observed of approaching the CPDP with requests for opinions regarding various topics from public life and from diverse data controllers. The analysis that can be made with regard to the subjects of such opinions and the controllers that requested them is that the subject of personal data protection becomes more relevant in all areas of modern society, especially after the entry into force of the new rules on personal data protection and bearing in mind the additional obligations imposed on controllers. From 25 May 2018, with the harmonization of data protection rules in the European Union and their modernisation in the light of new technologies, individuals are given greater control over their personal data in the digital world, and businesses benefit from greater clarity and legal certainty and a lower bureaucratic burden An increasing number of individuals who are data subjects are addressing the CPDP with different requests in relation to the protection of their personal data. After the obligation to register in the electronic register of PDCs maintained by the CPDP ceased to be in force, PDCs have sent to the Commission various inquiries and consultations on the preparation for the implementation of the General Data Protection Regulation.

1.1. Opinions regarding the obligation to declare property and income in accordance with the Counter-Corruption and Forfeiture of Illegally Acquired Assets Act (CCFIAA Act)

1.1.1. In 2018 the CPDP was approached by the Counter-Corruption and Forfeiture of Illegally Acquired Assets Commission (CCFIAA Commission) with questions regarding the application of the General Data Protection Regulation in the course of implementing the provisions of the new Act regarding the obligation to publish the declarations of the obliged persons that contain personal data.

The CPDP expressed the opinion that the PDCs have a legal obligation to maintain an online public register of the declarations submitted (according to Article 6(1)(c) of the General Data Protection Regulation).

The published declarations of the first category of obliged persons – those who hold senior public positions within the meaning of Article 6 of the CCFIAA Act – should not contain the following data: PIN, number of the identity document, address, signature of the declarant, bank account numbers and bank cards. With regard to third persons, only the personal data expressly provided for in the law are subject to publication.

When the declarations of the second category of obliged persons – officials within the meaning of § 2(1) of the Supplementary Provisions of the CCFIAA Act – are published, the personal data that can be published online are as follows: full name of the declarant, place of employment, position, control number of the declaration, as well as the public part concerning the interests in accordance with § 2(3) of the Supplementary Provisions of the CCFIAA Act.

Because the statutory time limit for access to the declarations published in the internet has not been defined, the principle of 'storage limitation' envisaged in Article 5(1)(e) of the General Data Protection Regulation shall be applied. According to this principle, data shall be stored for no longer than is necessary for the purposes for which they are processed.

The consent to the processing and disclosing personal data to third parties given at the end of the declaration is contrary to the provisions of the General Data Protection Regulation because it is not voluntary (it is a condition for the validation of the declaration). In this regard, the refusal to give said consent results in the impossibility of fulfilling the legal obligation to submit a declaration, and the failure to fulfil this obligation leads to administrative penal responsibility in accordance with the procedure laid down in the CCFIAA Act.

1.1.2. Request from the Inspectorate with the Supreme Judicial Council regarding the application of Regulation (EU) 2016/679 in the enforcement of the provisions of the Judicial System Act (JS Act) in its part concerning the publication of declarations of property and interests of magistrates.

After analysing the questions asked, the CPDP took the view that the publication of the names of the spouse of the declarant – judge, prosecutor or investigator or another person holding a senior public position – is a fulfilment of a legal obligation for the PDC and is not contrary to the principles of Regulation (EU) 2016/679.

The names of the person with whom the declarant lives as a stable non-marital partner shall be published in the event that no declaration of refusal has been filed pursuant to Article 175b(7) of the JS Act.

The publication of the names of minor children of the declarant is excessive and does not meet the principal requirement for increased protection of the rights and interests of children.

The balance between the public interest in publicity and transparency, on the one hand, and the protection of the privacy and personal data of natural persons indicated by the declarant in relation to the circumstances of property and income and of natural persons in whose activities the declarant has indicated a private interest, on the other hand, can be achieved by publishing minimized personal information in the form of initials of the persons concerned as the private interest is established by the administrative head of the relevant body of the judiciary who has access to the full information.

1.1.3. Another opinion expressed by the CPDP in 2018 is on a request by the CCFIAA Commission for direct access to the National Database 'Population' (NPD 'Population').

The request quotes that in the exercise of their powers the authorities of the CCFIAA Commission can request assistance, information and documents, including in electronic form, from state and municipal authorities, traders, credit institutions, notaries and enforcement agents, as well as from other natural persons and legal entities.

Until the entry into force of the CCFIAA Act, the relations relating to the access to the NDB 'Population' were regulated through Agreements for access provided by the Ministry of Regional Development and Public Works (MoRDPW). The MoRDPW has informed the CCFIAA Commission that in order to provide access to the personal data of the persons checked by the Commission it needs the permission of the CPDP in accordance with Article 106(1)(3) of the Civil Registration Act (CReg Act).

In connection with this, the CCFIAA Commission requested the CPDP to issue a permission for granting direct access to the NDB 'Population' on the grounds of Article 10(1)(4) of the PDP Act in conjunction with Article 106(1)(2) of the CReg Act.

When considering the request for an opinion, the CPDP took into account the fact that the CCFIAA Commission regulates the public relations relating to counteraction to corruption, as well as the procedure and conditions for forfeiture to the exchequer of illegally acquired assets. The objectives of the law are to protect the interests of society through combating corruption and preventing illegal acquisition and disposal of property.

In order to achieve these goals, the competent public authority – the CCFIAA Commission – has three main groups of powers:

– to verify the information from the declarations of property and interests submitted by persons holding senior public positions in terms of the authenticity of the declared facts in accordance with the procedure laid down in Article 43 et seq. of the CCFIAA Act;

– to counteract corruption by revealing actions of persons holding public positions in accordance with the procedure laid down in Article 82 et seq. of the CCFIAA Act, including by conducting operational-search activities;

– to establish illegally acquired assets, including to conduct inspections in accordance with the procedure laid down in Article 114 of the CCFIAA Act.

The functions and tasks of the CCFIAA Commission are interrelated. For example, a check to identify and seize illegally acquired assets can be initiated in the event of finding inconsistency or failure to file a declaration by a person holding a senior public position, as well as in the event of a conflict of interests established by an enforceable instrument. At the same time, the provisions of the CCFIAA Act for accessing different databases in the exercise of the institution's powers are not consistent.

In view of the above, on the grounds of Article 106(1)(3), third proposal of the CReg Act in conjunction with Article 106(1)(2) of the CReg Act, the CPDP allows the granting to the CCFIAA Commission direct access to the NDB 'Population' in respect of the data volume specified in the request so that the Commission can fulfil its statutory powers specified in Articles 43, 82 and 114 of the CCFIAA Act.

1.2. Opinions relating to the fulfilment of the obligations to protect the rights of individuals with regard to the processing of personal data in the judicial system

1.2.1. Request from the Legal and Institutional Affairs Committee to the Plenum of the Supreme Judicial Council (SJC) in connection with the application of the General Data Protection Regulation in the judiciary system

Regarding the questions posed by the Plenum of the Supreme Judicial Council, the CPDP is of the opinion that Regulation (EU) 2016/679 provides for a specific legal regime for courts which is characterised by a pronounced dualism in their capacity as PDCs. Courts process personal data in the course of performing their judicial functions, on the one hand, and as 'ordinary' PDCs, on the other hand.

The legal dualism is also reflected in the supervisory mechanism for the implementation of Regulation (EU) 2016/679. The CPDP is the body that monitors and enforces the rules for the processing of personal data by the courts as 'ordinary' controllers (the so-called general supervision). According to the AASPDP Act which is to be discussed at second reading by the National Assembly, the SJC Inspectorate is to supervise the processing of personal data by the courts, the prosecutor's offices and the investigative bodies when they perform their functions of

judiciary bodies and to consider complaints from individuals concerning the processing of their personal data (the so-called special supervision).

When the time limits for storing personal data are determined, the principle of 'storage limitation' envisaged in Article 5(1)(e) of the General Data Protection Regulation applies: when the statutory time limits are not defined by law, personal data shall be stored for no longer than is necessary for the purposes for which they are processed.

1.2.2. Request from the SJC for the issuance of methodological guidelines to the bodies of the judiciary with a view to the correct and uniform application of the PDP Act, Regulation (EU) 2016/679 and Directive (EU) 2016/680, in particular when instruments of judiciary bodies and information on their activities are published on their official websites

Recognising that Regulation (EU) 2016/679 excludes from the CPDP oversight the personal data processing activities of courts acting in their judicial capacity, the CPDP expressed the following position in connection with the request for an opinion:

Article 55(1) of Regulation (EU) 2016/679 outlines the competence of the CPDP for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with the Regulation on the territory of Bulgaria. At the same time, Article 55(3) of the Regulation contains a derogation according to which national supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity. Similar provisions are introduced in Article 45(2) of the Directive on personal data protection in police and criminal matters (Directive (EU) 2016/680).

The competence of the CPDP should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making (Recital 20 of Regulation (EU) 2016/679).

In connection with the request by the SJC for issuance of mandatory instructions of the CPDP on the grounds of Article 10(1)(5) of the PDP Act it should be noted that the mandatory instructions of the CPDP are a coercive administrative measure which has a legally binding effect and whose implementation is consolidated with state coercion. By their very nature, the instructions are a manifestation of subordination, of relations of authority and subordination that characterise the administrative relations, thus binding the PDCs with a specific behaviour perceived as lawful by the CPDP. In view of this, the mandatory instructions of the CPDP are objectively an administrative instrument within the meaning of Article 21(1) of the APC, notably they create obligations, respectively affect the powers of the entities concerned. In the specific case, there is no legal relationship with respect to judicial activity which implies the issuance of mandatory instructions

within the meaning of Article 10(1)(5) of the PDP Act as the case concerns the operational activity and the independence of the judicial system explicitly excluded from the application of Regulation (EU) 2016/679.

As regards the processing of personal data of judicial staff, this should be subject to the general rules laid down in the new legal framework in the field of personal data protection. Such processing is carried out in the context of employment/service relationships for which the CPDP has competencies and supervisory powers.

1.2.3. Request from the Sofia Bar Council in connection with limiting the access to electronic cases via an electronic portal for inquiries into cases based on the search criteria 'PIN' and 'name' of a natural person who is a party to a case

In order to render an opinion, the CPDP took into consideration that the processing of the data through providing information regarding cases does not take place within the court's proper judicial functions, but in the course of accompanying filing and information activities. Therefore the CPDP is competent to supervise and issue opinions regarding the compliance with the principles and rules of Regulation (EU) 2016/679.

Access to information in court proceedings is regulated in the relevant procedural laws, as well as in the Rules of Administration in the Courts (RAC) which were published in SG No 68 of 22 August 2017 and were adopted with a decision of the Plenum of the SJC on the grounds of Article 342(1) of the Judicial System Act. The provision of Article 77(1) of the RAC establishes a general obligation for the judicial administration to ensure 'openness, credibility and completeness of the information collected and held by the courts'. Paragraph 5 of the same article permits information regarding cases to be provided by means of remote access. The CPDP also took into account the fact that Article 77(3) of the RAC provides for a simplified procedure for access to information regarding cases by lawyers in accordance with Article 31 of the Bar Act. According to this procedure lawyers are entitled to free access and can consult information without a power of attorney for the specific case only on the basis of their capacity as lawyers, which they must certify by presenting a lawyer's card.

The CPDP concluded that the provision of the opportunity to inquire into registers of judicial authorities, including in alphabetical directories, using the three names or the PIN of an individual is admissible and lawful after the user has authenticated himself or herself with the identification means required by the information system.

1.2.4. Opinion regarding the processing of personal data by the Prosecutor's Office of the Republic of Bulgaria (PORB) when publishing press releases and providing information for journalistic purposes

The CPDP is of the opinion that, in order for the processing to be lawful, the controller, or the PORB in the specific case, must have independent legal grounds under Article 6 of the General Data Protection Regulation, respectively under Article 9 of the Regulation where special categories of (sensitive) personal data are concerned. In such cases the provision of Article 85 of the General Data Protection Regulation shall also be taken into account. According to this provision, Member States shall by law reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes. The rights in question are of equal strength and, therefore, a fair, reasonable and proportionate balance should be sought in their exercise and protection.

The prosecutor's office and other judicial bodies, in view of their statutory competence, do not process personal data for journalistic purposes and the special rules applicable to the media do not apply to them. Nevertheless, the publication of information from pre-trial proceedings, including personal data, could in certain cases be considered necessary for the performance of a task carried out in the public interest within the meaning of Article 6(1)(e) of the General Data Protection Regulation. The public interest could be justified by various factors to be assessed by the PORB.

The disclosure of personal data of accused persons in pre-trial proceedings on the prosecution offices websites and the provision of such data to the media for journalistic purposes is lawful when there is a legal obligation or an overriding public interest exists. In cases where, in view of the purpose of public interest, it is impossible or inappropriate to publish the information in an anonymised or pseudonymised form, the indication of the name, position or place of work of the accused person would be sufficient to achieve public awareness, whereas the publication of a PIN, address, links with third parties outside the process, etc. would be excessive.

As a general rule, personal data of other participants in pre-trial proceedings, such as witnesses, experts or third parties related to these categories, etc., should not be published or otherwise disclosed insofar as there is no legal obligation or overriding public interest. An exception can be made with respect to persons holding senior public positions within the meaning of Article 6 of the CCFIAA Act or other persons who, by reason of the nature of their activity, have an influence on society or where the publication of the information protects the vital interests of the data subject.

1.3. Requests for opinions relating to the precise definition of the 'data controller' and the 'data processor'

1.3.1. Request from the Bulgarian Association of Clinical Research (BACR) concerning the identification of the ‘controller’ and ‘processor’ of the personal data of persons involved in clinical trials

The BACR would like to understand the role of the medical treatment facility and the investigator regarding the processing of personal data in the course of each specific clinical trial. The CPDP is of the opinion that the sponsor of a clinical trial has the capacity of a PDC as it determines the purposes and the means of processing said data. It is the PDC that determines the role of the processor and, in principle, the other three entities, notably the contract research organisation, the medical treatment facilities and the medical specialists – investigators, should have the capacity as processors.

It is important to point out that according to Article 82(4) of the General Data Protection Regulation each controller or processor shall be jointly responsible for any damage caused by unlawful processing of personal data.

1.3.2. The CPDP received a request for an opinion from Speedy AD regarding the quality in which Speedy AD processes the personal data of the sender or the recipient of the universal postal service – that of a PDC or that of a data processor.

Within the motivational part of the opinion, a detailed analysis is made of the allocation of roles and responsibilities between controllers and processors and their main purpose, namely to ensure that the processing of personal data takes place in accordance with the requirements of Regulation (EU) 2016/679 and accordingly ensure the protection of the rights of data subjects.

The opinion of the CPDP is that, in general, companies that provide services subject to strict and comprehensive legal regulation on the basis of a licence or analogous individual authorisation from the State and that are subject to control by explicitly designated public authorities cannot in principle be regarded as data processors but are standalone PDCs. Examples of such PDCs are postal operators, banks and insurance companies.

In addition, given the diversity of public relations and in accordance with the principle of accountability regulated in Article 5(2) of Regulation (EU) 2016/679), participants in commercial and civil relations should determine on their own in each individual case their legal relationships with respect to the personal data they process – standalone controllers, controller and processor or joint controllers. Their choice should not be formal and should ensure the highest degree of compliance with the requirements of Regulation (EU) 2016/679 and effective protection of the rights of data subjects.

An identical opinion was expresses in connection with a request from Bulgarian Posts EAD.

1.3.3 The CPDP expressed its opinion on issues relating to the implementation of the General Data Protection Regulation when company cards for sport are provided to employees.

Many similar inquiries are made to the CPDP regarding the provision of company cards for sports to employees. It is essential to define the legal relationships between the participants as well as the grounds for processing the personal data of the employees who use the service. In this respect, the CPDP expressed the following opinion on issues relating to the implementation of the General Data Protection Regulation when such services are provided:

1. In its capacity as a PDC, the company (employer) may provide personal data of its employees to a company that offers the Multisport Card service, subject to explicit consent by the employees within the meaning of Article 6(1)(a) in conjunction with Article 4(11) of Regulation (EU) 2016/679).

2. It is acceptable that users of the service are also third parties, e.g. spouses and children of the employee, and consent should also be given as a basis for the lawfulness of the processing as regards their personal data.

3. As the employer and the company that offers the Multisport service process the personal data for different purposes, store them for different periods, transmit them to different recipients, apply different technical and organisational protection measures, etc., they are separate PDCs and therefore do not fall under the hypothesis of a data controller – data processor within the meaning of Article 28 of the General Data Protection Regulation.

4. When processing the personal data, both companies should strictly observe their obligation to provide the information referred to in Articles 13 and 14 in accordance with the requirements of Article 12 of Regulation (EU) 2016/679.

1.3.4. The CPDP also expressed an opinion on issues relating to the identification of the ‘controller’ and the ‘processor’ of personal data in the relations between insurance companies and medical treatment facilities.

The opinion is intended to provide guidance on identifying the ‘controller’ and the ‘personal data processor’ within the meaning of the General Data Protection Regulation in the case of contractual relations between insurance companies and medical treatment facilities in the context of the applicable special legislation in the field of healthcare:

1. Personal data processing activities in connection with medical examinations and tests cannot be carried out in the name of the insurer (controller). The reason for this is that such activities cannot be performed by the insurer but only by an organisation which is a ‘medical treatment facility’ within the meaning given by the Medical-Treatment Facilities Act.

2. Special legislation in the field of healthcare (laws and regulations) provides for a number of obligations, measures, mechanisms, procedures and conditions for the protection of health information containing personal data; a contract within the meaning of Article 28 of the General Data Protection Regulation cannot serve as grounds for derogation from these.

3. Taking account of their activities and the law applicable to them, the participants in commercial and civil relations should determine on their own their legal relationships with respect to the personal data they process – standalone controllers, controller and processor within the meaning of Article 28 or joint controllers within the meaning of Article 26 of the General Data Protection Regulation. Their choice should ensure not only in form but also in substance compliance with the requirements of Regulation (EU) 2016/679 and effective protection of the rights of data subjects. It should also be borne in mind that the provision of services whereby personal data is frequently exchanged between the contracting entity and the contractor does not automatically lead to the occurrence of a legal relationship between a data controller and a data processor within the meaning of Article 28 of the Regulation.

1.4. Opinions relating to video surveillance activities

1.4.1. Request from the Ministry of Education and Science (MoES) regarding the implementation of activities relating to controlling the organisation, conducting and evaluation of state matriculation exams (DZI), in particular video surveillance in the examination rooms during the DZI.

The request for an opinion raises the question of the lawfulness of the video surveillance. The opinion of the CPDP is that, from the point of view of the protection of personal data, video surveillance during DZI is an act of processing of personal data and as such can be done lawfully on the grounds of 'performing a task of public interest' within the meaning given by Article 4(1)(5) of the PDP Act and subject to the principles referred to in Article 2(2) of the law.

In order to create legal certainty, when the application of the General Data Protection Regulation starts on 25 May 2018 it would be advisable to amend and supplement Ordinance No 11 of 1.09.2016 on the evaluation of pupil's learning outcomes, issued by the Minister of Education and Science, so that it explicitly states that video surveillance can be performed during DZI as one of the measures to prevent bad practices and protect public interest.

1.4.2. One of the most important opinions delivered by the CPDP in 2018 was related to the request filed by the Chairperson of the State Agency for Child Protection (SACP) in connection with the great public response and public interest on issues concerning the introduction of video surveillance in childcare facilities (nurseries, kindergartens) as well as in schools.

The CPDP delivered an opinion as follows.

From the perspective of personal data protection, the introduction of video surveillance in nurseries, kindergartens and schools is permissible with a view to improving the security and transparency of care as well as solving emerging conflicts in childcare facilities as well as in schools, and with a view to protecting the life and health of the most vulnerable category of society as a whole – children and minor Bulgarian citizens.

At the same time, the public interest in introducing transparency in the care of children and adolescents should be taken into account because the issue of the safety, life and health of Bulgarian children and pupils is of paramount importance to society as a whole.

In the specific case, the provisions of Regulation (EU) 2016/679 applicable from 25 May 2018, as well as the national regulations in force until 25.05.2018 and laid down in the PDP Act should be applied as a legal prerequisite. In this case, two of the alternative grounds for lawfulness of the processing stipulated in Article 6 of Regulation (EU) 2016/679 can be applied, as follows: Article 6(1)(d) – processing is necessary in order to protect the vital interests of the data subject or of another natural person, as well as Article 6(1)(e), first proposal – processing is necessary for the performance of a task carried out in the public interest. The provisions of Article 4(1)(4) and (5) are valid in the extant PDP Act.

In order to protect the rights of children and pupils, video surveillance in dormitories, sanitary facilities, children's restrooms and personal hygiene premises is unacceptable, as installing devices in these premises would mean that children are not allowed to have privacy and preserve their personal dignity, as well as because such installing constitutes a violation of the right to privacy.

It is permissible to perform video surveillance in the common areas and courtyards to ensure the safety of children and pupils in games, activities and in their free time. Such video surveillance is only permissible in places of work if these are separate from dormitories and restrooms and in common areas of the building.

The PDCs need to take account of their obligations and responsibilities arising from the provisions of Regulation (EU) 2016/679 and bring data-processing activities through video surveillance in line with the new standards for personal data protection introduced by the provisions of the Regulation.

PDCs must notify the parents/guardians of children and minor pupils of the use of technical devices for video surveillance and control by placing information boards in a prominent location. Thus, the actions of the PDCs will also be in line with the provisions of Article 32(2), first proposal of the Constitution of the Republic of Bulgaria.

1.4.3. The CPDP received a request for an opinion on the installation of entrance and exit facial recognition cameras linked to the electronic register of a vocational high school. The request is based on recommendations issued by a regional education authority competent for the territory of the school and is supported by arguments about the need to effectively control pupils' attendance in classroom periods, protect pupils' health, prevent the risk of dropping out of school and social exclusion, prevent unauthorised spending of financial resources, including fair allocation and use of social products, etc. All these reasons stated in the recommendations are based on separate legal grounds.

The CPDP is of the opinion that certain categories of personal data are, by their very nature, particularly sensitive from the point of view of the fundamental rights and freedoms of individuals and that special protection is provided for them. These also include biometric data which, according to Article 4(14) of the General Data Protection Regulation, are personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

The General Data Protection Regulation prohibits the processing of special categories of personal data including biometric data except where one of the exceptions explicitly specified in Article 9(2) of the Regulation applies. A possible hypothesis applicable in the case under consideration could be the one specified in Article 9(2)(g) – processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The threshold for justifying the proportionality of processing sensitive data is even higher when data subjects are children, as is the case.

In view of the above arguments, the CPDP is of the opinion that, without denying or diminishing the public significance of the educational and social objectives pursued, they are not proportionate to the highly intrusive processing of sensitive personal data proposed. For these reasons, the use of face recognition cameras in schools is not in line with the mandatory requirements of the General Data Protection Regulation with respect to the lawfulness and proportionality of the processing of personal data.

1.5. Opinions relating to personal data processing by employers

1.5.1 Questions related to the processing of personal data by an employer when conducting tests of employees/workers for alcohol and other intoxicating agents

In relation to the questions raised in the request for opinion, the CPDP expressed the understanding that, insofar as the use of alcohol and intoxicating agents influences the functionality of the human organism, the results of these tests can be qualified as 'data concerning health' (Article 4(15) of Regulation (EU) 2016/679), respectively special ('sensitive') categories of personal data within the meaning of Article 9(1) of the Regulation.

The test results can be processed on the grounds of Article 9(2)(b) in connection with the provisions of the Labour Code concerning the employee's obligation to appear at work in a condition in which he/she can perform the assigned tasks, and not to use alcohol or other intoxicating substances during working hours. This obligation, when justified doubts exist, gives rise to the right of the employer to collect evidence of possible unlawful behaviour on the part of the worker/employee in order to take steps to invoke the latter's disciplinary liability.

The employer must fulfil the obligation to inform the employees about the envisaged processing as specified in Articles 12 and 13 of Regulation (EU) 2016/679, as well as to take appropriate technical and organisational measures in view of the high sensitivity of data from tests for alcohol and other intoxicating substances.

The results of the tests carried out should be processed in compliance with the 'storage limitation' principle, namely they shall be kept for no longer than is necessary for the purposes for which the personal data are processed (Article 5(1)(e) of Regulation (EU) 2016/679). In the case in question, the prescription and limitation periods set out in the Labour Code for judicial remedies for rights and interests can be applied.

In addition, the test results must be duly recorded, indicating the legal basis for their performance, the employee's explanations, the reasons, as well as the witness information if the record is signed by witnesses.

1.5.2. In 2018 the CPDP received a request from the Ombudsman of the Republic of Bulgaria for an opinion on the application of Regulation (EU) 2016/679 in connection with the certification of temporary incapacity to work before an employer. The request was sent in connection with a complaint to the Ombudsman concerning the existing procedure for certifying temporary incapacity to work before employers. According to the citizen who sent the complaint, the indication of the particular disease in the sick leave certificate is contrary to the protection of the information concerning the health of citizens provided for in the Health Act and in Regulation (EU) 2016/679.

The reasoning of the CPDP is that the Health Act is the statutory instrument which regulates public relations related to the protection of citizens' health. The issuing of a sick leave certificate is part of the medical expert examination of working capacity. The latter includes expert examination of temporary incapacity to work and expert examination of permanently reduced capacity for work.

On the other hand, the Ordinance on Medical Expertise (ME Ordinance) defines the criteria, principles and procedures for carrying out medical expert examinations. It also includes an expert examination of the temporary incapacity to work carried out by the medical/dental practitioner, by the Medical Advisory Commissions, by the Territorial Expert Doctors' Commissions and by the National Medical Advisory Commission.

The Ordinance on the procedure for submission to the NSSI of the data from the sick leave certificates issued and the appeal decisions (adopted by Council of Ministers Decree No 241 of 4 August 2014) sets out the procedure for submission by the medical expertise bodies to the NSSI of the data contained in the sick leave certificates issued and in the appeals decisions. The data contained in sick leave certificates are provided to the NSSI by medical/dental practitioners or medical advisory commissions. According to Article 13 of the Ordinance on the issuance of sick leaves for temporary incapacity to work, the data shall be entered by the persons specified above, shall undergo formal and logical control and shall be stored, after which the patient's sick leave shall be printed, signed and stamped with the seal of the medical treatment facility and handed over to the person. Annex No 3 [to the Ordinance] is the standard form of the sick leave certificate. One of the mandatory requisites is the diagnosed disease.

The CPDP has decided that the indicating of the particular disease on the sick leave certificate when temporary incapacity to work is certified before the employer is not contrary to the provisions of Regulation (EU) 2016/679. The data are processed on legal grounds in accordance with Article 6(1)(c) of the General Data Protection Regulation, respectively in accordance with Article 9(2)(b) of the Regulation, in conjunction with Article 13 of the Ordinance on the procedure for submission to the NSSI of the data from the sick leave certificates issued and the appeal decisions.

1.6. Opinions regarding the processing of data of deceased persons

In 2018 the CPDP was approached on several occasions with inquiries relating to personal data of deceased persons. On one of the issues raised (provision of personal data of deceased persons by a municipality in connection with the accountability to the Regional Health Insurance Fund), the CPDP expressed the following opinion:

The preamble of Regulation (EU) 2016/679, notably recital 27, states that **the Regulation does not apply to the personal data of deceased persons** and that Member States may provide for rules regarding the processing of personal data of deceased persons. In the case in question, the municipal administration can, on a monthly basis, provide the medical centre that services the settlements in the municipality with the requested information (such as names and personal

identification numbers of the deceased persons who have been residents in the municipality of Brezovo) in relation to the accountability to the Regional Health Insurance Fund in order to prevent abuse of data of deceased persons.

The controller (the municipality concerned) should take appropriate measures to prevent adverse effects on the rights and freedoms of others and/or on the public interest. In such cases the controller can provide data only if legal grounds for such provision exist.

1.7. Opinions regarding the processing of data in connection with the fulfilment of obligations of controllers under the Access to Public Information Act

1.7.1. In 2018, the inquiries to CPDP for opinions concerning the provision of information that contains personal data requested under the Access to Public Information Act (API Act) increased in number. In connection with a similar question concerning in particular the enrolment of children in kindergartens, the CPDP is of the opinion that the protocols from medical advisory commissions provided by the parents of children with special educational needs contain personal data concerning the health of children which constitute special categories of personal data within the meaning of Article 4(15) and Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council. In this case, none of the eligibility conditions for the processing of data from these documents (such as disclosure through transfers to third parties, dissemination or other means by which the data become available) is met, so the controller should not provide the applicant for the information according to the API Act with copies of the protocols from medical advisory commissions. Even deleting the children's names from copies of the protocols from medical advisory commissions can lead to the identification of a specific child due to the limited number of children with special educational needs in the kindergarten and the possibility for them to be easily identified, including based on external features.

1.7.2. Another interesting request for an opinion on issues concerning the provision of information that contains personal data requested under the API Act concerns a public sector controller – the Ministry of Transport, Information Technology and Communications (MoTITC). The opinion was requested in connection with the controller receiving a request for access to public information. The controller was requested to provide a 'list that contains the full names of all advisers to the Ministers for Transport, Information Technology and Communications during the period 1.01.2008—3.09.2018 and information regarding the period in which the persons described were advisers to the Ministry of Transport, Information Technology and Communications'.

The CPDP was asked whether the provision of the requested information was in conformity with the General Data Protection Regulation. The CPDP's opinion on this is that the list that contains the full names of all advisers to the Ministers for Transport, Information Technology and

Communications during the period 1.01.2008—3.09.2018 and the information regarding the period in which the persons described were advisers to the MoITC should be considered as public information which does not constitute personal data protected under the General Data Protection Regulation.

1.7.3. The CPDP delivered an opinion in connection with a question of a Member of Parliament in the framework of a parliamentary scrutiny procedure concerning the provision of information regarding additional remuneration paid/accrued in 2018 by the Ministry of Foreign Affairs and other ministries.

The question concerned the possible breach of provisions on the protection of personal data if the ministers respond in full to the question posed by the Member of Parliament. The CPDP expressed the following opinion:

The information regarding the additional remuneration paid/accrued in 2018 by the Ministry of Foreign Affairs requested in a question posed by the MP in the framework of parliamentary scrutiny over the executive in accordance with the procedure laid down in Article 90 of the Constitution of the Republic of Bulgaria does not constitute personal data and as such does not fall within the scope of the existing legislation in the field of the personal data protection and privacy.

1.8. Opinions relating to the implementation of new obligations of data processors and controllers stemming from the new legal framework in the field of data protection

1.8.1. In connection with the new obligation of PDCs to appoint data protection officers, a practice was established during the reporting period for data controllers to consult with the CPDP in relation to this obligation. The Ministry of Defence sent an inquiry asking questions regarding the designation of DPOs in the units of the Ministry. The question was also asked if it was possible to create a centralised unit at the Ministry of Defence directly reporting to the data controller designated for the Ministry and said unit to be responsible for the implementation of the requirements of Regulation (EU) 2016/679 with respect to the Ministry, the units that report directly to the Minister of Defence and the Bulgarian Army.

The CPDP's opinion was that, according to the provision of Article 37(3) of Regulation (EU) 2016/679, there was no legal impediment to the establishment of a centralised unit responsible for the implementation of the requirements of the Regulation by the Ministry of Defence, the units that report directly to the Minister of Defence and the Bulgarian Army and to designate a single DPO in said unit.

1.8.2. Request for an opinion on whether it is permissible for joint controllers to rely on a single statement of consent on the part of the data subject whose data they process in order to offer

direct marketing. The position of the CPDP is that there is no legal impediment for joint controllers to use a 'single consent' on the part of the data subject whose data are processed in order to offer direct marketing provided that the specific requirements for consent laid down in Article 4(11) and in Article 7 of Regulation (EU) 2016/679) are complied with and that the obligation for transparent processing in accordance with Article 5(1)(a), Article 13 and Article 26(1) of the General Data Protection Regulation is fulfilled.

1.9. Opinions relating to processing of special categories of personal data

1.9.1. The Bulgarian Medical Association sent an interesting request for an opinion which raised the following two issues:

1. If the control bodies referred to in Article 72(2) of the Health Insurance Act (HI Act) have the power to require that original health records be provided to patients for the purposes of inspections and said records to be taken outside the territory of the respective medical treatment institution in view of the exception provided for in Article 6(1)(c) and (d) of Regulation (EU) 2016/679.

2. If the control bodies referred to in Article 72(2) of the HI Act have the power to require certified copies of health records to be provided to patients for the purposes of inspections and said copies to be taken outside the respective medical treatment institution in view of the exception provided for in Article 6(1)(c) and (d) of Regulation (EU) 2016/679.

The HI Act regulates public relations related to health insurance in the Republic of Bulgaria. By its nature, this is an activity related to the collection of health insurance contributions and premiums, the management of the funds raised and their spending for the purchase of health activities and services and for the payment of goods. It should be noted that this activity is strictly regulated. The Manager of the Health Insurance Fund (NHIF) exercises the overall control of mandatory health insurance activities. According to Article 72(2) of the HI Act, control over the implementation of contracts with the NHIF for the provision of medical and/or dental care is exercised through inspections.

Account is taken of the provisions of the National Framework Contract for Medical Activities (NFCMA) between the NHIF and the Bulgarian Medical Association for 2018 which determines the health and economic, financial, medical, organisational and management, information and legal and deontological frameworks according to which the contracts between the NHIF and health care providers (HCPs) are concluded. Article 387 of the NFCMA concerns the initiating of inspections by the competent bodies of the NHIF/RHIF. Paragraph 4 contains the requirement that until the end

of the inspection the medical care providers are obliged to provide the control bodies with copies of the documents necessary for the inspection **certified by signature and stamp**.

The CPDP expressed the opinion that the control bodies referred to in Article 72(10) of the HI Act may require only a certified copy of the patient records required for the purpose of conducting inspections of medical activities on the grounds of Article 387(4) of the National Framework Contract for 2018.

1.9.2. During the reporting period the CPDP received another interesting request from the director of a psychiatric hospital in connection with a request from a private enforcement agent to disclose information regarding a natural person against whom enforcement proceedings have been initiated. According to the PEA, the information will help to establish with certainty whether the debtor is placed under incapacity.

The Private Enforcement Agents Act (PIA Act) regulates the organisation and legal position of private enforcement agents. According to Article 16(1) of the Act, PEAs are entitled to access personal data of the debtor where this is required for the execution. On the other hand, Article 431 the Civil Procedure Code regulates the powers of private enforcement agents to request documents from and send inquiries to third parties.

Private enforcement agents have the right to access information in the judicial and administrative services, including the bodies of the National Revenue Agency, the territorial units of the National Social Security Institute, the Central Depository, the persons which keep registers of government securities, the control bodies under the Road Traffic Act and other persons *which keep registers of property or have data on property*. PEAs can make inquiries and obtain information in relation to enforcement and request copies and extracts of documents. The provision quoted concerns the access to information that is relevant only to the **property status** of a debtor. Data regarding a potential disease contained in the medical records kept by the hospital would not be relevant to the person's property status, therefore the private enforcement agent would not be able to rely on that rule.

Ordinance No RD-02-20-9 of 21 May 2012 on the functioning of the unified system of civil registration, issued by the Minister of Regional Development and Public Works, regulates the procedure and the manner of establishing and maintaining the population register, as well as the procedure for providing access to and data from registers of civil status records, the National Electronic Register of Civil Status Records and the Population Register. The provision Article 100 of the aforementioned Ordinance is that the electronic personal registration card contains information regarding the type of **legal restriction** (if any such restriction has been imposed on the person) which may be **full legal disqualification, limited interdiction**, deprivation of parental

rights, limited parental rights. The above data is maintained by processing a Legal Restrictions Notice updating document. The updating document is processed by an official of the municipal administration where the permanent address of the person is located.

The CPDP expressed the opinion that there are no legal grounds for the provision of the data by the director of the state psychiatric hospital to the private enforcement agent. The private enforcement agent can obtain the information requested and required for the purposes of the enforcement by making an inquiry in the population register.

1.9.3. The Social Assistance Agency (SAA) approached the CPDP with a request for an opinion on issues concerning the publishing of personal data, including medical data, on the Agency's website in connection with the implementation of special measures for the adoption of a child with a health problem, special need or over seven years of age.

According to Ordinance No RD-07-7 of 5.10.2010 on the conditions and procedure for keeping and storing full adoption registers, the SAA must undertake special measures with respect to children with a health problem, special needs or over seven years of age. Special measures are taken on the basis of a reasoned decision of the Adoption Council (AC) with the relevant Regional Social Assistance Directorate (RSAD) where, within 6 months of entering the child in the register of children who may be adopted under the conditions of full adoption, the AC has not designated a suitable adoptive parent or none of the not less than three adoptive parents has submitted an application for adoption of the particular child, or if despite the efforts made it is not possible to identify a suitable adoptive parent. Information about the child's profile is sent by the RSAD to the SAA and is updated once a month between the 15th and the 20th day of each month. This information contains a profile of the child which includes: age, gender, special needs – information regarding the permanent disability and the possibility of social adaptation. The information also identifies the AC which took the decision on the implementation of special measures.

The CPDP expressed the following opinion on the issues raised:

1. The information in the draft profile of a child with a health problem, special needs or over seven years of age which is to be published on the SAA website in accordance with Article 21(1) of Ordinance No RD-07-7 of 5.10.2010 on the conditions and procedure for keeping and storing full adoption registers cannot lead to the identification of the respective child, therefore its publication in the proposed type and volume is not contrary to Regulation (EU) 2016/679.

2. The diagnoses of children with a health problem, special needs or over seven years of age contain 'health information' within the meaning of Article 27 et seq. of the Health Act and are subject to special regulation and protection. In this regard, from the point of view of proportionality, the information on the diagnosis of the child should not be published, but should be

provided as part of the additional information referred to in Article 22(2) of Ordinance No RD-07-7 of 5 October 2010.

3. The additional information referred to in Article 22(2) of Ordinance No RD-07-7 of 5.10.2010 allows direct or indirect identification of the child and when it is processed, including provided to potential adopters, both the special requirements of Article 22 of the Ordinance and the general rules of Regulation (EU) 2016/679 must be observed.

1.9.4. Opinion at the request of DSK Bank in connection with the implementation of voice biometry as an opportunity for customer identification. The letter sent details the desire of DSK Bank to introduce a Voice Biometrics Customer Identification System, which should be implemented in the Contact Centre for the purposes of identification when assistance needs to be provided to the Bank's clients with the products and services they use (the telephone call in combination with the voice recognition will be used), as well as when information is provided on the balance and movements on accounts (a combination of three customer identification methods – telephone, Voice biometrics and last four digits of an active bank card will be used).

The use of voice recognition as a system for identification of natural persons is not explicitly regulated in Bulgarian legislation. The method of identification proposed by the bank includes the use of a voice footprint which is a digital representation of the unique characteristics of the voice of a person and therefore is covered by the definition of 'biometric data' set out in Article 4(14) of Regulation (EU) 2016/679. As far as biometric data in this case is to be used by the PDC for the sole purpose of identifying an individual, they constitute a **special category of personal data** according to Article 9 of the General Data Protection Regulation and require enhanced protection of the rights and freedoms of the data subjects concerned.

In addition to the mandatory condition of obtaining consent, the PDC must give the Bank's client the right to opt for alternative identification methods that do not involve biometric data processing or an option to withdraw the consent at a later stage without any negative consequences for the client. Simultaneously, in view of the increased risk to data subjects, the PDC should pay particular attention to the mandatory requirements related to 'purpose limitation' and 'storage limitation'.

The CPDP's opinion is that the introduction of the described customer identification system is permissible subject to the express written consent of the Bank's clients after they have received detailed information regarding the purposes for which their personal data will be processed in the system introduced, the ways in which said data will be processed and the risks involved; and provided the clients are given the right to choose alternative methods of identification that do not

involve the processing of biometric data, respectively the possibility to refuse the service, without this causing any negative consequences for the natural persons – clients of the bank.

It is assumed that the controller DSK Bank must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data in accordance with Article 35 of Regulation (EU) 2016/679 arising out of the introduction of the Voice Biometrics Customer Identification System, as this is a new technology that, due to its nature, scope, context and purpose, can pose a high risk to the rights and freedoms of natural persons.

2. Participation in procedures for coordinating draft legislation relating to data protection issues

In 2018 representatives of the CPDP participated in different expert working groups regarding amendments to legislation. In addition, the CPDP received requests for coordination of drafts of statutory instruments, which the CPDP coordinates without comments or coordinates with remarks and comments which should be reflected in the relevant statutory instrument. A non-exhaustive list of draft instruments which were brought to the attention of the CPDP for coordination by competence is provided below:

1. Draft Ordinance to amend and supplement Ordinance No 4 of 2003 on the terms and procedure for entry into the register and requirements for the activities of currency exchange offices, Draft Ordinance to amend and supplement Ordinance No 7 of 2003 on the Terms and Procedure for issuance and withdrawal of authorisations to carry out activities as a food voucher operator and carrying out activities as an operator and providing reasons for such issuance and withdrawal.

2. Draft Concept paper for a centralised register of administrative criminal proceedings in electronic form.

3. Draft 2021 Census of the Population and Housing in the Republic of Bulgaria Act.

4. Draft Rules of Procedure (for the organisation) of the activity of the Joint Bulgaria – Baden-Württemberg Intergovernmental Commission.

3. Opinions regarding draft codes of conduct

Code of Conduct within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 is a voluntary instrument intended to contribute to the proper application of the Regulation and to help demonstrate compliance with statutory requirements in accordance with the principle of accountability, taking account of the specific

characteristics of the processing carried out in certain sectors or professions. Codes of conduct are drafted for a separate category of data controllers/processors, and in particular if they belong to the same sector or industry.

A Code of Conduct has added value only when it is tailored to a particular sector or industry, reflects its specific features and existing personal data processing practices such as the specific risks to data subjects' rights and freedoms and the appropriate technical and organisational measures for their mitigation. This logically means that the relevant sector, industry or category of data controllers/processors should have a sufficiently good level of self-organisation and effective mechanisms for internal coordination and control.

The initiative for developing a code of conduct should come from the respective sector or industry. When drawing up a code of conduct, or when amending or extending such a code, associations (associations, chambers) and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects (public consultation) where feasible, and have regard to submissions received and views expressed in response to such consultations.

Codes of conduct should be written in an accessible and understandable language and take into account national specificities and practices. Each code should comply with the provision of Article 40 of Regulation (EU) 2016/679 on data protection, which provides the legal framework for its content. The Code should specify the application of the requirements of the Regulation in the specific sector/industry. It is therefore inadmissible to use declaratory statements without such statements providing appropriate safeguards for the rights and freedoms of data subjects in the processing of their personal data and to copy texts of the Regulation.

The General Data Protection Regulation imposes on supervisory authorities the obligation to encourage entities to draw up codes of conduct so as to facilitate the effective application of the Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. It is the responsibility of the CPDP to give an opinion on whether a draft code or an amended or extended code of conduct complies with the Regulation and to approve this draft code or amended or extended code of conduct if it finds that said code of conduct provides appropriate safeguards. Approved codes of conduct that are not relevant to processing activities in several Member States are subject to registration and publication by the CPDP. At the same time, the CPDP has the power to accredit a body to monitor compliance with a code of conduct as well as the obligation to prepare and publish

the criteria for accreditation of bodies responsible for monitoring compliance with approved codes of conduct.

Regardless of the direct application of Regulation (EU) 2016/679, in July 2018 the CPDP adopted criteria and procedures for approving codes of conduct in order to facilitate the drafting of such codes of conduct. The adopted criteria and procedures aim at clarifying certain parameters of the Regulation in order to facilitate the uniform understanding and application of its requirements for the drafting of codes of conduct. In addition, a special section was created in the institution's website where information relating to codes of conduct is to be published and maintained. 'Criteria and Procedures for the Approval, Amending or Extending Codes of Conduct' and 'Guidance on the Drafting and Proposing Codes of Conduct in accordance with Article 40 of Regulation (EU) 2016/679' were published in this section in 2018. The criteria and procedures relating to the accreditation of bodies responsible for the monitoring of codes of conduct are subject to coordination with the EDPB, therefore they will be approved and published at a later stage.

The adopted 'Criteria and Procedures for the Approval, Amending or Extending Codes of Conduct' aim at facilitating the uniform understanding and application of the requirements for the drafting of codes of conduct set out in the Regulation. Codes of conduct are assessed in accordance with the requirements set out in Article 40 of Regulation (EU) 2016/679), as well as in accordance with the criteria adopted by the CPDP.

In 2018 the CPDP received 11 draft codes of conduct. The CPDP replied only with letters to the submitters of 5 draft codes of conduct without considering their merits because of their apparent non-compliance with the legal characteristics set out in Article 40(2) of Regulation (EU) 2016/679 and with the criteria and procedures issued by the CPDP. In connection with 5 draft codes of conduct, the CPDP delivered opinions stating the reasons for its refusal to approve the proposed code of conduct. At the end of the reporting period, a procedure for drafting an opinion was under way with respect to one draft code of conduct with a view to submitting it to a CPDP meeting to rule on the compliance or non-compliance with the requirements of Regulation (EU) 2016/679.

As a result of the experience gained during the assessment process, a number of principal shortcomings of and omissions in proposed draft codes of conduct were found. Some of them are as follows:

1. Insufficient evidence of the representative power of the submitter of the code with respect to the data processors/controllers in the sector/industry.

2. Lack of evidence of consultations with relevant stakeholders, including data subjects where feasible.

3. Copying texts of the Regulation and using declarative statements without specifying their application in the particular sector/industry and without said statements providing appropriate safeguards for the rights and freedoms of data subjects in the processing of their personal data.

4. Bodies responsible for monitoring the code are given functions relating to the implementation of the code.

5. Need to refine terminology in accordance with the Regulation.

6. Lack of information on whether processing activities are relevant to several Member States.

VII. PREPARATION FOR THE IMPLEMENTATION OF THE NEW EU LEGAL FRAMEWORK IN THE FIELD OF PERSONAL DATA PROTECTION: GENERAL DATA PROTECTION REGULATION AND DATA PROTECTION DIRECTIVE

1. Amendments and Supplements to the Personal Data Protection Act

In June 2016, an organisation was created in the CPDP for the preparation of the national-level activities required for the implementation of the new European legal framework in the field of personal data protection. The formulation of amendments to the PDP Act in order to ensure the implementation of Regulation (EU) 2016/679 and transpose Directive (EU) 2016/680 on the processing of personal data in police and criminal justice activities was an important element of this preparation. The draft Act to amend and supplement the PDP Act prepared at the end of 2017 by the CPDP in cooperation with the MoI was submitted to the Ministry of Interior to take action in accordance with its competence for initiating the proposed legislative amendments.

Although the Regulation has, as a rule, direct effect and does not need to be transposed into national law, Regulation (EU) 2016/679 also has certain elements of a directive. The draft law, in so far as it introduces measures for the implementation of the Regulation, lays down both the issues in which the Regulation has left the Member States the freedom to decide whether and to what extent to regulate a particular matter and the issues which require legislative measures at national level to be explicitly introduced.

In terms of structure, the draft Act:

- repeals a number of texts of the current PPD Act which are now explicitly regulated in the General Data Protection Regulation and the related rules are directly applicable (principles, individuals' rights, data controllers' obligations, transfers of personal data to third countries);
- amends and updates rules in line with the philosophy and spirit of the General Data Protection Regulation (tasks and powers of the CPDP in its capacity as a supervisory authority, exercise of rights of data subjects, remedies);
- formulates new texts the need for which arises out of Regulation (EU) 2016/679 (striking a balance between the protection of personal data and the freedom of expression and information, processing of personal identification numbers, processing of personal data in the context of employment, processing for archiving purposes in the public interest, scientific, historical research or statistical purposes, protection of professional secrecy);

- proposes provisions that transpose the provisions of Directive (EU) 2016/680 into national legislation (Chapter 8 of the draft Act).

The draft Act to amend and supplement the PDP Act was coordinated informally with the European Commission and the Commission's comments and remarks were reflected in the final version. In addition, the draft submitted to the National Assembly reflects the remarks and comments received in the course of the public consultation held between 30 April and 30 May 2018 with two stakeholder groups:

1. with the ministers and other state bodies whose activity is affected by the draft legal amendments and supplements (coordination of the draft law in accordance with the procedure laid down in Article 32 of the Rules of Procedure of the Council of Ministers and Its Administration);

2. with citizens and legal entities (public consultation on the grounds of Article 26 of the Statutory Instruments Act).

As a result of these consultations, the following general considerations were taken into account in the final draft of the Act:

- the minimum amounts of administrative fines and penalties were removed;
- the protection of professional secrecy was regulated and situations in which the exercise of the investigative powers of the CPDP might lead to the disclosure or breach of such secrecy, as well as of sources of journalistic information, were prohibited;
- the processing of the PIN as the sole identifier for the provision of public services electronically by remote access was prohibited;
- derogations from the rights of data subjects and the obligations of the data controllers were introduced where Regulation (EU) 2016/679 so permits (e.g. for the purposes of national security, defence and public order and security; for the investigation of criminal offences or the execution of criminal penalties; for other important objectives of general public interest, in particular an important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security; for the protection of judicial independence and judicial proceedings; for the protection of the data subject or the rights and freedoms of others; for the enforcement of civil law claims);
- the hypotheses of processing personal data for the purposes of archiving in the public interest, scientific and historical research, statistical purposes, journalistic purposes, humanitarian purposes and disaster situations were legally regulated.

The team of lawyers at the CPDP performed a huge amount of work during the preparation of the amendments and supplements to the PDP Act. In the course of the public consultation, the final document with the remarks and proposals of citizens, organisations and institutions and respectively the CPDP's comments on them had a volume of 400 pages. All opinions on the draft Act were thoroughly analysed and discussed.

The updated draft Act to amend and supplement the PDP Act was approved by decision No 503 of the Council of Ministers of 18 July 2018 and was tabled in the National Assembly on the same date. After the draft Act was adopted at first reading by the National Assembly, a working group was set up under the lead committee – the Committee on Internal Security and Public Order. The working group comprises a number of stakeholders who, together with representatives of the CPDP, the MoI and the Parliament, commented on the directions of the proposed legislative amendments in order to refine the final wording of the provisions in the Act and to find consensus on its texts. The draft Act to amend and supplement the PDP Act is expected to be adopted at second reading by the National Assembly at the beginning of 2019.

2. Publication and Dissemination by the CPDP of Practical Guidelines Relating to the General Regulation

In order to support the practical implementation of the General Data Protection Regulation, the CPDP published on its website a document containing ten practical steps for the implementation of the GDPR. The document has purely informational purposes, is not binding and does not pretend to be exhaustive. Its purpose is to synthesise in a comprehensible language the steps that each PDC needs to take in order to bring its data processing activities in line with the requirements of the new legal framework in this area. In addition to providing access to the information brochure through its website, during the reporting period the Commission has distributed more than 14 000 paper flyers that contain practical advice and guidance on the implementation of the General Data Protection Regulation.

3. Conducting a National Information and Awareness Campaign Relating to the New Legal Framework

The General Data Protection Regulation changes the way in which data controllers and processors across the European Union, as well as all organisations that process personal data of European citizens work. It introduces stricter rules for the processing of personal data and further develops the rights of citizens. The new rules affect seriously different types of controllers.

The direct application of the General Data Protection Regulation starts on 25 May 2018 and data controllers and processors need to take concrete action in order to avoid significant penalties for possible violations. As a national data protection supervisor, the CPDP has a responsibility imposed by the General Data Protection Regulation to explain to society in an accessible way the fundamental aspects of the EU personal data reform and the new legal framework created by the Regulation. At the same time, as a supervisory authority the CPDP seeks to promote public awareness and understanding of the risks, rules, safeguards and rights associated with the processing of personal data in all spheres of public life by various controllers.

At the beginning of the reporting period the CPDP initiated a large-scale information and awareness campaign. Between February and May 2018, the CPDP organised an awareness campaign in five regional cities – Plovdiv, Veliko Tarnovo, Varna, Burgas and Stara Zagora in order to respond to the public interest in awareness events involving immediate contact (meetings, seminars, conferences, etc.). The events aimed at achieving broad public awareness on all issues related to EU personal data reform and the new legal framework. They were targeted at the general public, PDCs from all spheres of public life and the economy and all stakeholders. The objective of the CPDP was to present the main points in the new legal framework and the practical steps that the PDCs need to take in order to implement in their activity the newly adopted standards for protection and processing of personal data.

At the end of January, in the News section of its website, the CPDP announced the timetable for the events in the first four cities as well as the organisation created for preliminary registration for the events. For the purpose of the awareness campaign, a special sub-section 'Information Campaign' was created in the 'Messages' section of the CPDP's website, where the regional events with the participation of representatives of the CPDP and the organisation for participation in said events were published.

Due to the large number of persons wishing to register, a cap on the presence of a certain number of representatives from each PDC was introduced. Local authorities played a key role in organising regional events. They provided logistical organisation and event support and gave information to regional media. The events announced were met with great interest because of the possibility for citizens and controllers to ask directly specific questions about the implementation of the new requirements.

Due to the increased interest of PDCs in the updated legal framework for personal data protection, in May 2018 the CPDP decided to expand its information and awareness campaign. The objective was to provide further clarifications on the philosophy of the General Data Protection Regulation, its basic concepts, the new responsibilities of data controllers, the rights of data

subjects, the functions of data protection officers and the requirements they need to satisfy, and to respond of questions that were raised during the initial stage of the CPDP's awareness campaign. Because of its limited human and financial resources, the Commission focused its efforts in the awareness campaign on the sectoral representative organisations of PDCs in order to achieve a multiplier effect.

During the reporting period, more than 60 individual events with more than 6 000 participants from both the public and the private sector, the academia and the non-governmental sector were organised in the two stages of the information and awareness campaign.

4. Notifications from Data Controllers and Processors that Have Designated a DPO Received in the CPDP

After the initial date of application of the General Data Protection Regulation, the controllers and the processors are required to designate a data protection officer in any case where:

– the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

– the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

– the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10 of the General Data Protection Regulation.

In cases other than those specified above (where the designation of a DPO is mandatory), the controller or processor may designate a data protection officer at their own discretion.

The controller or the processor must publish the contact details of the data protection officer and communicate them to the CPDP. A total of 3 222 data controllers and processors notified the CPDP of the designation of DPOs during the reporting period.

VIII. PARTICIPATION OF THE CPDP IN THE EU COORDINATION AND COOPERATION MECHANISMS

1. Participation in the meetings of the European Data Protection Board and the expert subgroups under it

The European Data Protection Board (EDPB) is a new body of the EU established with Regulation (EU) 2016/679 and operating as of 25 May 2018. It is responsible for the uniform application of the Regulation in all EU Member States. It consist of the heads of all data protection supervisory authorities of the EU Member States and of the European Data Protection Supervisor or their respective representatives. The European Commission participates in the Board's meetings without voting rights. The EDPB is the successor of the Working party referred to in Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (repealed when Regulation (EU) 2016/679 became applicable).

The first meeting of the EDPB was held on 25 May 2018. **The Chairperson of the Bulgarian data protection supervisor Mr Ventsislav Karadjov was elected unanimously as its deputy chair.** Mr Karadjov's election is a recognition at European level of the active involvement of the CPDP in the development of the new European legal framework on personal data protection and in the preparation for its implementation.

The reporting period was extremely intense with regard to all supranational forms of cooperation in the personal data protection sector. In connection with the start of the functioning of the EDPB and all issues that the General Data Protection Regulation leaves to the Member States to decide alone or through co-operation, the expert subgroups of the Article 29 Working Party and the EDPB, respectively, completed a considerable amount of work throughout 2018.

Among the busiest subgroups in which representatives of the CPDP were involved was the Technology Subgroup. In 2018 the subgroup continued the intensive preparation of draft guidelines for certification and accreditation in accordance with Articles 42 and 43 of the General Data Protection Regulation. Following a lot of discussion during the year, a compromise text of the Certification Guidelines was prepared and at the end of the reporting period was in the public consultation phase. The work on the two documents and their annexes will continue in 2019.

The experts in the Technology subgroup also worked intensively on the preparation of Video Surveillance Guidelines. Given the different regulation of this sector in individual countries, the discussions will continue in 2019.

At the end of the reporting period, the preparatory (organisational) stage was completed and the actual work on the development of Guidelines on privacy by design and default started. Work

on these guidelines and the future work on Biochain technology guidelines will be carried out during the next reporting period.

In 2018, 28 lists of the types of processing operations were discussed for which data protection impact assessment is required pursuant to Article 35(4) of the General Data Protection Regulation. The subgroup assessed all criteria proposed, developed and implemented a uniform approach to analysis and evaluation and presented these at EDPV meetings for approval. The work of the subgroup was adopted unanimously by the Heads of National Supervisory Authorities at the EDPB meeting.

The ongoing disclosure of notifications of personal data breaches received from national supervisors continued and in the coming reporting periods this information will serve to carry out an in-depth analysis and propose concrete measures to be taken at national level and in cooperation among the data protection authorities of the EU Member States.

During the reporting period the subgroup also started work on the development of guidelines to regulate the processing of **personal data in the field of electronically connected vehicles and artificial intelligence.**

Active discussions took place in 2018 with the participation of representatives of the CPDP in the 'International Transfers' (ITS) and 'Borders, Travel and Law Enforcement' (BTLE) expert subgroups as well.

2. Exchange of Information via the Internal Market Information System

The Internal Market Information System (IMI) is a secure multilingual environment for online exchange of information.

It is designed to facilitate the exchange of information between public administrations within the EEA and the European institutions and bodies that take part in the practical implementation of EU legislation. Information and documents on cases that are of a cross-border nature, i.e. in which citizens in several EU Member States may be affected, are published in it.

In terms of personal data protection, the movement of documents and information in IMI is carried out on the basis of the General Data Protection Regulation and the rules of the EDPB.

As at 31 December 2018 the register of cases maintained in the IMI contained 255 cases of cross-border cooperation, including:

– 176 cases initiated as a result of complaints received;

– 79 other cases such as investigations and initiatives of a national supervisor, legal obligation, media reports, etc.

As a result of the cases mentioned above, actions were started in connection with:

– 397 procedures related to mutual assistance. These procedures could lead in the future to cooperation based on the one-stop-shop mechanism;

– 43 procedures based on the one-stop-shop mechanism (Article 60), in connection with which for 2 a final decision has been prepared, for 20 a draft decisions is in place, one draft decision has been redrafted and for 20 informal consultations have been held;

– 25 requests to treat cases as national (local) in accordance with Article 56 (2);

– consistency procedures: 30 under Article 64, of which 29 (lists of processing activities that require an impact assessment) have been completed by adopting final opinions.

In addition, 574 procedures were initiated to identify the lead data protection authority and the data protection authorities concerned (300 ongoing, 274 closed).

The CPDP published in the system information regarding 1 case under Article 56 requesting that another supervisor be designated as the lead supervisor on the specific alert based on the location of the PDC (outside Bulgaria). The CPDP joined another case as a concerned supervisor given the fact that the data controller contacted citizens of several EU Member States (including Bulgarian citizens).

Via the cooperation mechanism, the CPDP received through IMI requests for information from the Hungarian Data Protection Authority (5 requests) and the Swedish Authority (1 request). The main areas in which information was requested were notifications of personal data breaches by data controllers, the appointment of the DPOs, the use of CCTV and the designation of joint controllers.

The CPDP drew up and coordinated the list of personal data processing operations that will require an impact assessment outside the situations already mentioned in Article 35(3) of Regulation (EU) 2016/679.

IX. INTERNATIONAL ACTIVITY

1. Participation of the CPDP in the activities of the Bulgarian presidency of the Council of the EU during the first half of 2018

Between January and June 2018, the Republic of Bulgaria had the rotating presidency of the Council of the European Union for the first time. The Bulgarian presidency was part of a trio together with Estonia and Austria.

During the reporting period, the CPDP was actively involved in the implementation of the priorities and objectives of the Presidency and was fully committed to their implementation in the area of personal data protection.

This section of the annual report on the activities of the CPDP provides summary information about the concrete results achieved by the CPDP within the framework of the Bulgarian Presidency of the Council of the EU.

Preliminary preparation and internal organisation in the CPDP

The CPDP was involved in the general process of preparation and specialised training of the state administration for the fulfilment of the tasks arising from the Bulgarian Presidency. A team was formed at the CPDP, comprising the Chairperson and one member of the CPDP (Mrs Mariya Mateva), eight representatives of the administration, as well as an external expert. Due to the nature of the commitments and the fact that the Presidency coincided with the final stage of the preparation for the implementation of the General Data Protection Regulation, only part of the team was directly involved in the Brussels activities while the rest assisted the work from Sofia.

It is important to note that, unlike the ministries and other autonomous agencies, the CPDP does not have a representative in the Permanent Representation of the Republic of Bulgaria to the EU in Brussels (PP–Brussels). This further complicated the practical participation in the sessions of the working bodies of the Council in Brussels and the communication with the institutions and other EU Member States.

Specific commitments of the CPDP in relation to the activities of the DAPIX Working Party

During the Bulgarian Presidency, the CPDP took over the management and organisation of the activities of the Working Party on Information Exchange and Data Protection (DAPIX), 'Data Protection' format (E.23). In addition, CPDP representatives supported and participated in the discussions in the Working Party on Cooperation in Criminal Matters (COPEN), in particular on

the proposal for a Eurojust Regulation, and in the Permanent Representatives Committee (COREPER-2).

In connection with the above, the Chairperson of the CPDP was nominated as a chair of DAPIX, and Mrs Mariya Mateva was nominated as a deputy chair of DAPIX. In addition, Mrs Mateva was appointed Deputy Chair of the Working Party's specialised format on Traffic Data Storage.

Between January and June 2018, the CPDP team organised 8 (eight) regular meetings of DAPIX in Brussels and one informal meeting in Sofia and participated in one meeting of COREPER and two meetings of COPEN. The three political trialogues with the European Parliament and the Commission, the three technical trialogues with the Council's Legal Services, the EP and the European Commission, as well as the preparatory interinstitutional meeting at the level of rapporteurs were equally important and complex to prepare. In addition, the chairperson and the lead expert carried out a series of informal working meetings in Brussels with all relevant EU institutions and bodies as well as with the delegations of virtually all 27 other Member States.

In view of the great dynamics of the negotiation process on the open files in the field of personal data protection and the above-mentioned fact that the CPDP has no representative in the PP–Brussels, all regular meetings of DAPIX were held in a Friends of Presidency format, i.e. with English as a working language and without interpretation.

Examined Dossiers and Results Achieved

Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions (modernised Regulation No 45/2001)

The proposal for a regulation updates and modernises the provisions of the currently effective Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data in order to bring them in line with the new EU legal framework in the field of personal data protection adopted in April 2016.

The Bulgarian Presidency took the dossier from the Estonian Presidency completely blocked politically due to the opposing views of the Council and the EP on the scope of the new regulation in the field of Justice and Home Affairs and, in particular, its application to the operational personal data. There were other open controversial issues, such as the possibility of limiting certain rights of data subjects by internal instruments of EU institutions and bodies, the procedure for the selection of the European Data Protection Supervisor, etc. Nevertheless, the CPDP team began to work from the very first days of the Presidency to find a workable and sustainable compromise solution that

guarantees a high level of protection of data subjects' rights and at the same time does not jeopardise the effectiveness of the work of EU's law enforcement agencies (Europol, Eurojust, the European Public Prosecutor's Office and Frontex).

Despite the initially strong opposition from most delegations, including Germany, France, the UK, etc., the CPDP's negotiating team managed to change the positions of all the participants in the legislative process, including of the 28 Member States in the Council, the political groups in the EP and the European Commission, and on 23 May 2018 they **unanimously supported** the final compromise on the regulation proposed and negotiated by the Bulgarian Presidency. The key elements of the compromise were as follows:

– the modernised Regulation 45/2001 includes a separate chapter with common rules on the protection of data subjects' rights in the processing of operational personal data by Union agencies in the field of justice and home affairs. At the same time, the legal acts whereby the agencies in question are established can provide for special rules that deviate from the general rules where this is necessary and justified (*lex specialis derogat legi generali*);

– the provisions of the new chapter on operational personal data are identical or as close as possible to the rules laid down in Directive 2016/680 (the Police Directive). This ensures harmonization of the rules applicable to national law enforcement agencies and EU agencies;

– the provisions regarding operational personal data will be implemented immediately for Eurojust and Frontex, and for Europol and the European Public Prosecutor's Office – after 4 years and following a preliminary analysis to be carried out by the Commission.

Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust)

Regardless of the fact that the proposal for a Eurojust Regulation was considered in another working group by a team of the Ministry of Justice, the EP bound it to finding a solution to the issue of operational personal data (the so-called legislative package). For this reason, the successful conclusion by the CPDP of the negotiations on the modernised Regulation 45/2001 became the most important factor for reaching an agreement on the draft Eurojust Regulation on 19 June 2018.

Modernisation of Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

The negotiations for the modernisation of Council of Europe Convention No 108 started in 2012. During the Bulgarian Presidency, the dossier became a priority political issue in the field of personal data protection, as the document is the only international legal instrument in this area. The

modernisation of the Convention in fact encourages and promotes globally the introduction of the high EU standards for the protection of privacy and personal data.

Despite the serious political and diplomatic obstacles, at the last possible moment the EC managed to reach a compromise on the disputed texts with the Russian Federation and thus paved the way for the signing of the Protocol amending Convention No 108.

The final open issue on the dossier, to which the CPDP team had to find an urgent solution, was the clauses concerning the entry into force. The Council of Europe's legal committee proposed that the amendment should enter into force through classical ratification by all parties, while the EU, through the EC, insisted on a more ambitious and quick approach. The EU Member States were initially divided and supported three different options. Nevertheless, the Bulgarian Presidency managed to negotiate a **unified position of all Member States** on a compromise proposal for the entry into force of the Amending Protocol, which allowed the modernised Convention No 108 to be approved and adopted by the Committee of Ministers of the Council of Europe on 18 May 2018.

Other topics

During the Presidency, the CPDP team also organised discussions in DAPIX on other topical issues in the field of personal data protection, including ICANN, personal data protection clauses in EU trade agreements, the Japan Adequacy Decision and others.

2. Preparation for and Holding of the 40th International Conference in 2018

Following more than a year of preparatory work, between 22 and 26 October 2018 the CPDP organised the most important international annual forum in the field of personal data protection together with the European Data Protection Supervisor (EDPS) – the International Conference of Data Protection and Privacy Commissioners (ICDPPC). The conference has been held since 1979 and is the largest and most significant annual event for exchange of experience, good practice and analysis of trends in the personal data protection sector, bringing together 121 accredited organisations worldwide. The hosting of the conference is entrusted to countries with proven experience and capacity in the area of personal data protection and respecting human rights and freedoms.

The conference includes a closed session for accredited members and observers and an open session and additional events for all registered participants – a wide audience from the privacy and data protection community, industry, civil society, academia, government bodies and non-governmental organisations.

The jubilee edition of the conference in 2018 was special for a number of reasons. Sofia was the first capital on the Balkan Peninsula, and the Republic of Bulgaria was only the second country after Poland from Central and Eastern Europe to host the forum for almost 40 years. For the first time in the history of the conference, the seminar programme was held simultaneously in two different locations – in Sofia and Brussels, and was organised jointly by a national supervisory authority and a European institution.

In mid-2017, the joint nomination for the 40th edition of the conference was officially announced. 2018 provided the opportunity for the CPDP and the EDPS to highlight the leading role of the European Union in shaping policies and instruments for personal data protection and access to information worldwide.

The 40th International Conference contributed to the development of the discussion on the ethical dimensions of personal data processing in the digital age and was conducted under the title 'Debating Ethics: Dignity and Respect in Data Driven Life'. The conference outlined how the digital age changes society, how it influences the values and everyday life of people, how dignity and respect can be maintained in a technology-oriented world of digitised societies and economies.

A representative of the CPDP participated actively in the closed session held on 22 and 23 October in Brussels and attended by 350 representatives of accredited members and observers. Issues related to the management of the forum and its future, recommendations and scenarios for its further development and relevance were discussed. The working parties reported on the work done and their plans for the future.

Declarations and resolutions of the 40th conference were presented, discussed and voted. A presentation was made on the next 41st conference to be held in 2019 in Tirana, Albania. The possible hosts the 42nd edition of the conference, which will take place in 2020, were explored. It was officially announced that the 42nd conference will be held in Mexico. The closed session discussed issues relating to the implementation of the General Data Protection Regulation, ethics and data protection in artificial intelligence systems.

The programme in Sofia was targeted at businesses, the non-governmental sector and academic circles. The event in Sofia was officially opened with a welcome address by the CPDP Chairperson Mr Ventsislav Karadjov and by Mr Rossen Jelyazkov, Minister for Transport, Information Technology and Communications. The six plenary debates as well as the accompanying events were intended for over 200 registered participants. Moderators, lecturers and participants in discussions included representatives of Bulgarian, European and international institutions and organisations — the Council of Europe, the European Commission, Europol, the European Data Protection Supervisor, the State e-Government Agency, the Communications

Regulation Commission, the Ministry of Interior and others. Representatives of the supervisory authorities of Spain, the Russian Federation and Japan, as well as of the International Association of Privacy Professionals (IAPP) were present. The Bulgarian NGOs were represented by the Access to Information Programme, the Law and Internet Foundation and the LIBRe Foundation. The presence of representatives of the business community was especially pronounced. Attendants included Nymity, OneTrust, Amatas, AT&T, EY, Inveo Srl, Cisco, Sophia Lab, Telelink, Software Group, Sensika Technologies, Euroins Insurance Group, SAS, CENTION profesioal IT security, Vilivosoft and I&S Vassilev, Vivacom, European Investment Bank, Municipal Bank, UnitedLex Corporation/Marshall Dennig and others.

The topics of the plenary discussions that formed part of the conference programme in Sofia were as follows:

- 'Privacy and Human Dignity: Universal Values in a World without Borders', which presented the modernised Convention No 108 as the new global framework for data security and data protection, as well as the European Commission's decision on the adequate level of protection provided by Japan. Participants were particularly interested in the positions expressed by the representatives of Japan, Russia, the European Commission and others.
- 'Balancing Between Public Interest and Data Subjects' Rights' brought together the views of supranational organisations, private businesses, academia and the non-governmental sector.
- 'Smart Solutions for Data Security and Accountability' enabled participants to learn about up-to-date solutions to ensure compliance with the General Data Protection Regulation.
- 'Digital Ethics in the Age of Global Communications and Virtual Reality' – consecutive presentations presented solutions on both sides of the Atlantic.
- 'Privacy Protection in the Financial Sector: Fintech Innovations and Traditional Banking' ended with the announcement of a large-scale innovative initiative called Regtech Sandbox, which is due to be implemented next year. It should be noted that such an idea in the field of privacy and personal data has not yet been implemented in Europe.
- 'Cyber Security Insurance – Building upon GDPR Compliance' presented the possibilities of using insurance products in the field of cybersecurity as well as the difficulties in formulating such products.
- 'Outsourcing Data – Global Data Transfer and Cloud Services' – trends and threats in the implementation of global business initiatives were considered.

The topics of individual events in Sofia were as follows:

- 'Canaries in a coal mine? Data Protection Officers in the data mine!' presented by the data protection officer of Europol and his team.

– ‘Drones: Ethics of a PlayStation Mentality’ presented by LIBRe Foundation and United Drone Community.

– ‘The First Five Months of the GDPR’ presented from the point of view of international private sector organisations and of a national supervisory authority.

– ‘GDPR – Questions and Answers’ (regarding the national implementation of the General Data Protection Regulation) presented by the host data protection supervisor, a state institution and a non-governmental organisation.

– ‘EU-funded projects as a partnership and data protection instrument’ presented by the Bulgarian national supervisory authority.

Within the framework of the Sofia programme, the participants had the opportunity to visit and get acquainted with the activities of the Laboratory of Artificial Intelligence and CAD Systems and the Cyber Security Laboratory on the territory of Sofia Tech Park.

Discussions from Brussels could be viewed from Sofia through an all-day videoconferencing between the two venues of the event. All participants, regardless of their location, had the opportunity to participate fully in the discussions through the Mobile Application of the Conference. In this way, the participants from Sofia followed open sessions in Brussels with a central topic ethics in the digital world. During the two seminar days, the participants heard many welcome addresses and video addresses: from Giovanni Buttarelli (European Data Protection Supervisor), Mariya Gabriel (Digital Economy and Society Commissioner); Věra Jourová (Justice, Consumers and Gender Equality Commissioner); Guido Raimondi (European Court of Human Rights President, video interview), Isabelle Falque-Pierrotin (Chair of the ICDPPC Executive Committee and President of the French supervisor). Video feeds were sent by the CEOs of the two of the world’s largest technology companies, Google and Facebook – Sundar Pichai and Mark Zuckerberk.

Participants in Sofia had the opportunity to follow the speech of Tim Cook, CEO of Apple Inc, in which he declared his support for the imposition of comprehensive privacy legislation for protecting personal data on the Internet, similar to regulation in the European Union, and said that the time has come for the rest of the world to follow the example of the EU in creating a clear framework for the protection of consumers’ personal data. Within 5 sessions, an interactive, multidisciplinary and comprehensive debate took place and reflected the digital revolution, its impact on society and how digital ethics could help maintain dignity and respect in technology-driven life.

In the first session, ‘Beyond Compliance: Why Digital Ethics?’, the strategic importance of defining global digital ethics was presented. An overview was made of how digital technology has

brought society to where it is now, what are the biggest technological trends over the next 20 years are, how they will change our lives, and insights into where we can get were provided. The second session, 'Right versus wrong', was devoted entirely to ethics – what is ethics, what is its place in the internet environment, how ethics interact with law, how it is implemented in life sciences, what role it plays in solving social and political dilemmas. Discussions revolved around the questions about the role of ethics in human society, how it has evolved over time, who defines the ethical standards and whom they serve, where personal freedom, dignity and mutual respect in different cultures originate. The subject of ethics was expanded in regards to the notions of human dignity, economic interests, work relations, scientific progress, healthcare as well as the interaction between humans and machines. The third session, 'The Digital Dividend', was devoted to the benefits that digitisation has brought to people and society. The interaction between technology, on the one hand, and the values and rights of people and society, on the other, was presented.

A special focus was placed on children and the most vulnerable groups. Data-driven technologies were discussed: who benefits from them and who does not, whether technology really serves people. Answers to some of the most pressing questions were sought: how digital technology is changing the way we behave and interact; does digital technology strengthen or weaken civic freedom and harmony; how do notions of harmony, morality and trust combine with big data and artificial intelligence.

In the 'Creative Café' interactive session held in Brussels on 25 October, representatives of regulators, academia, civil society and the private sector discussed the topic 'How to move towards Digital Ethics'. The participants in the fourth session, 'Towards a Digital Ethics', discussed what does 'data protection beyond compliance' mean, who is entitled to speak about it and take action; what should be the role of data protection authorities, and what intended and unintended consequences could digital ethics frameworks have. The role of independent data protection authorities in the management of digital ethics was discussed.

The final, fifth session, 'Move Slower and Fix Things', brought the themes together and drew conclusions on what needs to be done. Reflections on digital life and the role and limits of regulatory intervention were presented. The 40th International Conference of Data Protection and Privacy Commissioners was closed on 25 October 2018 with a closing address from the heads of the host institutions – Ventsislav Karadjov and Giovanni Buttarelli. The manner in which the conference was organised and held proved that with the help of modern technologies professionals in the field of personal data protection can be more united in their efforts than ever before.

3. Participation in Schengen monitoring and evaluation coordination groups

In 2018 the participation of the CPDP in the work of the specially established joint supervisory bodies and coordination groups for supervision of the large-scale information systems of the EU continued. These collective bodies are managed by the EDPS and comprise representatives of the national data protection authorities of the EU Member States: the Europol Cooperation Committee, the Customs Joint Supervisory Authority, the supervisory coordination groups of the Schengen Information System (SIS II), the Visa Information System (VIS), EURODAC, the Customs Information System (CIS) and the Internal Market Information System.

In 2018 the CPDP continued to provide assistance within its competence to the full accession of Bulgaria to the Schengen area.

The practice of participation of CPDP representatives in Schengen evaluations in the field of personal data protection in other Member States continued. During the reporting period the Member State evaluated was Estonia.

4. Participation in international data protection forums

At the beginning of 2018 Pristina in the Republic of Kosovo hosted a one-day regional Cyber Security and Privacy Conference under the slogan 'General Data Protection and Incident Response'. Representatives of Kosovo, the Czech Republic, Macedonia, Albania and Bulgaria (the CPDP) attended.

On 8 and 9 October 2018 the Chairperson of the CPDP took part in the international forum on technologies that guarantee the right to privacy held in London, United Kingdom.

An International Conference on Personal Data Protection was held in Moscow on 7 and 8 November 2018. The event was organised at the highest level by the Federal Service for Supervision of Communications, Information Technology and Mass Media of the Russian Federation. Representatives of the supervisory authorities of the Republic of Bulgaria, Italy, Hungary, Azerbaijan, Bosnia and Herzegovina, the Republic of Serbia, the People's Republic of China, Jordan, the Republic of South Africa, Morocco and others participated in the forum. The representative of the Bulgarian supervisory authority Prof. Veselin Tselkov (Member of the CPDP) made a presentation on 'Methodology for assessing conformity with the requirements of the General Regulation'.

During the reporting period a CPDP member participated in the European Conference of Data Protection Authorities. The conference has made a significant contribution to the development of the fundamental right to personal data protection not only in Europe but also globally. It is a forum for discussing issues of common interest, exchanging knowledge, experiences and ideas for

interaction and elaborating unified methods of action for data protection authorities. In 2018, the event was entitled ‘A New Framework for Cooperation’. In the context of the new European data protection rules, a natural and expected topic of the discussions was related to the practical implications for national legislators, data protection authorities and controllers. Lectures were presented on ‘The role of guidelines, recommendations and codes of good practice to promoting a coherent application of the General Data Protection Regulation’, ‘The ‘one-stop-shop’ mechanism according to Chapter VII of the General Data Protection Regulation – advantages and possible obstacles’, ‘Interaction between European Union Legislation and National Procedures’.

One of the panels of the Conference was dedicated to the interaction and supervision to be carried out by data protection authorities with regard to the processing of personal data by national security authorities. Given the paramount importance of national security in today’s precarious world where challenges and threats endangering the security of European citizens constantly occur, data protection authorities discussed their crucial importance with regard to protection measures, challenges and opportunities for protection of privacy.

X. SUPPORTING THE ACHIEVEMENT OF THE CPDP OBJECTIVES THROUGH THE IMPLEMENTATION OF NATIONALLY AND INTERNATIONALLY FUNDED PROJECTS: GENERAL INFORMATION REGARDING PROJECTS AND PARTNER CONSORTIA

At the end of 2015 a project proposal by the CPDP under the Erasmus+ Programme entitled 'Innovative Postgraduate Programme: Meeting Market Needs and Introducing New Models' was approved. The project was developed and submitted in partnership with the data protection authorities of Poland and Macedonia and the universities of Lodz, Poland, and Ohrid, Republic of Macedonia. The total budget of the project is BGN 329 840.95 (EUR 168 645). The lead partner in the project consortium is the University for Information Science and Technology 'St. Paul the Apostle' in Ohrid.

The objective of the project proposal is to overcome the lack of specialists and experts in the field of e-government and digital business through multidisciplinary actions aimed at modernising higher education curricula. The project aims at creating an innovative postgraduate programme that is accessible at supranational level through an online learning platform. The project includes development, appraisal and implementation of the curriculum at the universities from the project consortium, as well as activities related to ensuring sustainability of results, such as training of staff to work with the platform and raising public awareness.

During the reporting year, the detailed curricula of the subjects included in the overall curriculum were completed, two international coordination meetings of the project teams from the partner organisations were held in May and August 2018, short-term training for trainers for their employees was held and 2 events for the dissemination of the results took place on the territory of Bulgaria in July and August 2018. It is important to note that the first event promoted the project among representatives of the academic institutions in Bulgaria and the second one – among students and employees.

The project was successfully completed at the end of August 2018.

At the beginning of 2017, in cooperation with the personal data protection authorities of Italy, Spain, Poland and Croatia, a project proposal with the subject 'T4DATA: Training Data Protection Authorities and Data Protection Officers' was submitted under the Rights, Equality and Citizenship Programme of the European Union. The lead partner of the project consortium is the Italian foundation Lelio e Lisli Basso – Onlus. The total budget of the project is BGN 1 101 339.71 (EUR 563 106.05). The project proposal was approved and proposed for financing in the middle of 2017.

The project objective is to provide support for training provided by data protection supervisors to current and future data protection officers in public authorities. The training is related to the practical implementation and interpretation of the General Data Protection Regulation. The project brings together a wealth of expertise from 5 EU Member States. The project will support data protection authorities in the interpretation and implementation of Regulation (EU) 2016/679 as regards the reporting requirements applicable to public authorities and institutions as well as in cases of mandatory designation of data protection officers.

A number of activities were prepared and implemented under the project in 2018. The first working version of the Manual for Organising and Conducting Training Events for Data Protection Officers in the Public Sector was prepared and presented. Representatives of the CPDP participated in two international project coordination meetings in April and October 2018. Experts from the CPDP administration participated in the two training for trainers events envisaged under the project in June and October 2018. Future project activities include the organising of a series of pilot electronic training events for data protection officers.

At the end of March 2017 the CPDP submitted a project proposal under the Erasmus+ Programme. The proposal was approved and proposed for financing. The grant contract was signed in September 2017. The project subject is: 'e-OpenSpace – European innovative open platform for electronic exchange of information and sustainable provision of education for adults in the field of personal data protection and privacy'. It brings together the efforts of the data protection authorities of Poland and Croatia, the Jagiellonian University and the Sofia University, and the Italian NGO GVMAS. The total budget of the project is BGN 357 719.35 (EUR 182 899). The coordinator of the project efforts and lead partner is CPDP.

The e-OpenSpace project was developed to provide an effective solution for strategic supranational cooperation to ensure the security and free movement of personal data in the EU. It aims to provide a single cloud space for national data protection authorities to carry out their tasks in the field of training in line with the new legal framework.

The main goal of the project is to promote informal digital training and awareness in the field of privacy and personal data protection. The project partners will look for flexible learning pathways to integrate practical and theoretical knowledge in order to provide skills in the field of data protection and promote a common approach and synergy between EU Member States in conducting training and awareness raising initiatives. The main practical means to achieve this goal will be to develop a web-based solution in order to provide a collaborative environment and open, innovative and inclusive informal digital learning.

During the reporting period, the second international project meeting took place and the implementation of the following intellectual products started: 'Guidelines for the electronic implementation of non-formal digital training in the field of personal data protection', 'The Common Curriculum', 'Open educational resources for informal digital data protection training', and the development of e-OpenSpace – the single pilot platform for implementation of the training events developed and for coordination and cooperation between the participating national data protection authorities was launched.

Plans for 2019 include the completion of intellectual products under the project, the holding of the last two international partner meetings, short training for trainers for the employees of the project partners, as well as the implementation of events for the dissemination of results on the territory of the EU Member States where project activities are being implemented.

The duration of project activities is two years, by the end of August 2019.

At the end of 2017, in partnership with the Union of Lawyers in Bulgaria and 'Apis Europe', the CPDP started preparing a project proposal funded under the call for proposals 'Ensure the highest level of protection of privacy and personal data' under the EU Rights, Equality and Citizenship Programme. At the beginning of 2018, the CPDP as a lead partner and applicant organisation submitted a project proposal that brought together the efforts of Bulgarian and Italian partners. In addition to the partners above, partners include EY – Bulgaria, the Italian Data Protection Authority, the Roma Tre University and the European Women Lawyers Association – Bulgaria Branch.

The project proposal aims at providing small and medium-sized enterprises (SMEs) with practical tools for achieving compliance with the General Data Protection Regulation. Following the implementation of the project activities, SMEs will have integrated digital solutions for access to a valuable database containing the practice of both national supervisors and courts at national and European level, accessible via a mobile application and a self-learning algorithm. The administrative procedures relating to signing the financial assistance contract were completed at the beginning of December 2018 and this made it possible to start the actual implementation of the project as early as the end of 2018.

The total budget of the project is BGN 1 089 961.92 (EUR 557 288.68) and the project implementation is envisaged to be completed at the end of November 2020.

Initiatives to be part of project consortia as well as the implementation of already approved projects are a continuation of the CPDP's prevention policy by providing PDCs with useful practical tools and models to enhance the level of protection in data processing.

XI. THE COMMISSION FOR PERSONAL DATA PROTECTION IN THE CAPACITY OF DATA SECURITY SUPERVISOR UNDER THE ELECTRONIC COMMUNICATIONS ACT

1. Statistics and analysis of requests for access to traffic data

The CPDP is a supervisor under the EC Act with regard to the retaining of and access to traffic data. In pursuance of Article 261a(5) of the EC Act, by 31 May every year the CPDP submits to the National Assembly and the European Commission summarised statistics regarding the cases of provision of traffic data to competent authorities for the purposes of national security and for preventing, detecting and investigating serious crimes. The statistics is prepared based on the data regarding the previous year provided by undertakings that provide public electronic communication networks and/or services regarding:

− cases where data have been provided to competent authorities;

− the time elapsed from the initial date of storage until the date on which the competent authorities requested the transmission of data;

− the cases where the request for data could not be responded to.

Based on the information submitted in 2018 by 93 undertakings providing public electronic communication services, the following statistics can be summarised:

− The total number of requests for access to traffic data was 65 420, which is comparable to that in the previous year.

− The cases where data were provided to competent authorities in accordance with Article 250b(1) and Article 250c(4) totalled 65 073, or the trend of such cases exceeding 99% of all requests remained unchanged.

− The time elapsed from the initial date of storage until the date on which the competent authorities requested the transmission of data was mainly up to 3 (three) months – in 63 % of the cases (Figure 14).

− The cases where the request for provision of traffic data could not be responded to were 347 which was considerably lower compared to all previous years.

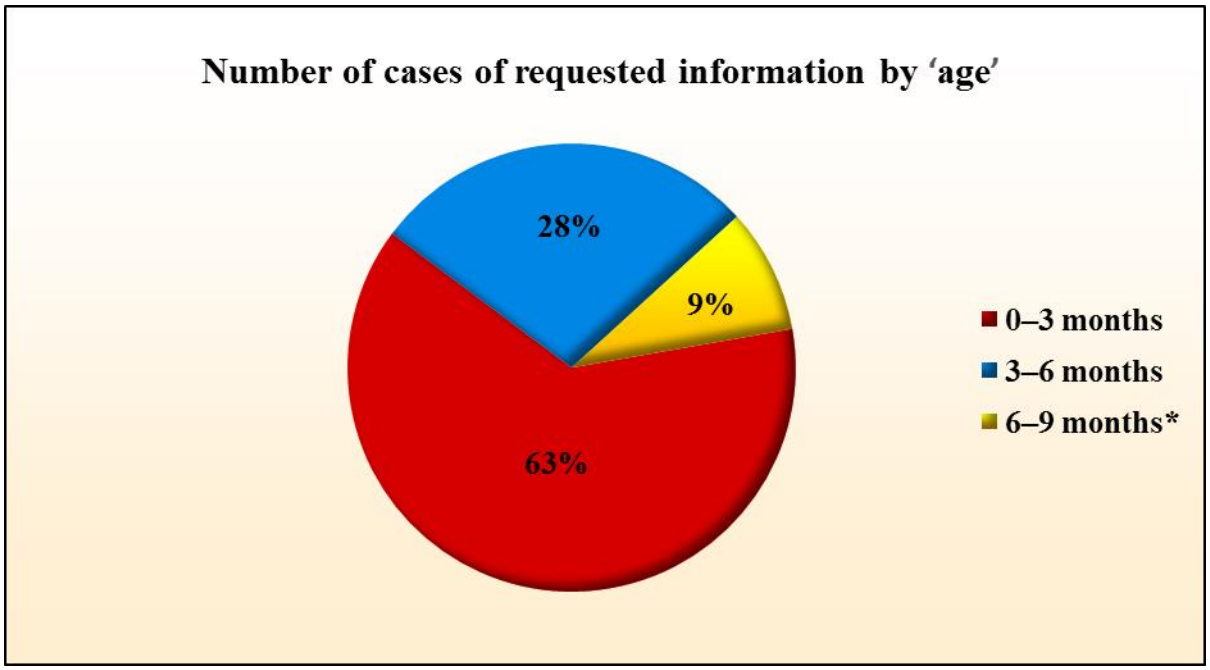

Figure 14

2. Statistics of received protocols regarding destroyed traffic data

In pursuance of its responsibilities according to Article 251g(1) of the EC Act, for the purpose of exercising effective ongoing and ex-post control the CPDP maintains a register of the protocols received from undertakings regarding destroyed data.

Statistics regarding the protocols received during the reporting year is presented in Figure 15.

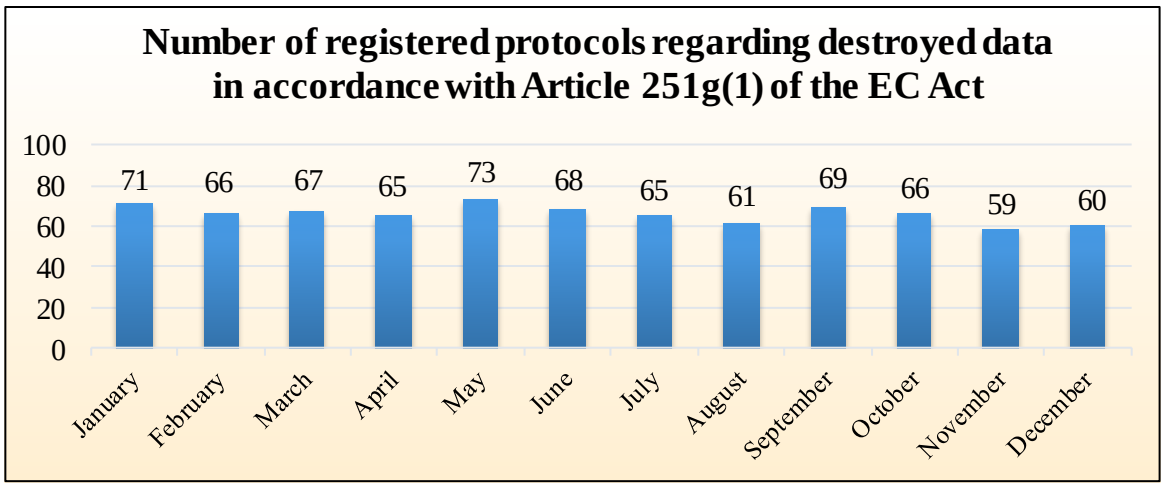

Figure 15

The number of undertakings that fulfil their obligation to provide monthly protocols regarding destroyed data in accordance with Article 251g(1) of the EC Act was 66 a month on the average during the reporting year.

XII. INSTITUTIONAL COLLABORATION. PARTNERSHIP WITH MEDIA REPRESENTATIVES AND INFORMATION AND EDUCATIONAL ACTIVITY

1. Cooperation with government bodies and non-governmental organisations

In connection with the power of the CPDP to issue compulsory instructions to undertakings that provide public electronic communication networks and/or services in accordance with Article 261a(3)(2) of the EC Act, during the reporting period, a series of meetings with representatives of the Parliamentary Committee for Control of the Security Services, the Application and Use of the Special Intelligence Means and the Data Access under the Electronic Communications Act (the **SRS-NS Committee**) as well and with undertakings that provide electronic communications services were held. The purpose of the meetings was to streamline the accountability activities of companies as well as the control exercised by the two committees in accordance with their responsibilities and competences based on the experience gained.

As a result of these meetings, with a decision dated 4 July 2018 the CPDP updated the compulsory instructions issued in accordance with Article 261a(3)(2) of the EC Act to the undertakings that provide public electronic communication networks and/or services.

In relation to its obligations under the EC Act, the CPDP also maintains regular communication and interaction with the Communications Regulation Commission (CRC).

Immediately after 25 May 2018, after high level meetings between the CPDP and the Ministry of Education and Science, a cooperation agreement was signed on the protection of personal data in the field of education and science. The cooperation and activities under the agreement will continue during the next reporting period.

At the invitation of a number of public authorities, in 2018 the CPDP held numerous individual meetings, training and awareness events on the new European legal framework in the field of data protection. As part of bilateral cooperation, the supervisory authority also provided PDCs with individualised views on the General Data Protection Regulation.

2. Media policy and coverage of events relating to CPDP activities

In pursuit of its public awareness policy and driven by its belief in ongoing civic engagement on personal data protection issues, in 2018 the CPDP continued to initiate meetings, seek partnerships and conduct different principal initiatives with the participation of the business, trade unions and government institutions, as well as to build on the information and education campaign envisaged in the plan for 2017 through open and adequate communication with the mass media in Bulgaria. All this was done by respecting the legitimate interests of stakeholders and seeking pragmatic solutions that benefit citizens and businesses.

On 29 January 2018 the CPDP commemorated the **European Day of Personal Data Protection – 28 January** for the 12th consecutive time. This day is called 'European' because the idea of celebrating it was initiated by the Council of Europe. Currently 28 January is celebrated in many countries not only in Europe but throughout the world.

The main objective of celebrating the European Day of Personal Data Protection is to raise awareness and promote initiatives and good practices aimed at understanding the risks, rules, safeguards and rights associated with the processing and protection of personal data. An environment that fosters dialogue among all stakeholders is created, observance of privacy rules is promoted and the development of technological tools that give people control over their personal data is encouraged. The celebrating of this day on an international scale creates opportunities for cooperation between data protection authorities, governments, industry, academic circles, non-governmental organisations.

The CPDP is a government institution with a mission aligned with citizens and their rights. For this reason, the focus in 2018 continued to be on the dialogues with citizens and PDCs. Traditionally, an **Open Day** was organised, when the officials in the administrative departments accept anyone wishing to get familiar with their work and receive up-to-date information on specific issues of their interest. At the same time, an **open reception** for citizens and personal data controllers was opened in the meeting room of the CPDP.

Every year on that day the CPDP submits its **Annual Activity Report for the previous year** to the National Assembly. Due attention in the 2017 report was paid to activities relating to international cooperation and the implementation of the information and awareness campaign relating to the most important elements of the new European legal framework in the field of personal data protection.

On the occasion of the Day of Personal Data Protection, Mr Ventsislav Karadjov, Chairperson of the CPDP, awarded for the second consecutive year the **Prize for Journalism**. The Commission awarded a diploma and a plaque to the bTV News reporter Gabriela Naplatanova for **the largest journalistic contribution in 2017** in promoting citizens' rights to privacy and protection of personal data. The institution expressed gratitude to the reporter and the entire team of bTV Media Group for the active, objective and well-intentioned coverage of topics of public importance related to the activities of the CPDP.

The 'Annual Prize for Journalism' announced on 28 January 2016 is given for publications, broadcasts and actions of public importance of a journalist that regularly reported on the institution's activities in the past calendar year. The prize is awarded for active and well-intentioned coverage, either on own initiative of the reporter or at the invitation of the CPDP, of events that

present the activity of the Commission, while adhering to the Code of Ethics in the Bulgarian media. The public interest and civic engagement, the rapid and accurate journalistic response on topical issues in the field of personal data protection, the coverage of events and initiatives at national and supranational level are evaluated. Journalistic materials must be impartial and fair and contain objective criticism. It is of particular importance that they originate from a reliable source and that the public doesn't doubt them, as well as that they are presented in an accessible and comprehensible language. The prize is awarded for professional journalism which creates and publishes information materials and journalistic investigations in the print media, the electronic media and the new-generation media and considers a variety of aspects in the field of personal data protection.

The largest event in Bulgaria on the occasion of the entry into force of the General Data Protection Regulation, **the 'GDPR Sofia' Conference**, took place on 29 January 2018. The interest in it was very high. The forum was organised by the Digital National Coalition with the assistance of the Ministry for the Bulgarian Presidency of the Council of the EU and the CPDP. The conference was opened by Ms Mariya Gabriel (Digital Economy and Society Commissioner), Ms Lilyana Pavlova (Minister for the Bulgarian Presidency), Mr Ventsislav Karadjov (Chairperson of the CPDP) and Ms Gergana Passy (Chair of the Digital National Coalition). More than 300 participants from across the country, including experts from the European Commission, rapporteurs from the European Parliament and representatives of some of the largest business companies, took part in the event.

A **number of workshops** were held during the year with some of the largest PDCs that process data of millions of citizens. On 2 March 2018 the CPDP Chairperson and experts from the Commission had a meeting with representatives of the three electricity distribution companies in Bulgaria – CEZ Bulgaria, EVN Bulgaria and Energo-Pro Bulgaria. On 29 March 2018 CPDP representatives took part in a discussion of the implementation of the General Data Protection Regulation in the in the tourism industry, held at the annual conference of the industry. Many other similar meetings were organised with increasing intensity: with the National Association of Secretaries of Municipalities in Bulgaria, with judges from the Supreme Administrative Court and the Sofia City Administrative Court, with the Bulgarian Chamber of Commerce, the Bulgarian Union for Customs and Foreign Trade Services, the Bulgarian Chamber of Commerce and Industry, the State Commission on Information Security, the Industrial Capital Association, the Bulgarian Medical Association, the Bulgarian Dental Association, the New Bulgarian University, different community centres, insurance companies and others.

In 2018, the CPDP continued its initiative for publicity and dissemination of up-to-date information on the protection of personal data and the privacy of citizens through the **mass media**. Maintaining sustainable and beneficial relations with media representatives from all over the country lead to more than 150 interviews and materials/broadcasts with the participation of the Chairperson, members and experts of the CPDP. The desire for transparency, open dialogue with the Bulgarian society and reaching out to a wide audience was realised thanks to the support and the personalised contact created between the mass media and the CPDP. Informing the public and easier access to valuable and practical information was accomplished through numerous publications in the print media of 'Trud' newspaper, '24 Hours' newspaper, 'Monitor' newspaper, 'Capital' newspaper, 'Banker' newspaper, 'Chernomorski far – Burgas' newspaper, 'Business Club' magazine and others. The electronic media of BNT, BNT2, bTV, Nova TV, BgOnAir, TV+, Bloomberg TV Bulgaria, as well as the Bulgarian National Radio (Sofia, Horizon and Hristo Botev Programmes), the BNR in Vidin, Kardzhali, Burgas, Shumen, Varna, Blagoevgrad; the students' radio Reaction, Darik Radio and other continue to reflect regularly the CPDP's point of view and to transmit interviews on topical issues related to personal data. Answers to various questions asked by media and the public can be read daily on the websites of new-generation media Novini.bg, Economy.bg, Technews.bg, Manager.bg, Lex.bg, Debati.bg, Clinica.bg, etc.

The **topics** that attracted the largest public interest during the reporting period were the issues related to the implementation of the General Data Protection Regulation. As a consequence, another current topic during the reporting period were the expected amendments and supplements to the Personal Data Protection Act. In this connection, the Chairperson and the members of the CPDP continued to give their competent opinions through all mass media and as lecturers in business conferences of national and international importance.

The CPDP provides promptly information to journalists on their written or oral request. This resulted in the publication of a many information materials and journalistic investigations concerning various aspects of the protection of personal data. Throughout its many years of work, the CPDP is constantly striving to ensure maximum awareness of its day-to-day activities and long-term projects.

3. Other informational and educational tools

The institutional website of the CPDP is the most essential and fundamental tool for the implementation of the Commission's information activities. Maintaining up-to-date information on the site is an established and proven tool for providing information and clarifications both on the

activities of the CPDP and on the processes and innovations in the field of data protection on national, European and global scale.

As far as the information and awareness activities are concerned, it should be noted that the information activities of the CPDP are of a permanent nature and the Commission's purpose is to reach the widest possible range of stakeholders – citizens and PDCs.

In 2018, the CPDP had the responsibility, as a data protection supervisor, to explain to society in an accessible way the fundamental aspects of the EU personal data reform and the new legal framework created by the **General Data Protection Regulation** (Regulation 2016/679). **Preparing for the practical application of the new standards in the field of personal data protection was one of the main objectives and a priority task for 2018.** The past year was characterised by a particular intensity of activities and events in the world of personal data protection arising out of the implementation of Regulation (EU) 2016/679 and the body that monitors compliance with the rules is the CPDP. In this connection, explanatory materials and recommendations on the implementation of the Regulation were published on the institution's website: guidelines of the CPDP, of the European Commission, of the Working Party under Article 29 of Directive 95/46 (whose successor is the European Data Protection Board established by said Regulation). All available informational materials – brochures, instructions, guidelines – are regularly published on the website. The following materials were published in the website in 2018 in connection with Regulation (EU) 2016/679:

1. New EU Legal Framework in the Field of Personal Data Protection:

- General Data Protection Regulation — Regulation (EU) 2016/679;
- Directive on personal data protection in police and criminal matters

2. Information and clarification materials with regard to the General Data Protection Regulation:

- European Commission Guidance on upcoming new data protection rules across the EU;
- Guidelines of the Article 29 Working Party on the application of the General Data Protection Regulation;
- Data Protection Impact Assessment (EIA) Guidelines and determining whether there is a likelihood of processing operations resulting in 'high risk' for the purposes of Regulation (EU) 2016/679;
- Guidelines of the right to data portability;
- Guidelines for personal data protection officers (DPOs);
- Guidelines for identifying a controller or processor's lead supervisory authority;

- Guidelines on the application and determination of administrative penalties 'fine' or 'financial penalty' for the purposes of Regulation (EU) 2016/679;
- Guidelines on Personal data breach notification under Regulation (EU) 2016/679;
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation (EU) 2016/679;
- Guidelines on consent under Regulation 2016/679;
- Guidelines on Transparency under Regulation 2016/679;
- Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) of the General Data Protection Regulation;
- Ten practical steps for implementing the General Data Protection Regulation – content of a brochure printed for dissemination with the help of public authorities and industry organisations;
- Practical issues relating to personal data protection after 25 May 2018 – content of a brochure printed for dissemination with the help of public authorities and industry organisations;
- Clarification on the practical application of the General Data Protection Regulation by local authorities (municipalities);
- Obligations of data controllers;
- Data protection officer;
- Rights of individuals;
- Consent according to the General Data Protection Regulation.

In 2018, a section on codes of conduct under Regulation (EU) 2016/679 was created on the institutional site with the aim of publishing and maintaining information related to the codes. At the end of 2018, the following were published:

- Guidance on Drafting and Proposing Codes of Conduct in accordance with Article 40 of Regulation (EU) 2016/679;
- Criteria and Procedures for the Approval, Amending or Extending Codes of Conduct.

In connection with the information and awareness campaign conducted in 2018 in different district towns, the CPDP published information on upcoming events on its website in a timely manner.

One of the priority tasks in 2018 was to prepare and host the jubilee 40th International Conference of Data Protection and Privacy Commissioners. In this connection, the site provided information about the conference, the programme of events in Sofia and Brussels, the registration for participation (for which a special pop-up window was developed).

In accordance with the requirements of Regulation (EU) 2016/679, in 2018 the CPDP published on its website its **Policy for Transparency in the Processing of Personal Data** in the overall work of the institution as a data controller.

Over the past year, activity continued in relation to maintaining information on the website (regular publishing of news), as well as to maintaining the main information sections: 'Legislation', 'Practice', 'Information', 'International Cooperation', 'Schengen Area', 'Personal Data Controllers', 'The Institution', 'Administrative Service', 'Media'.

In the 'Legal Framework' section the main international and Bulgarian statutory instruments in the area of human rights and protection or privacy are published – laws, regulations, directives, rules.

In line with the strategic objective of improving the openness and transparency process, the 'Practice' section reflects the CPDP practice by focusing on the publication of opinions of public interest as well as of anonymised decisions on complaints that ensure transparency regarding the CPDP's practice in its decision-making on different cases.

The 'International Cooperation' section provides information about the activities of supervisors and groups and the work of European and global forums and initiatives. In 2018, a sub-section on the European Data Protection Board established by Regulation (EU) 2016/679 was established. It contains information regarding the Board and a link to its official website.

The work of the CPDP in relation to achieving full accession of Bulgaria to the Schengen area was another priority task in 2018. In this context, extremely detailed and up-to-date information on the Schengen area is provided: legal framework, a guide on the exercise of the right of access to the Schengen information system, catalogues of good practices. The right of individuals in the field of personal data protection in the Schengen area are described in detail.

The 'Personal Data Controllers' section changed substantially in 2018 because PDCs are no longer required to register with the CPDP and the CPDP is no longer required to keep the related registers. At present, instructions on the notification of the CPDP of the designation of DPOs by data controllers and the relevant standard form are published in this section.

'The Institution' section contains up-to-date information about the institution, financial information and information about CPDP's project activities. In terms of providing information about the institution to the public, the maintaining and publication of two registers and one list in accordance with the CCFIAA Act on the CPDP's website began in 2018:

- Register of the declarations submitted by the employees of the CPDP administration in accordance with Article 35 of the CCFIAA Act;

- Register of declarations of incompatibility and declarations to change circumstances declared in the declarations of incompatibility of the persons referred to in Article 35(1) (senior public officials) before the appointing authority in accordance with the CCFIAA Act;
- List of the persons who failed to submit within the deadline declarations in accordance with Article 35 of the CCFIAA Act.

The 'Administrative Service' section provides information relating to the provision of administrative services and the access to public information.

The 'Media' section, which is extremely useful for all stakeholders, publishes articles and interviews with the Chairperson and members of the CPDP and provides first-hand information about all current and topical issues in the field of personal data protection.

In 2018, the 'Archive' section was considerably expanded, and part of the information that became obsolete after 25 May 2018 was moved there:

- Ordinance No 1 of 30 January 2013, which was repealed as of 25 May 2018;
- Lists relating to the registration of PDCs – archive as at 24 May 2018;
- Questions regarding the implementation of the PDP Act – archive as at 24 May 2018;
- Questions regarding the holding of elections – archive as at 24 May 2018;

In 2018 the website continued to be part of the means to engage in active dialogue with citizens and PDCs through the forms for submitting complaints and the forms for asking questions. Access to standardised forms of communication and interaction with the institution was provided, clear guidelines were developed for individuals on how they can exercise their rights in a complaint procedure should they believe that PDCs have failed to fulfil their obligations. In 2018, 1 522 inquiries that used these forms were received on a wide range of issues and 324 complaints and alerts were filed.

Another means to achieve public awareness is the CPDP's **Information Bulletin**. Six bulletins were issued in 2018. The bulletin is issued bi-monthly in electronic form and is published in the website of the institution, and can thus be accessed by every visitor of the website. At the same time, there is an option to subscribe, as a result of which subscribers receive a notification that the next issue of the bulletin is already published. In 2018, 420 new subscribers subscribed, and the number of subscribers reached 1 010. The bulletin has its own ISSN 2367-7759.

The bulletin reflects both national and European and worldwide events and initiatives in the field of protection of personal data. In line with the priority set for 2018 to prepare for the practical application of the new rules in the field of personal data protection, the central theme of all bulletin issues in the past year was the General Data Protection Regulation. Guidance and information and

clarification materials of the CPDP, the Working Party referred to in Article 29 of Directive 46/95 (whose successor is the EDPB) and the European Commission were published. After 25 May 2018, the CPDP started publishing regular information on the activities of the European Data Protection Board established by Regulation (EU) 2016/679. The bulletin provides coverage of international events and forums with the participation of representatives of the CPDP. The main event in 2018 was the 40th International Conference of Data Protection and Privacy Commissioners organised jointly by the CPDP and the European Data Protection Supervisor. A report on the results achieved in the field of data protection during the Bulgarian Presidency of the Council of the EU was also published in the bulletin.

Decisions and opinions of the CPDP and general statistics on control activity are published on a regular basis in the bulletin. Three articles of CPDP members: 'General Data Protection Regulation – New Challenges' and 'Practical Guide to IT Security in the Processing of Personal Data' by Prof. Veselin Tselkov and 'Personal Data Protection as a Right of the Person and the Citizen and History of Its Affirmation in Europe and Bulgaria' by Tsanko Tsolov, were published in 2018.

The CPDP is a public sector organisation and, as a result, it is obliged pursuant to the Access to Public Information Act to publish the public information it collects, creates and maintains in an open machine-readable format allowing re-use. The publishing in the Open data portal of public information of public interest collected, created and maintained by CPDP, the re-use of which has high added value (lists, excerpts from registers relating to the registration of PDCs), which started in 2016, continued until 25 May 2018. After 25 May 2018 this information is no longer published because the statutory obligation to maintain such registers is no longer in force. At the moment the Open Data Portal contains a link to the 'Archive' section of the CPDP website, which provides final information with archival value on the registration of PDCs which is not subject to further maintenance and updating.

The CPDP received a prize from Citizens Against Bureaucracy Foundation for its overall policy of comprehensive and open provision of information about both the activities of the Commission and the processes and innovations in the field of personal data protection. For year 2018, the CPDP received an award in the 'Transparency in Management' category. When handing the diploma, the Foundation's manager Stefan Hristov pointed out that an effective tool used by the CPDP to achieve public awareness is the regular publication of an electronic Information Bulletin which reflects the decisions and opinions of the Commission. This is the third acknowledgement of the CPDP in a row. In 2017 the Commission received the Foundation's award for 'State Institution of the Year' and in 2016 – for 'Best Citizen Service'.

XIII. ADMINISTRATIVE CAPACITY AND FINANCIAL RESOURCES

1. Administrative Capacity

The ability of the CPDP as an administrative structure to fulfil its statutory tasks and respond to the public expectations is inextricably linked to the professionalism and motivation of its employees. Providing administrative capacity for the CPDP to adequately fulfil its functions as a supervisor and to achieve its mission is a permanent and purposeful process.

At the end of the reporting period the CPDP employed 51 members of staff under civil service relationships and 18 under employment relationships (including the Chairperson and the members of the CPDP).

During the period January–December 2018, 12 members of staff were promoted in rank and 5 members of staff were promoted in position.

Experts are found and recruited in accordance with the requirements of the Civil Servants Act.

- Competitions: 7 competitive procedures for filling vacancies in the CPDP administration were held, 5 of them were completed with appointments and another 2 were terminated because there were no applicants satisfying the conditions for appointment.
- Mobility – transferring to civil service from another administration with a tripartite agreement: 7 procedures were announced, in 2 of which no documents were submitted.

For the CPDP, staff training is an important element of the human resources management function. During the reporting period, the employees increased their professional qualification by participating in 108 courses for 44 training events conducted mainly by the Institute for Public Administration and the Diplomatic Institute under the Ministry of Foreign Affairs. Four newly appointed civil servants and 2 people appointed in a senior position for a first time underwent mandatory training.

The high staff turnover over the past two years needs to be pointed out. The entry into force of the General Data Protection Regulation and the obligation for a large number of PDCs to designate DPOs triggered increased demand (in all spheres) for experts with high professional knowledge in personal data protection processes. This resulted on leading experts leaving the CPDP attracted by better pay in the private sector. Between 24 May 2016 (the entry into force of the Regulation) and the end of 2018, 29 employees left the CPDP and only 18 officials were appointed during this period. Twelve members of staff, of which 10 under civil service

relationships and 2 under employment relationships, were appointed during the reporting period. The employment relationships with 13 members of staff were terminated.

At present, the CPDP does not have the financial resources required to retain its experts by raising their remuneration. This puts at risk not only the normal administrative processes but also the overall application of the legislation in the field of personal data protection. This outflow of staff mainly from the specialised administration also leads to a sharp escalation of the workload of the remaining employees. The tasks have increased at least 5-6 times, while the number of experts decreased and new functions and tasks stemming from the General Protection Regulation of the data need to be performed.

Although there is no formal practice in the CPDP to conduct interviews with the employees when they leave in order to clarify the reasons for seeking another job, it can be assumed that the main reasons for this are the opportunity for new employment with better financial parameters and a more convenient location. The staff turnover is particularly high in one of the directorates of the specialised administration, the Legal Proceedings and Supervision Directorate. Taking into account the fact that the work in this administrative unit is busy, specific and highly qualified, the main relevant reasons for turnover are the following:

– the disproportionately lower remuneration in the public sector than in the private sector for legal and IT specialists, which are essential in the directorate;

– the sustained rapid increase in workload accompanied by almost unchanging number of staff. In particular, it should be pointed out that one of the administrative units in this directorate, the Legal Proceedings and Procedural Representation Department, was established at a time when the workload was up to 100 complaints per year. In recent years the volume of complaints has grown at least 5-6 times. This volume reflects both on the number of court cases and on the services provided to of individuals.

2. Administrative services

2.1. General information

In compliance with the requirements of the Ordinance on Administrative Services, the users of the administrative services make contact with the CPDP through the Administrative Service Unit (ASU). The administrative service activity is carried out in full compliance with the Internal Rules on Administrative Services and the Customer Charter which aim at enhancing the quality of the administrative services and encouraging the participation of citizens and employees in discussing the services, the manner of their provision, the quality required and the standards for execution. The

activity of the ASU is performed by four employees in an uninterrupted working process within the working day. In the course of fulfilling their duties, all employees of the administration carry a distinguishing sign with a photograph and information about their names, position, administration and unit to which they belong.

During the reporting period, the employees of the Administrative Service Unit processed a total of 17 470 documents – letters, requests, applications, complaints, internal documents, etc. from and to citizens and institutions. The document flow system processes all documents entered into the Administrative Service Unit. The established rules for scanning incoming and outgoing documents guarantee the transparency in the work of the administration.

During the reporting period (1 January 2018 – 31 December 2018), no complaints and reports related to the administrative service performed by the administration were received.

Since May 2018, the CPDP has the access to registers of the public administration in the environment for exchange between registers RegiX, which it needs in order to perform its administrative activities. This, in turn, facilitates and makes easier the provision of administrative services to citizens.

2.2. Report on the requests for access to public information and requests for re-use of information received at the CPDP in 2018

In accordance with the requirements of the API Act, a section 'Get Informed' was included in the CPDP website. It includes:

- procedure for consideration of requests for access to public information and provision of information for re-use;
- description of the unit that accepts requests for access to information and information for re-use;
- standard costs for requests for providing access to public information and information for re-use by the public sector;
- procedure for access to the public registers of the CPDP;
- description of the information arrays and resources used by the CPDP administration;
- list of issued instruments and texts of the issued statutory and general administrative instruments;
- list of the categories of information subject to publishing on the Internet and the formats in which it is accessible;

- annual report on the received requests for access to public information and re-use of information from the public sector, including information regarding denied access and the reasons for denial.

Total number of received requests for access to information:	**16**
- from citizens of the Republic of Bulgaria;	**14**
- from foreign citizens;	0
- from media;	1
- from NGOs;	1
- from private individuals.	0
Total number of decisions granting access to public information:	**4**
- full access to public information granted;	4
- partial access to public information granted;	0
- access granted in the cases of overriding public interest;	0
- refusal of access to public information:	0
Notification of the absence of the requested public information	0
Referrals of request where the CPDP does not have the requested information but knows where it is located	**4**
Information provided under the procedure for providing administrative services or in accordance with the procedure of the APC	**2**
Requests which do not comply with Article 25(1) of the API Act in conjunction with Article 2(1)	**6**
Total number of received requests for provision of information for re-use	**0**

3. State of play of the implemented information and communication systems in the CPDP in 2018

During the reporting period, the System for management of documents and workflows in the CPDP and for control of decisions was brought in line with the Electronic Document Circulation System and with the single technical protocol approved by the Chairperson of the State e-Government Agency for the exchange of documents in the public administration. From 1 November 2018, the CPDP exchanges documents with the other administrations included in the system for electronic exchange of documents. With the introduction of the Electronic Document

Circulation System, fast and secure document circulation with all the departments of the public administration was ensured.

The possibility of faster and more efficient handling of incoming mail, the significant reduction of paper documents and the acceleration of information flows can be highlighted as results.

The contracts for maintenance of the information systems critical to the activities and processes of the CPDP were renewed in a timely manner. Server and personal certificates are delivered and installed on a regular basis in line with the deadlines for renewal.

Inspections and repairs of technical equipment are carried out within the shortest time possible in accordance with the established procedures.

During the reporting period, the CPDP continued its cooperation with Executive Agency 'Electronic Communication Networks and Information Systems' which is responsible for GovCERT Bulgaria (National response centre for information security incidents).

The CPDP continued its participation in Working Group 'Digital Bulgaria 2020' under the Ministry of Transport, Information Technology and Communications.

Commission representatives participated in the Council for Network and Information Security of the Information Systems of the Administrative Authorities under the State e-Government Agency.

4. Public Procurement

In order to provide resources for the activities of the CPDP in 2018, public procurement procedures were awarded as follows:

Through open procedures:

– 'Delivery of hardware for the needs of the Commission for Personal Data Protection';

Through public tendering:

– 'Provision of air tickets for the carriage of passengers and baggage for the business trips abroad of CPDP officials, as well as provision of additional travel-related services';

Through collecting offers with a notice:

– 'Development and implementation of a specialised automated information system for maintaining the registers in the CPDP';

– '24-hour physical security of the building in which the administrations of the Commission for Personal Data Protection, Institute of Defence "Prof. Tsvetan Lazarov" are located and of the parking lot in front of it';

– ‘Delivery of fuel and accessories for vehicles owned by the Commission for Personal Data Protection through charge cards for cashless payment’.

5. Financial resources – general information on budget spending of the CPDP for 2018

The operating budget of the CPDP in the amount of **BGN 2 530 000** was approved with the 2018 State Budget of the Republic of Bulgaria Act. During the year, in pursuance of Council of Ministers Decree No 15 of 1 February 2018 approving additional expenses/transfers in 2018 for securing the Bulgarian Presidency of the Council of the European Union in 2018, and on the basis of the actual costs of organising and holding meetings of DAPIX in Brussels and organising the event in Sofia, the CPDP’s budget was changed and was increased by BGN 67 428. The total budget of the CPDP approved for 2018 amounted to **BGN 2 597 428.**

The operational expenditure of the Commission for Personal Data Protection and its administration and the expenditure on organising events as part of the Bulgarian Presidency of the Council of the European Union amounted to **BGN 2 568 947,** or **98.9 %** of the approved estimates for the year. The expenditure types by headings of the Unified Budget Classification (UBC) are presented in the following table:

Heading	Description of the expenditure	Amount (BGN)
01-00	Salaries and wages for staff employed under employment and civil service contracts	1 260 638
02-00	Other remunerations and staff payments	82 188
05-00	Mandatory social insurance contributions paid by employers	322 410
10-00	Running costs	660 128
19-00	Taxes, fees and administrative sanctions paid	15 329
46-00	Expenditure on membership fees and participation in non-commercial organisations and activities	250
52-00	Acquisition of long-term tangible assets	132 090
53-00	Acquisition of long-term intangible assets	95 914
	Total budget expenditure	**2 568 947**

XIV. CPDP GOALS AND PRIORITIES IN 2019

Given the need to finalise the national data protection legal framework in order to ensure the implementation of the General Data Protection Regulation and of Directive (EU) 2016/680 after its transposition into the PDP Act, the CPDP sets the following objectives and priorities for the next reporting period:

1. To provide the human and technical resources in the field of personal data protection required for the CPDP activities.

One of the priority activities of the CPDP during the next reporting period is related to providing the institution with an administrative capacity that is adequate to its new tasks and powers. Despite the objective factors that lead to an increased outflow of highly qualified staff of the CPDP, the supervisor will continue to invest its efforts in recruiting experts with legal and IT background in order to secure its main activities. This priority remains particularly relevant in the light of the enhanced new powers of the CPDP and the increased expectations of the public for enhanced protection of individuals with regard to the processing of their personal data. In addition, in pursuance of its commitments to participate in the work of the EDPB, in 2019 the CPDP will develop and equip a complex videoconferencing system. The obligation to provide such equipment arises not only for the CPDP but also for data protection supervisors of all Member States due to the fact that the EDPB is a permanent body whose decisions are legally binding and which will hold remote sessions via videoconferencing in order to ensure adequate and urgent deliberation on issues within its competence.

2. To adopt the instruments of secondary legislation in the field of personal data protection.

After the AASPDP Act is finally adopted and enters into force, the CPDP will focus its efforts on developing rules for the implementation of the statutory obligations of data controllers and processors arising out of the Act. The first instrument of secondary legislation which the CPDP is expected to adopt is the Rules of its activity and the activity of its administration. In addition to regulating the structural changes in the institution's administrative organisation resulting from the General Data Protection Regulation, the Rules will regulate the conditions and procedure in accordance with which procedures in the CPDP proceed in all new areas of activity. Within 6 months of the entry into force of the AASPDP Act, the CPDP will adopt the remaining instruments of secondary legislation provided for in the Act. For the instruments for which an

opinion from the EDPB is required within the framework of the Consistency Mechanism, the draft law provides for a 12-month deadline for adoption.

The timely finalisation of the process of establishing the secondary-level legal framework in the field of personal data protection in the Republic of Bulgaria is a guarantee for conducting the supervisory authority's policy in the conditions of legal certainty, transparency and predictability.

3. New focus of control activities.

For the purposes of exercising its controlling power, the following main directions will remain unchanged in 2019:

- Developing up-to-date supervisory mechanisms in the light of the AASPDP Act and Regulation (EU) 2016/679, including developing different methodologies in line with the current priorities in the control activity.

- Effective and efficient supervisory activity, including through bringing the professional experience in carrying out sectoral inspections in line with the new legal framework.

- Performing the inspections required in relation to the requirements the Republic of Bulgaria needs to fulfil in order to achieve full accession to the Schengen area and the EU Visa Information System (VIS).

For this purpose, inspections of the national SIS II and inspections of at least two consular services in embassies of the Republic of Bulgaria abroad that issue a large number of Schengen visas will be planned and carried out.

- Strengthening the cooperation with the Ministry of Interior in relation to the fulfilment of the requirements of Directive (EU) 2016/680.

In this regard, inspections will be planned and carried out at the Europol, Eurodac and Interpol National Unit in 2019. In view of these commitments as well as in connection with the transposition of the Directive (EU) 2016/680 in the national legislation, the CPDP will strengthen its cooperation and interaction with the MoI and other structures of the internal security system, taking full account of their legal competences and the requirements for independence of the supervisory authority.

- Preparation of the CPDP for joint inspections in compliance with the requirements of the EDPB for cooperation between the supervisory authorities of the EU Member States.

4. To contribute to the efforts for full membership of the Republic of Bulgaria in Schengen and VIS.

The work of the CPDP in relation to the achievement of full membership of the Republic of Bulgaria in the Schengen area remains a priority task in 2019. The active participation of Commission representatives in Schengen evaluation missions in the field of personal data protection will continue and this not only increases the expert capacity of the institution in this field, but is also an indicator of the international reputation of the Bulgarian supervisory authority.

5. To promote the activities of the European Data Protection Board.

Although the EDPB as a new independent structure is relatively unknown to the general public, its role in aligning and furthering the data protection practice in the EU Member States will become increasingly important over time. Its powers provided for in the General Data Protection Regulation include, *inter alia*, the issuing of guidelines, recommendations and best practices for the implementation of the Regulation. Documents resulting from EDPB's activities are binding on interested parties and should therefore reach all addressees in an accessible and timely manner. The objective of the CPDP is to provide up-to-date information on the Board's activities through its website.

6. To strengthen international cooperation in relation to the requirements of the General Data Protection Regulation for a 'one-stop-shop mechanism'.

The General Data Protection Regulation seeks to make it as easy as possible for PDCs operating in more than one Member State and citizens to exercise their right to protection of their personal data. This is why Article 77 of the Regulation allows the person to choose and said person has the right to lodge a complaint with the supervisory authority in the Member State of his or her habitual residence or place of work or, alternatively, with the supervisory authority in the Member State in which the alleged infringement was committed. This provision is intended to be applied directly in its entirety. That is why the CPDP will make use of all available administrative channels to assist data subjects within the EU. An electronic system for the exchange of information between all supervisory authorities already exists and is operational, but it does not preclude the use of direct contact between the lead supervisor of a complaint and all other national authorities involved within the territorial scope of the Regulation.

7. To continue the CPDP information and awareness campaign.

The CPDP has registered a sustained interest expressed by PDCs, public bodies and citizens in training events and further clarifications on the implementation of the General Data Protection Regulation. In this connection, the information and awareness campaign implemented in 2018 will be expanded.

In view of the limited resources that the CPDP can invest in such a campaign, it will again be targeted both at data protection officers and target groups with a common focus, such as separate industrial branches, similar administrative and/or public structures, etc.

To achieve the maximum positive result in the described direction, the CPDP will seek to implement practical partnerships with various public and private initiatives. Thus specific issues and issues at both local and transnational level will be highlighted and common solutions valid for a particular sector or more generally for a large group of data controllers and data subjects will be offered.

The Annual Report of the Commission for Personal Data Protection for its activities in 2018 was adopted by a Decision of the Commission at a meeting held on 28 January 2019 (Protocol No 4).

CHAIRPERSON:

Ventsislav Karadjov (signed)

MEMBERS:

Tsanko Tsolov (signed)

Tsvetelin Sofroniev (signed)

Mariya Mateva (signed)

Veselin Tselkov (signed)