REPUBLIC OF BULGARIA

COMMISSION FOR PERSONAL DATA PROTECTION

ANNUAL ACTIVITY REPORT

of the Commission for Personal Data Protection

for 2017

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
BICA	–	Bulgarian Industrial Capital Association
APC	–	Administrative Procedure Code
ASCC	–	Appellate Specialised Criminal Court
SCAC	–	Sofia City Administrative Court
SEAV	–	Statement establishing an administrative violation
SAC	–	Supreme Administrative Code
SJC	–	Supreme Judicial Council
SANS	–	State Agency for National Security
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
SCIS	–	State Commission on Information Security
DPO	–	Data Protection Officer
TSIPC	–	Tax and Social Insurance Procedure Code
DFZ	–	State Fund 'Agriculture'
PIN	–	Personal Identification Number
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
SANS Act	–	SANS Act
API Act	–	Access to Public Information Act
EC Act	–	Electronic Communications Act
EG Act	–	Electronic Governance Act
HA	–	Health Act

PDP Act	–	Personal Data Protection Act
AASSANS Act	–	Act Amending and Supplementing the SANS Act
AASPDP Act	–	Act Amending and Supplementing the Personal Data Protection Act
CI	–	Compulsory instruction
DPCGLSG Act	–	Direct Participation of Citizens in Government and Local Self-Government Act
Acc Act	–	Accountancy Act
ElC	–	Election Code
IPA	–	Instrument for Pre-accession Assistance
QES	–	Qualified electronic signature
CPDP	–	Commission for Personal Data Protection
CRC	–	Communications Regulation Commission
MoI	–	Ministry of Interior
MFA	–	Ministry of Foreign Affairs
MoH	–	Ministry of Health
MoES	–	Ministry of Education and Science
NRA	–	National Revenue Agency
NDB ‘Population’	–	National Database ‘Population’
NHIF	–	National Health Insurance Fund
RICF	–	Research Institute of Criminology and Forensics
PD	–	Penal decree
CrPC	–	Criminal Procedure Code
RACPDPA	–	Rules on the activity of CPDP and its administration
SCC	–	Specialised Criminal Court
UIN	–	Unique Identification Number
NP	–	Natural Person
CEC	–	Central Electoral Commission
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 01.01.2017-31.12.2017.

The Report presents information on the main areas of CPDP activity during the period with a focus on the control and administrative-penal activities, the consideration of complaints lodged by citizens, and the provision of consultations to natural persons and personal data controllers (PDCs). Statistics regarding the registration of PDCs is provided. Due attention is 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. The degree of achievement of the objectives and priorities set for year 2017 is analysed, and the administrative capacity and financial position of CPDP during the reporting period are reported.

II. Analysis of the Degree of Achievement of the Objectives and Priorities of CPDP set in the 2017 Annual Report

The main objectives of CPDP and the related priorities for 2017 are grouped in three groups:

1. Focusing the effort of CPDP in key areas of national and supranational importance: the Bulgarian presidency of the Council of the EU, the 40th International Conference of Data Protection and Privacy Commissioners, and the accession to the Schengen area;

2. Ensuring the readiness of Bulgaria to implement its commitments stemming from the new European legal framework in the field of personal data protection, with a special focus on the interinstitutional and legislative preparation for the implementation of the new legal framework, the development of a national training centre and the development and implementation of an information system in pursuance of the requirements of the new legal framework.

3. Enhanced control activity in areas of high societal and social importance.

Under the first group of priority objectives of CPDP a significant amount of work was carried out in 2017, and as a result we can report that CPDP is absolutely ready to perform its tasks during the Bulgarian presidency of the Council of the EU in the first half of 2018, as well as to host, together with the European Data Protection Supervisor (EDPS), the 40th International Conference of Data Protection and Privacy Commissioners in October 2018. Some of the more important activities in this direction are:

A team for the Bulgarian Presidency of the Council of the EU, comprising 8 people and headed by the Chairperson of CPDP and one of the CPDP Members, was set up. All team members attended specialised training in public administration. In addition, each expert in the team is specialised in specific legislative files and EU topics.

A permanent coordination mechanism with EDPS was established, which includes, among other things, regular video conferencing. Conference halls for the international conference were selected and booked, and a draft programme of the events in Sofia was prepared.

In 2017 CPDP continued to provide assistance within its competence to the full accession of the Republic of Bulgaria to the Schengen area, taking into account the fact that the process is largely political. During the reporting period CPDP representatives participated in Schengen evaluation missions in Norway, Sweden, Iceland, Spain and Portugal, including in the capacity as lead experts, thereby further reinforcing the reputation of Bulgaria in the field of personal data protection.

In 2017 a significant progress was also achieved under the second group of priority objectives. With the assistance of the MoI, CPDP fulfilled one of the most important commitments related to the preparation for implementation of the new European legal framework in the field of personal data protection, namely a comprehensive draft law amending and supplementing the Personal Data Protection Act (AASPDP Act). It sets out the necessary national measures for the implementation of the General Regulation (Regulation 2016/679) and transposes the Directive on Data Protection in Police and Criminal Justice Activities (Directive 2016/680).

The new moments in the statutory regulation of the protection of personal data call for specialised and targeted training of PDCs to prepare them to meet the requirements of the General Regulation. This is especially valid for data protection officers, who must be covered by the training held. The analysis carried out by CPDP clearly demonstrated that the most effective way to respond to the training needs of the public and private sector in Bulgaria is to establish a National Training Centre for Personal Data Protection within CPDP, which shall be adequately supported by human and financial resources and shall assume the responsibilities relating to the training of data protection officers in Bulgaria as well as supporting tasks relating to the accreditation and certification in compliance with the General Regulation. The preparation for the development of the National Training Centre, including the development of a curriculum and learning content oriented towards the different target groups, in particular data protection officers, is at a very advanced stage. In addition, during the reporting period CPDP developed and published on its website a practical guide for PDCs with ten concrete steps to be taken to fulfil the new obligations arising from the General Regulation.

In pursuance of the requirements of Regulation (EU) 2016/679 of the European Union and of the Council, in 2017 and 2018 CPDP created the organisation required for the development and introduction of an information system maintaining the following public and non-public registers:

– Public register of personal data protection officers;

– Public register of accredited certifying bodies;

– Public register of codes of conduct;

– Non-public 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 general requirements for the information system, the description, the purpose and the structural data for each register are developed in order to be used at the 'Business Analysis of the System' stage and for preparing terms of reference for its development.

Under the third priority – enhanced control activity in areas of high societal and social importance, in 2017 CPDP organised and conducted an inspection in the Healthcare sector. Thus CPDP successfully built on the control activity already carried out in the inspection carried out in 2016 in the Education sector. Based on the actions carried out during the inspection, the findings and the conclusions made, a report was prepared containing recommendations, which play the role of instructions to the PDCs in the sector. The final report will be sent to the Minister of Health.

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

Pursuant to Article 10(1)(2) of the Personal Data Protection Act, CPDP keeps a register of PDCs and the registers of processed personal data maintained thereby. The PDC Register is public and is maintained electronically.

The CPDP's activity for maintaining the PDC Register is consistent with the e-Government concept and aims to provide citizens with a highly efficient and user-friendly service based on the 'single window' technology, as well as on the principle of 'single collection and generation of data' within the meaning of the Electronic Governance Act (EG Act). This activity is performed based on the information system for electronic registration of personal data controllers (eRALD). The system is a web-based application accessible from the CPDP website, which supports all PDC registration functions. It enables PDCs to submit electronic applications for registration as well as update the already uploaded data in accordance with the requirements of the PDP Act. The system contributes to reducing the administrative and bureaucratic burden on the activity of PDCs.

The public registers can be queried about registered PDCs and personal data registers maintained thereby, PDCs exempted from the registration requirement and PDCs the registration of which has been refused by CPDP.

The system is also accessible via the Single Portal for Electronic Administrative Services (egov.bg).

In 2017 the trend of PDCs registering via the Internet, including using a qualified electronic signature (QES), continued.

Between the inception of eRALD in 2009 and 31.12.2017 the total number of system users reached 371,044, of which 339,315 applied for PDC registration and 31,729 requested an exemption from the registration requirement (Figure 1).

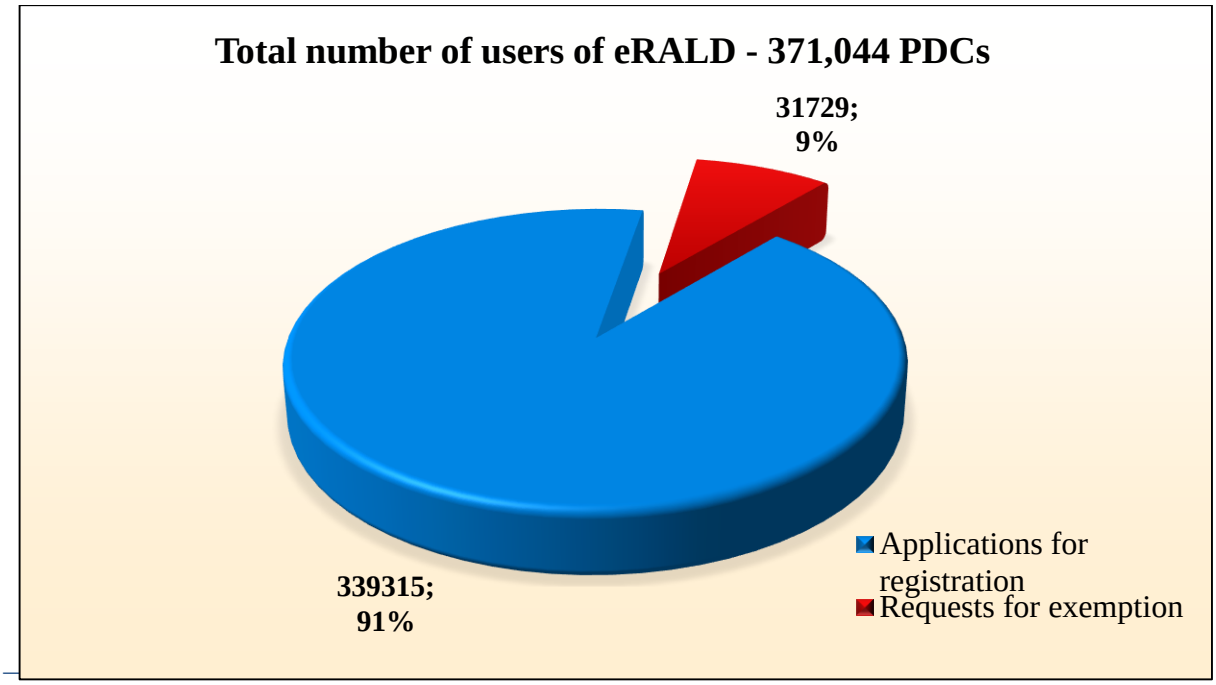

Figure 1

In 2017, CPDP registered 8,832 new PDCs. Thus, the overall number of PDCs entered in the register became 293,424 (Figure 2).

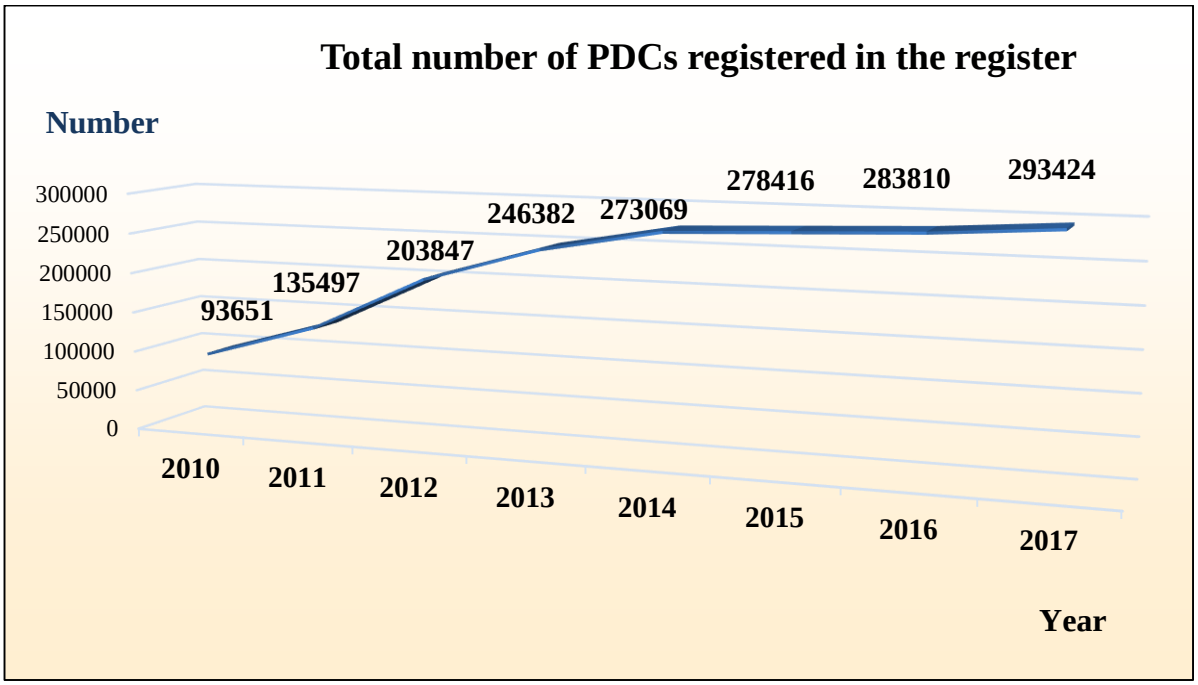

Figure 2

During the reporting period CPDP exempted from the obligation to register 429 PDCs, whereby their total number as of 31.12.2017 reached 28,464 (Figure 3).

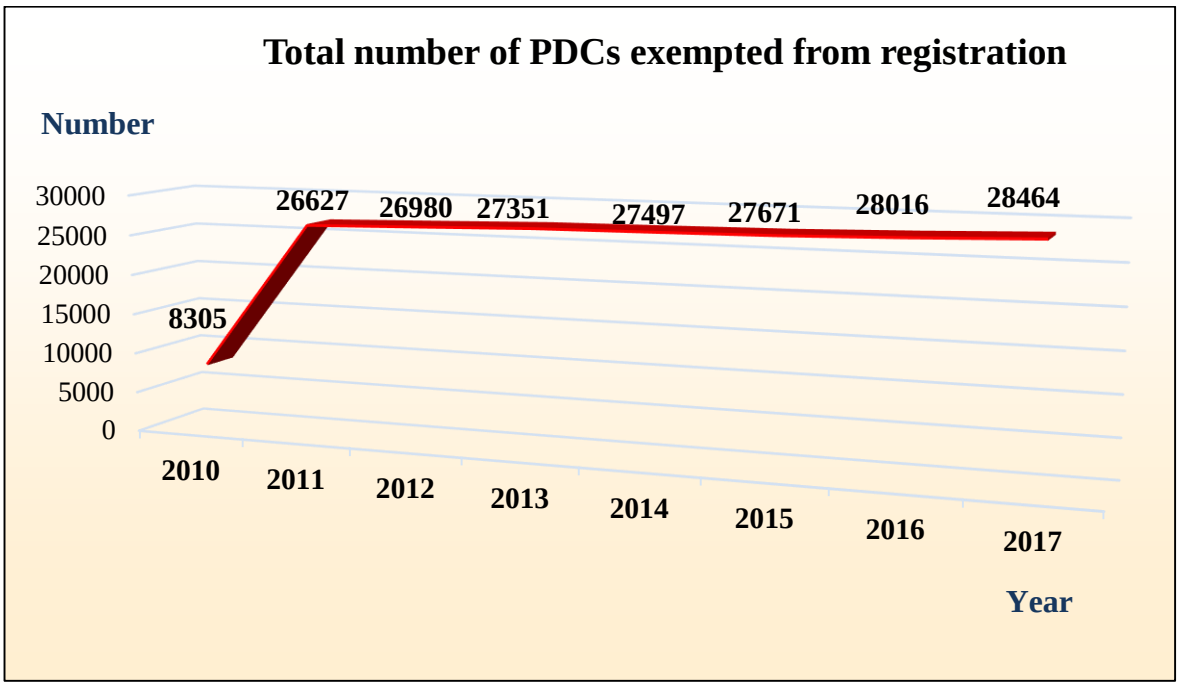

Figure 3

In 2017 CPDP deregistered from the register 68 PDCs, and the total number of deregistered PDCs reached 439.

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, 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 reporting period, 1,015 PDCs were subjected to ex ante inspections before being registered in the PDC Register under Article 10(1)(2) of the PDP Act.

Statistics relating to the registration of PDCs and registers kept thereby in 2017 confirms the conclusions made during the previous year, in particular:

– the processes relating to the registration of PDCs are stable, as shown in Figure 2 and Figure 3;

– the ratio between the number of applications for registration in the register and the number of requests for exemption from registration remains 91% to 9%.

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 CPDP

As part of its supervisory remit in the area of personal data protection, 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 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 an electronic signature; or via the CPDP website, and in this case the complaint shall also be in the form of an electronic document.

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 or inadmissibility. 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 CPDP which is an individual administrative act subject to two-instance judicial review.

With its decision on the merits of a complaint, CPDP may not honour the complaint as unfounded where no infringements of the complainant's rights are established, and in the case of a well-founded complaint 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 established by Article 12 of the PDP Act.

We shall 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 CPDP for the same offence or if the Commission's decision on the same violation has been appealed and no enforceable court ruling exists.

In recent years a trend is observed for individuals to initiate proceedings before the courts under the procedure established by Article 39 of the PDP Act. However, insofar as CPDP is requested to provide information on the absence of proceedings before it between specific parties and on specific occasions, it may be pointed out that the proceedings initiated under Article 39 of the PDP Act are very few in number compared to the proceedings initiated before CPDP. It is necessary to point out that insofar as the possibility to refer a case to 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 CPDP and thus the ability to protect the rights, provided for in the PDP Act, is available to all individuals.

- **Complaints Considered**

The total number of complaints filed with CPDP during the reporting period was 476. In addition, the Commission considered again 9 complaints returned by the court with instructions regarding the application of the law.

The statistics below do not include the results from the completed proceedings in connection with complaints relating to the processing of personal data for the registration of parties, coalitions or initiative committees for participation in the information campaign of the national referendum held on 6 November 2016 and for the registration of parties, coalitions or initiative committees for participation in the elections for President and Vice President of the Republic held on 6 November 2016.

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

1. on whether the complaints are founded – 120 decisions;

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

3. on inadmissibility of complaints – 45 decisions;

4. on irregularity of complaints and requests – 52 decisions.

Sixty-one complaints were rejected as unjustified since CPDP did not find violations of personal data processing rules or of complainants' rights. The ratio of justified vs. unjustified complaints is presented in the table below (Figure 4):

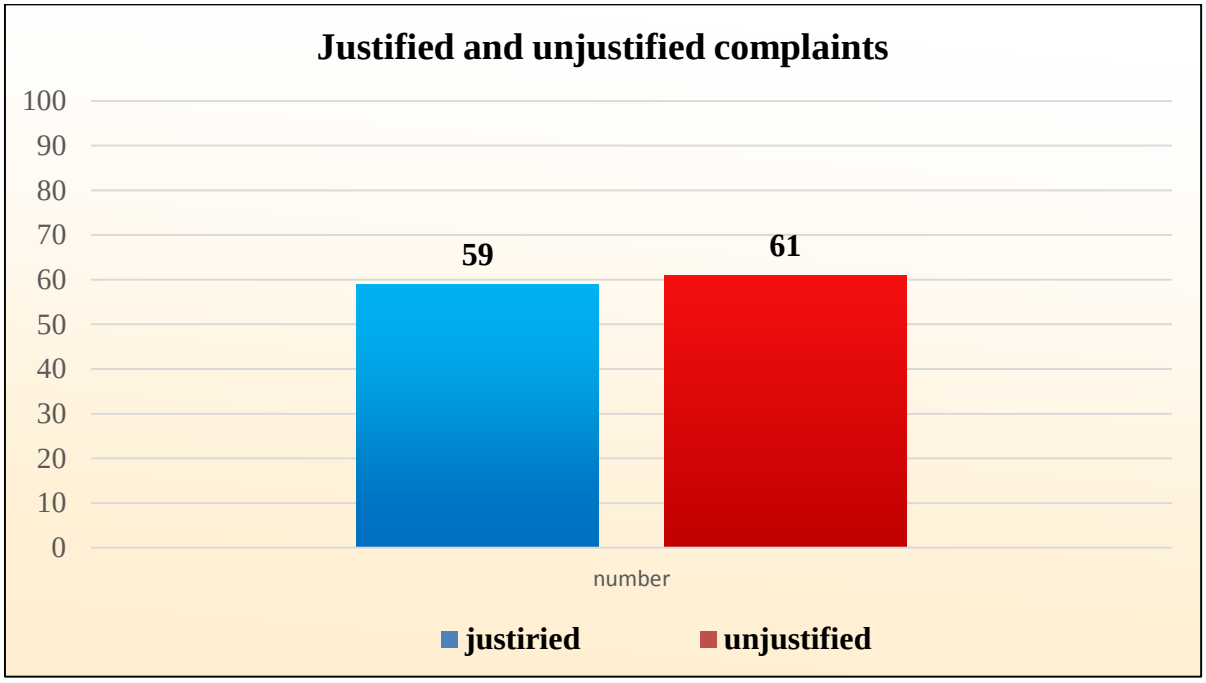

Figure 4

CPDP found 59 complaints to be justified. The proceedings closed with imposing administrative penalties were related to 25 complaints, and under 34 complaints CPDP issued compulsory instructions. The ratio is shown in the following table (Figure 5):

Figure 5

Figure 5: Compulsory instructions issued and sanctions imposed

□ **sanctions**

□ **compulsory instructions**

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

– processing of personal data in violation of the principles of lawfulness, proportionality of the data processed and processing of the personal data for specific, clearly defined and legitimate purposes (Article 2(2) of the PDP Act): 4 violations, in respect of which CPDP imposed pecuniary sanctions in the total amount of BGN 76,000;

– processing of personal data in the absence of a lawful reason for the data processing operation (Article 4 of the PDP Act): 12 violations, in respect of which CPDP imposed pecuniary sanctions in the total amount of BGN 130,000;

– 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): 8 violations, in respect of which CPDP imposed pecuniary sanctions in the total amount of BGN 7,700;

– failure of the PDCs to assist the CPDP exercise its supervisory powers (Article 22(5) of the PDP Act): 4 violations, in respect of which CPDP imposed pecuniary sanctions in the total amount of BGN 20,000.

– failure of PDCs to provide the individual with information regarding the PDC and its representative; the purposes of the processing of personal data; the recipients or the categories of recipients to which the data can be disclosed; data regarding the mandatory or voluntary nature of the provision of data and the consequences of the refusal to provide the data; and information regarding the right of access to and the right to rectify the data collected. CPDP established 1 violation, in respect of which it imposed a pecuniary sanction in the amount of BGN 2,000.

In 7 of the administrative procedures closed due to inadmissibility, the complainants withdrew their complaints; in practical terms this means that CPDP was de-seized.

In 59 of the administrative proceedings completed in 2017, CPDP decided that the complaints were founded, and in its decisions relating to the proceedings issued 34 compulsory instructions to PDCs to take measures and actions for personal data protection, and established a total of 30 administrative violations of the PDP Act, in respect of which it imposed pecuniary sanctions and fines in the total amount of BGN 233,700.

- **Statistics of Complaints by Sectors**

There are several sectors with a large number of complaints.

Although fewer complaints were received in 2017 than in 2016, the leading sector is 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.

Next come the complaints against banks and companies offering 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.

A trend of increase in the number of complaints is also observed with regard to video surveillance. With regard to the subject of complaints to 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.

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

Telecommunications – 91 complaints

Video surveillance – 32 complaints

Banks and credit institutions – 23 complaints

Political entities – 32 complaints

Judicial and executive authorities – 28 complaints

Media – 12 complaints

Employment and social security services – 18 complaints

Education – 6 complaints

Local authorities – 9 complaints

- **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:

CPDP was approached by an individual in connection with the provision of his personal data by his employer to a bank for the purposes of opening a current account and issuing a bank card. The evidence collected in the course of the administrative proceedings show that the employer and the bank have concluded a contract for processing of transfers of employment remuneration. The purpose of the contract is to settle the relationships between the parties in relation to the transfer of salaries, employment remuneration, advance payments,

bonuses and other amounts payable by the employer as employment and equivalent remuneration to the bank accounts of workers and employees with the bank and other commercial banks in the country. In pursuance of the contract, the employer has provided the personal data of the complainant to the bank without the consent of the individual.

Given the violation and the activities of the company, and in view of the fact that this is the first violation of the PDC, CPDP considers it appropriate to issue a compulsory instruction to the company, believing that this will act as a warning and have a preventive effect and will contribute to the compliance of the company with the established legal procedure. In the specific case, by issuing a compulsory instruction, individual prevention will be achieved as the objective of the administrative measure of constraint, taking into account the fact that the imposition of the administrative penalty pecuniary sanction would unreasonably create financial barriers to the conduct of the company's activity.

CPDP was approached with a complaint alleging unlawful processing of the personal data of the complainant by 'Urban Mobility Centre' EAD in the hypothesis of scanning a personal identity card in connection with the issuing of a personalised electronic travel card for public transport in Sofia.

The complainant states that she has filed an electronic application for the issuance of an electronic travel card for public transport in Sofia and has attached an electronic photograph to the application. She adds that the next day she visited a point of sale of the company to receive the card she requested, and presented a printed electronic application and an ID card for reference. She claims that an employee of the company scanned her ID card without her knowledge and consent, and the issued personalised travel card for public transport is with the photograph from the ID card which is different from the photograph attached to the application for the issuance of the card.

In the course of the on-site verification at the point of sale for travel documents, specified in the complaint, it was found that the complainant's personal data were stored in the company's database – name, personal identification number, date of birth, address and telephone. The team carrying out the verification did not find a stored copy of the ID card of the complainant.

In this regard, and in view of the scanning device and the application software of the company, and the conclusion of the CPDP team carrying out the inspection, the Commission considers that the company's assertions that it has scanned only the person's photograph contained in the ID card and not the entire ID card, and that the company does not store a scanned copy of the complainant's identity card, are true, and any concerns as to the contrary are unfounded.

Although the technology deployed by the company – the scanning device and the application software – are undoubtedly in the public interest and for the benefit of the company's clients, their use without the knowledge and consent of the client in the particular case of the complainant violated her rights under the PDP Act. In view of the fact that the complainant's photograph – image is attached to the electronic application submitted thereby, it must be concluded that the collection in the form of scanning of an image from the complainant's identity card and the use of the image for the issuance of a public transport card is in breach of Article 4(1) of the PDP Act. The scanning has been made without the knowledge and consent of the complainant, a fact which is not disputed by the respondent, and without any of the other preconditions mentioned in the provision for admissibility of the processing of the complainant's image contained in her identity card.

CPDP was approached with a complaint containing allegations of unlawful processing of the personal data of the complainant, in particular names, address and information regarding the real estates owned, through the provision of documents containing such data by the Sofia Municipality to a commercial company and through publishing the data at www.nss.gis-sofia.bg, where they are freely available.

The complainant claims that after typing his full name in the search engine Google he established, that his personal data are freely available at: http://nss.gis-sofiq.bg/get_pdf.php?pdf_id=5104, where a penal decree issued by Sofia Municipality, 'Architecture and Urban Planning' Division, 'Municipal Development Control' Directorate is published. He adds that the document is freely accessible and contains his personal data. Only the personal identification number is blotted in the document, but the remaining data – names, address and information regarding the real estates owned, are available to an unlimited number of people.

In the course of the administrative proceedings it was established that penal decree No РД-ХХ-УУ/2015 and resolution No РД-ХХ-УУУ/2014, issued by Sofia Municipality, 'Architecture and Urban Planning' Division, are published and freely accessible on the site www.nss.gis-sofia.bg. Contrary to the assertions of Sofia Municipality that the documents are published in the site of Sofia Municipality www.sofia-agk.com, it was established that the documents are also published and freely available on another site – www.nss.gis-sofia.bg, a public address space registered and maintained by 'Geographic Information System – Sofia' EOOD, and the access to this site is possible via a link from the website of Sofia Municipality www.sofia-agk.com.

It should be pointed out that the information contained in the published documents, i.e. three names and address of the individual, is sufficient for his indisputable identification and has the nature of personal data of the person, contrary to the arguments of the respondent to the contrary.

In view of the established violation of the provisions of the PDP Act and in order to discontinue the violation both with regard to the processing of personal data of the complainant and with regard to personal data of other individuals – addressees of the published instruments, CPDP considered it expedient to issue a compulsory instruction to the PDC to implement the required technical and organisational measures and to strike out or anonymise the personal data contained in the published documents.

CPDP was approached with a complaint containing allegations of unlawful processing of the personal data of the complainant for the purpose of conclusion of a contract for the provision of electronic services and purchase of an end device. Based on the circumstances collected in the file it was established that three contracts between the PDC and the complainant were drawn up in the office of the company processing personal data on behalf of the PDC.

These contracts contain the three names, the Personal Identification Number and the number of the ID card of the complainant and these are indisputably personal data according to the legal definition of Article 2(1) of the PDP Act in view of the fact that they can be used to directly identify the complainant. In the specific case there is assignment of the processing of personal data within the meaning of Article 24(1) of the PDP Act with a volume of the obligations of the parties, set out in an agreement.

The evidence collected in the administrative file shows that the company processing personal data has processed the personal data of the complainant for the purposes stated in the agreement – three contracts were drawn up. Pursuant to the partnership agreement, the company processing personal data is obliged to submit to the PDC the originals of all service contracts and other documents based on which services are activated and provided.

After receiving the contracts, the PDC has also processed the personal data of the complainant by performing the actions 'use' and 'provision', specified in § 1, item 1 of the Supplementary Provisions of the PDP Act. The company has used the data to treat the complainant as a client and to accrue liabilities under the prepared contracts. In order to collect the accrued liabilities under the specified invoices and accounts, the PDC has provided the personal data of the complainant consecutively to two companies. The provided letters show that the provided personal data contain at least three names and address.

CPDP considers that the complainant's allegations that his personal data have been unlawfully processed by the personal data controller and by the personal data processor in connection with the concluded contracts are well founded, although they have been challenged by the respondent companies.

The evidence collected in the administrative file and, in particular, the results from the expert assessment show that the signatures under the contested contracts were not affixed by the complainant. This leads to the conclusion that there is no consent from the individual within the meaning of § 1, Item 13 of the Supplementary Provisions of the PDP Act – freely given, specific and informed statement of volition by which the individual to whom personal data relate signifies unambiguously his or her consent to such data being processed. In this sense, the grounds under Item 2 of Article 4(1) of the PDP Act for the processing of personal data for the purposes of the contracts do not exist.

In the specific case none of the remaining hypotheses specified in Items 1, 3, 4, 5, 6 and 7 of Article 4(1) of the PDP Act exist – the processing was not carried out in order to comply with an obligation imposed on the PDC by a piece of legislation, it was not necessary for the fulfilment of obligations under a contract to which the individual is a party, it was not necessary in order to protect the life and health of the individual or for the performance of a task carried out in the public interest, or for the exercise of an official authority vested by law in the PDC, or for the realisation of the legitimate interests of the PDC overriding the interests of the individual.

This means that the personal data of the complainant have been processed by the personal data controller and the personal data processor without any grounds for admissibility of the processing under Article 4(1) of the PDP Act, thereby breaching the principle of processing of personal data in legal compliance and in a bona fide manner stipulated in Item 1 of Article 2(2) of the PDP Act. The personal data of the controller have been processed by the personal data processor by actions of collecting and use for drawing up the contracts, and the PDC has used them to accrue liabilities and has provided them to other companies for collection of receivables. In this connection, one of the highest pecuniary sanctions at the time for each of the violations was imposed on the two companies.

2. Case Law Relating to Appealed Decisions of CPDP

In 2017, the Sofia City Administrative Court (SCAC) initiated 44 cases on appeals against administrative instruments issued by CPDP. The cases before the Supreme Administrative Court (SAC) in the capacity of appellate court were forty-six (46), and all of them were initiated in prior years.

During the reporting year, sessions of panels of the SCAC were scheduled for 39 cases, of which 18 cases initiated in 2016 and 21 cases initiated in 2017. It shall be noted that 5 of the cases initiated before SCAC in 2017 were scheduled for consideration in 2018.

Of all cases considered by the SCAC, 36 were concluded with judgements, and 8 are pending the judgement of the corresponding panels. Also, in 2017 the SCAC ruled on 11 court cases which were announced for ruling in 2016.

The information available shows that 30 judgements confirmed the appealed administrative instruments of CPDP. In 3 of them the court decreased the penalty imposed by CPDP, in 3 judgements the CPDP decisions were partially repealed, and in 10 judgements the instruments issued by the Commission were rescinded.

The figure (Figure 6) shows the number of confirmed and cancelled decisions of CPDP:

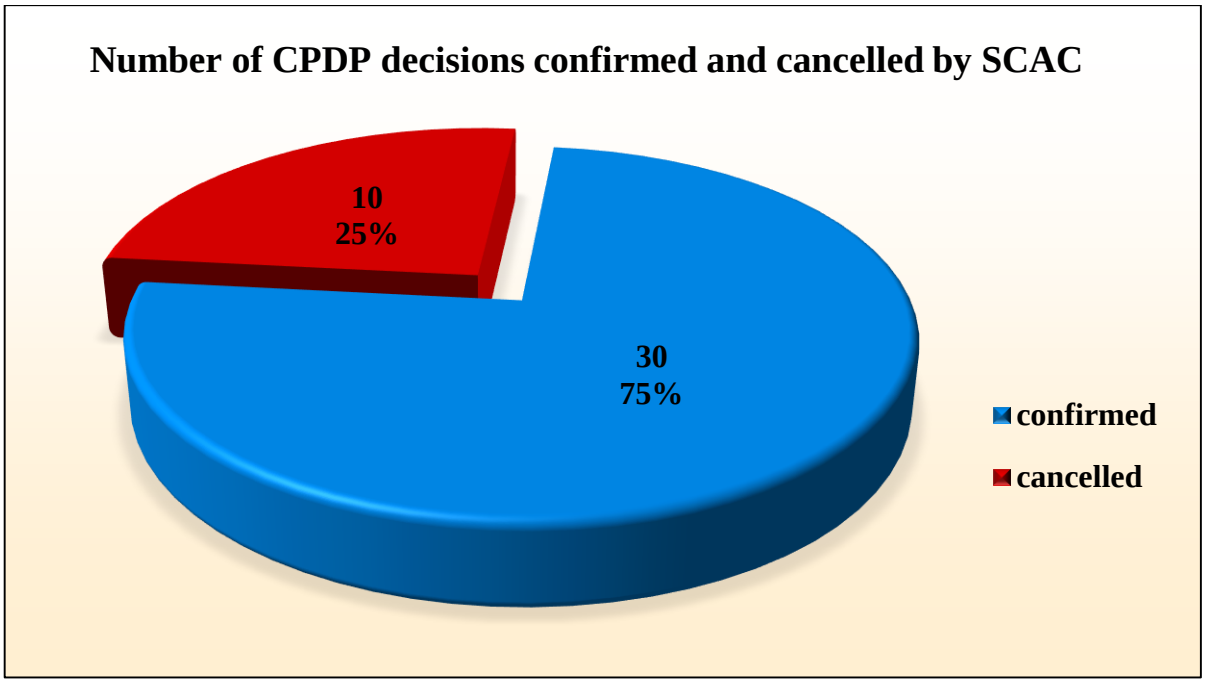

Figure 6

In 2017, SAC held sessions on 46 cases, of which 1 case initiated in 2015 and the rest – in 2016. In 2017 SAC did not hold sessions on cases initiated in 2017. These cases are scheduled for consideration in 2018 and 2019.

SAC confirmed 13 judgements of the SCAC confirming the instruments issued by CPDP and rescinded 5 judgements of the SCAC thus confirming the corresponding instrument issued by CPDP. In 2 judgements the SAC rescinded the judgements of the SCAC and amended the CPDP decision, and 3 judgements confirmed the judicial instrument issued by the SCAC and rescinding the instruments of CPDP. In 2 judgements the SAC rescinded both the judgement of the SCAC and the decision of the Commission.

In conclusion, it can be said that following a two-instance judicial control of 48 cases related to appeals against decisions of CPDP, 21 decisions of CPDP were enforced, and 9 were rescinded.

In view of the final result, the practice of SAC with regard to instruments issued by CPDP can be expressed graphically as shown below (Figure 7):

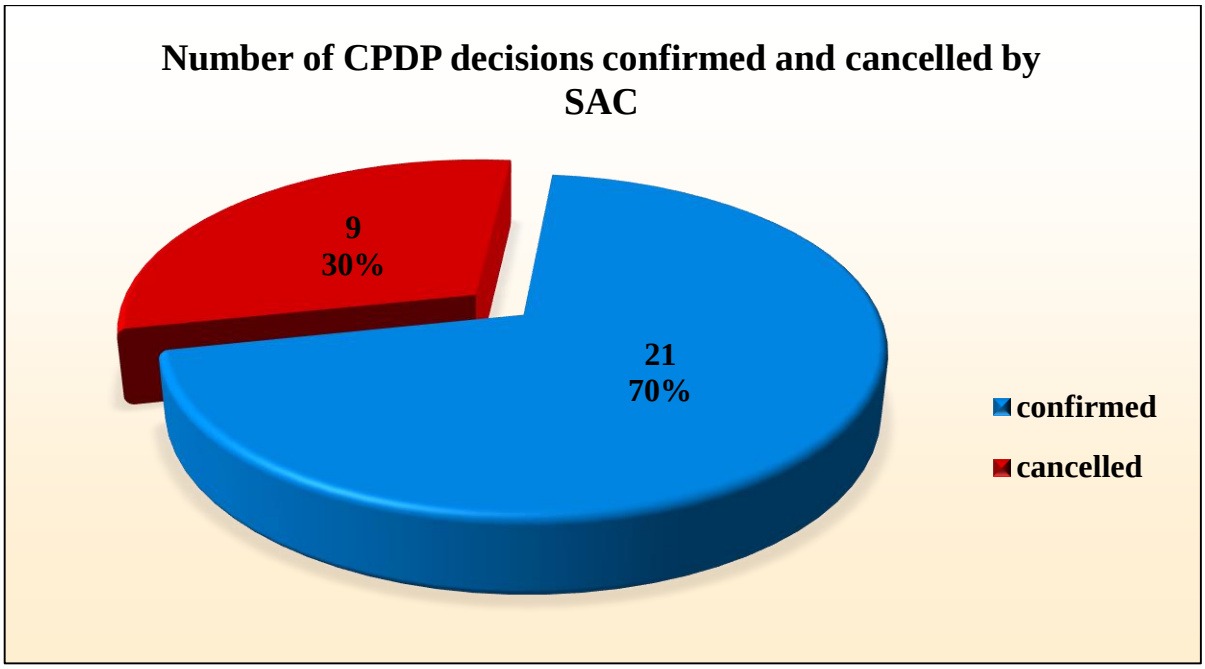

Figure 7

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

The total amount of the penalties imposed by CPDP administrative instruments in 2017 was BGN 544,000. The amounts collected pursuant to CPDP decisions in 2017 came to BGN 112,850, of which BGN 13,500 were collected coercively by the NRA.

4. Advice Provided to Citizens

Questions from citizens received by CPDP in 2017 covered different spheres of public life. Citizens are becoming more active in seeking assistance and explanations in relation to the application of the personal data protection rules. An evidence to this is also the statistical analysis of the answers provided by CPDP – 362, which is an increase compared to previous years of 120% on 2015 and 90% on 2016. The reported increase is due to different factors.

On the one hand, increased interest from businesses and citizens in the new data protection measures introduced by Regulation 2016/679 (the General Data Protection Regulation).

At the same time, the increase is also due to the fact that CPDP provides different opportunities for consultations with experts from its administration. This makes it easier for citizens to contact CPDP, because the experts are available for communication via e-mail, telephone and on-site in the CPDP building. The goal is to satisfy inquiries by providing the most complete and useful information. The results from the hard work are in place – in 2017 the Citizens against Bureaucracy Foundation nominated the Commission for Personal Data Protection as the 'State Institution of the Year'. This recognition is a distinction for the comprehensive assessment of the work of the institution for the benefit of businesses and citizens. This is a second award in a row for CPDP, given by the Citizens against Bureaucracy Foundation. In 2016 CPDP received an award in the category 'Best service to citizens'.

The inquiries regarding the implementation of the General Data Protection Regulation are increasing. Questions concern the scope of the regulation, the new obligations of data controllers and processors, the abolition of the registration obligation for PDCs, etc.

The most numerous inquiries in relation to the General Data Protection Regulation concern the obligation to appoint a Data Protection Officer. The criteria for appointment of a data protection officer in private companies are listed in Article 37 of the Regulation and are related to the operations of the relevant PDC, in particular: 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 key activities for achieving the objectives of the controller or the processor can be regarded as core activities. They also include activities for which the data processing comprises an integral part of the operations of the controller or the processor. On the other hand, all organisations perform certain auxiliary activities, such as making payments to their employees, or have standard IT support activities. These are auxiliary functions necessary for the core activity of the organisation. Although these activities are not required or material, they are commonly considered as ancillary functions rather than core activities.

During the reporting period many requests were received in connection with giving consent under the General Data Protection Regulation. The guidelines provided by CPDP in

its responses to citizens are that consent is one of the alternative grounds for the lawful processing of personal data, both in the current Directive 95/46/EC and in the new legal framework. The Regulation further develops the consent as a legal construct and gives a more detailed legal definition in Article 4, paragraph 11, according to which 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It is stipulated that the consent of the data subject can be given by a statement or by a clear affirmative action, establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. The PDC should be able to demonstrate (and to provide the relevant evidence) that the data subject has given consent to the processing of his or her personal data. The consent shall be 'unambiguous', i.e. shall demonstrate by clear actions leaving no room for doubts that the data subject agrees to the processing of his or her personal data. One of the elements of the consent of the data subject with regard to the processing of his or her personal data is that the consent shall be 'informed'. This means that the conditions envisaged in Article 13 of the Regulation shall be complied with, and in particular information shall be provided regarding the identity of the PDC, the purposes of the processing, the recipients or categories of recipients of the personal data, etc. On the other hand, the data subject shall be provided with the opportunity to withdraw his or her consent at any time without detriment.

- **Inquiries from Citizens and PDCs**

Many questions in 2017 were also related to the registration of PDCs and to the providing of technical and operational measures for protection. All persons that process personal data and keep registers of information constituting personal data are obliged to register as PDCs. Even where such persons and bodies discontinue their operations, the activity relating to the processing of personal data may continue in connection with their storage – for example, keeping of a large number of files containing personal data of former employees. If the PDC is already registered, the registration shall be updated upon each

change in the circumstances relating to the person.

The CPDP's responses in connection to the obligation of PDCs to register focus special attention on the fact that from the start of the application of the General Data Protection Regulation the obligation of PDCs to register is abolished. This is justified by the principle of accountability provided for in the Regulation, namely that the processing of personal data shall comply with the requirements set out in the Regulation, and PDCs at all times shall be able to demonstrate this. PDCs shall also be obliged to keep their own registers of the personal data processing activities.

It is interesting to note that on several occasions during the reporting period CPDP received requests in connection with the wish of different individuals to prepare in electronic form an album – register of teachers and all the alumni of the IV Language School in Varna**.** The desire of individuals is to have access to data – a photograph, date of birth, place of birth, and year and class in which each pupil graduated, but the school principal does not grant access because of the fact that these are personal data and should not be provided. It is stated in the CPDP's responses that the activities, relating to the access to and using of a photograph, date of birth, place of birth, year and class in which each pupil graduated, constitute 'processing of personal data' according to the legal definition in § 1(1) of the Supplementary Provisions of the PDP Act. In this case, the provisions of Article 4(1) of the PDP Act shall be applied with respect to the lawful conditions under which the processing of personal data is allowed. This text sets out alternative grounds in the presence of which personal data may be processed only in the cases where at least one of the specified conditions is met. Paragraph (2) of the same Article states that personal data processing shall be allowed also in cases when performed exclusively for the purposes of journalism, literary or artistic expression to the extent to which such processing does not violate the right to privacy of the person to whom the data relate. On the other hand, when personal data is processed the main principles of the PDP Act shall also be complied with, in particular: data shall be processed in legal compliance and in a bona fide manner; they shall be captured for specific, precisely defined and legal purposes and not be submitted to additional processing in a manner incompatible with such purposes; and shall be maintained in a form that enables identification of the respective individuals for a period not to exceed the time necessary for the purposes for which such data are being processed.

In 2017 CPDP observed a trend for questions relating to the need for registration of professional building managers and condominium managers as PDCs. The CPDP response in these cases is that the persons acting as professional condominium managers shall register as PDCs in the Electronic Register of PDCs kept by CPDP.

With regard to condominium managers (chairpersons of management boards), in the cases where the individuals are owners or lessees in the building, CPDP decided that these persons are PDCs and, simultaneously, on the grounds of Article 17a(2) of the PDP Act waived the obligation of condominium managers to register as PDCs due to their large number and frequent change.

In 2017 CPDP also received inquiries regarding the processing of personal data by condominium managers, including professional condominium managers. The inquiries concern the capacity of these individuals as PDCs, the receiving of data from other controllers, including municipal administrations, other/previous building managers, etc.

During the reporting period questions were frequently asked in connection with the fact that employers require from their employees at the time of appointment to provide a copy of their ID cards. In connection with this, the inquiries regarding the photocopying of ID cards by employers also became frequent.

The CPDP position on this issue is that the employer does not have the right to make a copy the ID card of the worker/employee for the purpose of storing it in the employment file, but only has the right to copy the data in it and return it to its owner.

In 2017, requests from air carriers relating to provision of scanned copies of passenger ID documents increased. One reason for these questions is that the official website of CPDP explicitly states that only PDCs which have legal grounds stipulated in a statutory instrument have the right to photocopy ID cards. In this connection, CPDP was asked if airlines have legal grounds to require from passengers a copy of an ID and, if so, under what conditions such a copy can be provided to the carrier. The question asked concerns the hypotheses under which the carrier is a legal entity registered in the Republic of Bulgaria, in a European Union Member State, or in a third country. In this connection the CPDP responses

state that data contained in ID cards of customers of air carriers fall within the category of 'personal data' protected by the PDP Act. Taking a copy of an ID card is an action of processing of personal data within the meaning of the PDP Act. Prior to taking a copy or processing the ID card in any other manner, the PDC shall inform individuals about: the purpose of taking a copy; the recipients to whom the data may be disclosed; whether taking a copy is mandatory or voluntary; the consequences of the refusal for the respective individual; the right of access to and the right to rectify already collected data. At the same time, the replies of CPDP emphasize that the provisions of Article 42b(1) of the State Agency for National Security Act list exhaustively what personal data the air carriers collect, namely they are obliged, on their own account or through an authorised service provider, to transmit to the National Unit passenger name records for all flights to, in or from the Republic of Bulgaria. Exhaustively listed data collected with respect to passengers do not contain a requirement for air carriers to process in the form of copying and to provide a copy of an identity document.

In 2017 CPDP received questions from farmers in connection with the submission of applications under coupled support schemes for realisation of fruit and vegetables. Farmers submit to the State Fund 'Agriculture' (DFZ) accounting documents as evidence of the realisation of the relevant production. Farmers provide scales receipts that show that they are sellers, in the capacity as farmers, with BULSTAT and address, and with regard to buyers, who in most cases are natural persons, the following data are required: names and settlement, type of produce, quantity, unit price and total amount. In the questions to CPDP it is reflected that DFZ refuses to accept scales receipts because the buyers have not indicated their personal identification number and address. In this connection, the questions are asked in what capacity and on what grounds farmers should require personal data such as personal identification numbers and addresses from their buyers.

In connection with the information presented and in order to make am objective ruling, CPDP made a formal inquiry to the Executive Director of DFZ on the issues raised. In response to the inquiry, information was received that the requirement for entering names, addresses and personal identification numbers of individuals in the scales receipts was based on Ordinance No 3 of 17 February 2015 on the Conditions and Procedure for the Application of Direct Payment Schemes. The procedure for implementation of the schemes is related to

declared participation in the coupled support schemes for fruit, coupled support schemes for vegetables and coupled support schemes for greenhouse vegetables. Pursuant to the provisions of the ordinance, applicants under the schemes shall prove yields from the declared areas for the requested crop by submitting a declaration and an inventory in a standard form approved by the Executive Director of DFZ for the production during the year of application, as well as documents proving its realisation. Documents proving the realisation of the produce are as follows: invoices and/or fiscal receipts issued by a fiscal device where the applicants are traders within the meaning of Article 1 of the Commerce Act; documents containing the requisites under Article 6(1) of the Accountancy Act where the applicants are persons under Article 9(2) of the Personal Income Tax Act. As stated in Article 6(1) of the Accountancy Act, primary accounting documents addressed to external recipients shall contain as a minimum the following information:

1. Name and number of the document containing only Arabic numerals;

2. Date of issue;

3. Company name or name, address and identification code from the Commercial Register or unified identification code under BULSTAT, or personal identification number, or personal number of foreigner of the issuer and the recipient;

4. Subject, physical and value expression of the business transaction.

DFZ assures that they strictly observe the provisions of the national legislation, which predetermines the need for all documents provided to contain the mandatory requisites described in Article 6(1) of the Accountancy Act.

In 2017, there were numerous inquiries related to the provision of personal data by mobile operators to debt collection companies. Usually the companies – creditors provide the personal data of the customers – debtors to debt collection companies with the prior knowledge and written consent of the customers – individuals. This is done by including relevant texts in the General Terms and Conditions provided to customers at the time of signing individual contracts with them. The General Terms and Conditions are an integral part of individual contracts, and at the time of signature of contracts, the customer is provided with a copy of the General Terms and Conditions. Additionally, individual contracts include texts that specify the purpose for which the customer's data may be provided to third parties, namely for the recovery of claims due under the contract.

A number of inquiries relating to video surveillance were received during the year. Citizens are interested in the lawfulness of this activity in different places, including public locations, schools, kindergartens, entrances to housing units, etc. The matter of the obligation to register as a PDC when performing video surveillance is also of interest.

Inquiries about the legality of copying identity cards by banks in carrying out banking operations continue. The CPDP responses contain information to the effect that the Measures Against Money Laundering Act introduces preventive measures with respect to certain legal entities, including banks, in particular actions for identifying customers and verifying their identification. Individuals are required to present an official identity document and banks shall register its type, number, issuing authority, as well as name, address, personal identification number, and for individuals having the status of sole trader – also to present the documents identifying it in its commercial capacity.

Another trend is the increase in the inquiries regarding the obligation of Internet merchants to register as PDCs within the meaning of the PDP Act.

- **Inquiries Received through the Centre for Information and Contact**

The Centre for Information and Contacts (Call Centre) of CPDP is an important communication channel for direct communication with citizens and improving the quality of services. Its goal is to satisfy inquiries by providing as full information as possible from the very first call. In 2017, 6,765 inquiries were received in the Centre for Information and Contacts. Compared to the previous year, their number is relatively higher, with an increasing tendency to use the call centre as an opportunity for direct contact with CPDP experts. The average monthly number of calls to the Centre for Information and Contact is approximately 677. Among the most frequently asked questions are those regarding the registration of PDCs as well as questions relating to filing complaints in cases of misuse of personal data of citizens during the 2017 Parliamentary elections and complaints about the misuse of personal data by social networks, institutions and the so-called

collection companies. Recently, questions relating to upcoming training events on the new requirements of Regulation (EU) 2016/679 have increased.

This year as well there were numerous questions relating to the registration of PDCs. The number of inquiries to the call centre relating to the registration of PDCs has almost doubled compared to the previous year.

Frequently PDCs find it difficult to determine the scope of personal data registers processed by them, respectively the number and the statutory grounds for keeping such registers. Applicants are frequently not familiar with the statutory regulations and therefore need to get support from the call centre operators. A large number of issues giving rise to problems with the description of registers is that frequently requisites pertaining to different types of registers are combined. The questions relating to the recovery of a username and a password for access to the registration of PDCs are many. It can be summed up that a large portion of PDCs do not keep the information entered in the electronic register up-to-date.

There is frequently lack of clarity in the applications for processing of personal data relating to health (data within the meaning of Article 5 of the PDP Act), with regard to which special legal requirements exist.

The Centre for Information and Contacts receives 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.

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

A significant number of questions are related to the misuse of personal data in the lists submitted to the Central Electoral Commission (CEC) by initiative committees and parties in connection with the 2017 Parliamentary elections. A large portion of the inquiries to the Centre for Information and Contacts concerns the ways of filing a complaint with CPDP.

Summary information on the frequency and number of inquiries at the Centre for Information and Contacts during the reporting period according to their subject is presented below:

- regarding registration of PDCs – 3,119 inquiries with a frequency of approximately 312 inquiries a month;

- regarding the signing of the confirmation sheet with an electronic signature – 1,145 inquiries with a frequency of approximately 114 inquiries a month;

- regarding the issuing of certificates to PDCs – 1,053 inquiries with a frequency of approximately 105 inquiries a month;

- inquiries regarding user names and passwords for logging into the system of the electronic register – 934 inquiries with a frequency of approximately 93 inquiries a month;

- regarding the registration as PDCs of companies selling online products over the Internet – 394 inquiries with a frequency of approximately 39 inquiries a month;

- inquiries regarding Regulation (EU) 2016/679 and the amendments to the PDP Act relating thereto during the second half of 2017 – 85 inquiries with a frequency of approximately 14 inquiries a month;

- questions relating to filing complaints about the misuse of personal data of citizens in connection with the 2017 Parliamentary elections – 35 inquiries with a frequency of 18 inquiries a month.

Complaints/alerts and questions are also sent via the standard forms for filing on the CPDP website. Access to standardised forms of communication and interaction with the institution is provided, clear guidelines are 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 are numerous and varied in nature, and those reporting misuse of personal data in social networks, fast-track lenders and government institutions prevail. The case of the website of the Commission for Disclosure of Documents and Exposure of the Affiliation of Bulgarian Citizens to State Security and the Intelligence Services of the Bulgarian People's Army, where the personal data of a staff member of the National Social Security Institute – Targovishte are disclosed, is indicative.

The number of alerts relating to the collecting of information about the educational level and employment status of the families of pupils by a work card – module 'Characteristics of the environment' sent by the MoES to schools and kindergartens increased.

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

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 continues.

There was a significant number of complaints relating to the misuse of personal data in the lists submitted to the CEC by initiative committees and parties in connection with the 2017 Parliamentary elections.

In connection with the children's competition 'What others know about me?' organised by CPDP, during the reporting period questions relating to the requirements and proposals for awards to participants were received.

In 2017 inquiries were received about the legality of 'Blizoo Media and Broadband' EAD requiring a personal identification number when users refuse to use digital/cable TV. In this connection CPDP delivered an opinion on the case and published it in its website.

Through the form for submission of questions via the CPDP website, inquiries are made by foreign individuals regarding the interpretation of the new EU Data Protection Regulation as well as questions relating to the Schengen visa and the tax obligations of Bulgarian citizens living abroad.

There are numerous requests for meetings in connection with the implementation of Regulation (EU) 2016/679, as well as questions related to PDP training, queries regarding seminars and certification of companies falling within the scope of the European Regulation. Requests for training are received from banks, mobile operators and law firms. Some of the questions are related to the new obligations of personal data controllers and processors to appoint a data protection officer pursuant to the requirements of Regulation (EU) 2016/679.

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.

The requests from companies and legal entities for provision of access to the register of registered PDCs became more frequent. CPDP has published in an open machine-readable format data from its public registers in the 'Open Data Portal of the Republic of Bulgaria', where the requested information is available.

Complaints and questions outside the competence of CPDP were also received in 2017. They were forwarded to the relevant competent government institutions.

Summary of complaints/alerts and questions received through the provided submission forms through the CPDP website by subject matter is presented in the table below:

Nature of the problem	**Number**
Complaints regarding the misuse of personal data by employers in companies and officials in government institutions	66
Complaints/alerts regarding the unlawful use of personal data in social media	52
Complaints and questions outside the competence of CPDP, which are forwarded to the relevant competent government institutions	47
Complaints and questions relating to the provision of personal data by mobile operators and fast-track lenders to the so-called collection companies	23
Complaints relating to the misuse of personal data in the lists submitted to the Central Electoral Commission (CEC) by initiative committees and parties in connection with the 2017 Parliamentary elections	8
Alerts from citizens related to the placing of video surveillance cameras in residential buildings without the consent of residents under the Condominium Management Act, as well as their improper directing beyond their intended purpose	10
Inquiries about the legality of 'Blizoo Media and Broadband' EAD requiring a personal identification number when users refuse to use digital TV	7

Inquiries by foreign individuals regarding the interpretation of the new EU Data Protection Regulation as well as questions relating to the Schengen visa	5
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	7
Children's competition 'What others know about me?'	4

V. Control and Administrative-penal Activity

1. Control Activity

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 established 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 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 alerts 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, prescription of 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.

In 2017, 1,146 inspections were initiated, of which:

- 1,016 ex-ante inspections;

- 73 ongoing inspections;

- 57 ex-post inspections.

The total number of inspections carried out in 2017 (Figure 8), including inspections initiated in 2016, was 938. Of these:

- 825 ex-ante inspections;

- 54 ongoing inspections;

- 59 ex-post inspections.

During the reporting period 200 requests were received. Of these, 177 were closed, including inspections initiated in 2016.

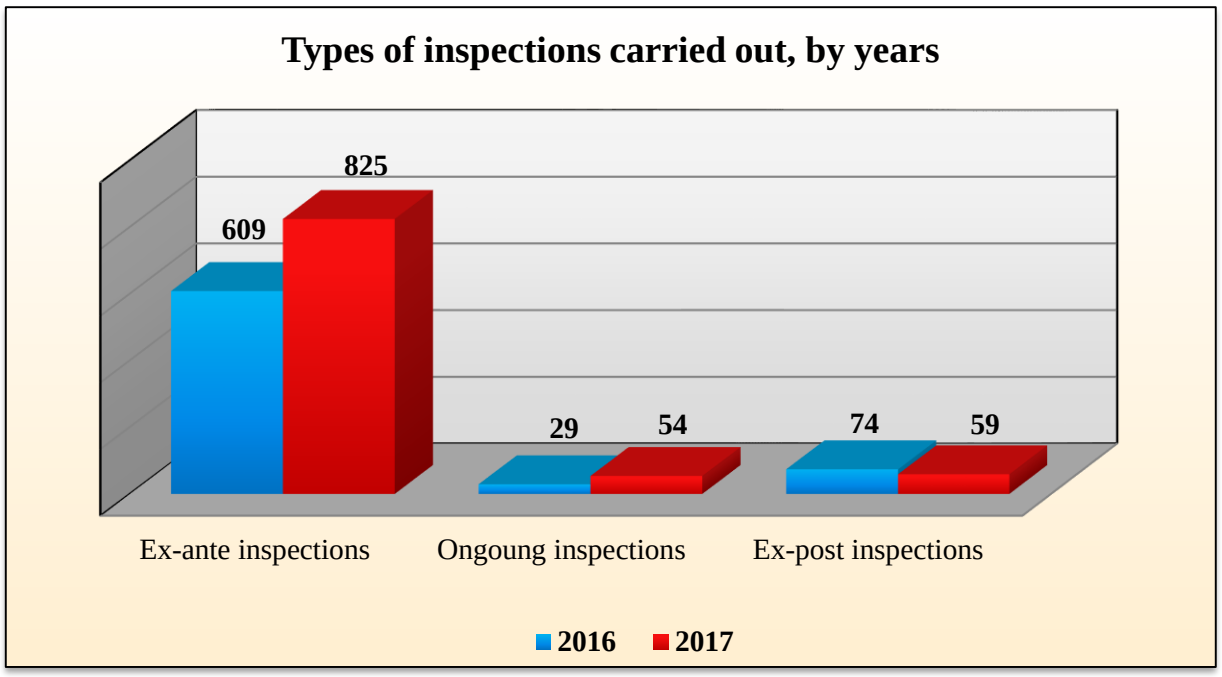

Figure 8

The control activity resulted in the drawing up of 938 statements of findings and the issuance of 17 compulsory instructions and 11 statements establishing administrative violations.

The comparative statistics show a considerable increase in all types of files, such as inspections, requests and alerts. The small difference between assigned and completed cases leads to the conclusion that cases are dealt with quickly and within the time-limits. The specific environments in which personal data is processed mean that there is a need to differentiate the inspections. In pursuance of its activities in 2017, CPDP carried out inspections in the following sectors and areas:

SECTOR/AREA	NUMBER
Healthcare	460
Education and training	190
Commerce and services	73
Video surveillance	42
Non-profit legal entities	27

Industry and trade	19
Hotels and restaurants	16
Financial and accounting services	14
Legal services	14
Information technology and services	13
Consulting activities	11
Central, regional and local authorities	10
Insurance	8
Real estates	6
Human resources	6
Transport	5
Social activities	4
Construction	4
Other	22

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 under 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.

In 2017, a total of 825 ex-ante inspections were carried out, including 21 inspections in which a refusal of registration was ruled in previous years.

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 include 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 is 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 results from the insufficient knowledge or lack of knowledge of the relevant legislation and personal data protection issues in their activities. These findings were fully confirmed by the inspections carried out in the Education and Healthcare sectors. In addition to the sectoral trainings that CPDP plans and conducts periodically during the year, in each specific case under a given preliminary inspection, the relevant employee to whom it is assigned provides the necessary assistance to bring the instruction in line with the PDP Act.

1.2. Ongoing Inspections

Although the number of ongoing inspections under Article 12(3) of the PDP Act is much lower than the preliminary 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 CPDP on the basis of the control plans adopted thereby for the corresponding year.

Fifty-four ongoing inspections were carried out during the reporting period (Figure 8). They resulted in the issuance of 7 statements establishing administrative violations (SEAV) and 7 compulsory instructions (CI).

Inspections were carried out in connection with the compliance with the provisions of the PDP Act regarding:

- existence of undertaken technical and organisational measures for protection of personal data in accordance with the PDP Act and Ordinance No 1 of 30 January 2013;
- unlawful processing of personal data of customers;
- copying of identity documents of individuals – customers of the corresponding companies;
- unregulated video surveillance by individuals and legal entities;
- unregulated use of databases of personal data of customers, received from third parties;
- sending unsolicited telephone messages to customers of the corresponding companies.

The ongoing inspection carried out in pursuance of a resolution of CPDP in 2017 in the field of personal data protection in the activity of PDCs in the sector of Healthcare (Sectoral inspection), including the administration of the Ministry of Health (MoH), was the inspection with the greatest factual and legal complexity and of significant public interest.

The sectoral inspection was the second of its kind in the activity of CPDP. With a CPDP resolution, Veselin Tselkov, Member of CPDP, was appointed as a leader, and Tsvetan Ivanchovski, Head of the Control of APP Department – as a coordinator.

For the purposes of the inspection, a total of 38,650 structural units acting in the capacity as PDCs within the meaning of the PDP Act were identified. They include both medical treatment facilities for hospital and outpatient care within the meaning of the Medical Treatment Facilities Act and administrative units or mixed regime units – the MoH administration, regional health inspectorates, other second-level spenders of budgetary appropriations to the Minister of Health, such as different agencies, commissions and national centres, etc. In compliance with the methodology, the sectoral inspection was completed with a summary report to CPDP.

At a regular meeting held on 13 December 2017 CPDP adopted the report and decided that a short version thereof shall be sent to the MoH for information and dissemination via appropriate channels to its structures. Pursuant to the CPDP decision, medical treatment

facilities and the respective administrative structures having the quality of PDCs shall take the following actions within 6 months of the date of receipt of the attached report:

- develop/update their instructions for protection of personal data;
- request/update registers, and mandatorily registers containing data on health;
- conduct training in connection with the new Regulation 2016/679 of the European Parliament and of the Council in order to train data protection officers, especially within the PDCs for which they will be mandatory – large hospitals, NHIF, RHIs, etc.;
- include a data protection clause in the codes of conduct of professional organisations.

Regarding the activities of teams carrying out sectoral inspections, together with the report on the inspection in the Healthcare sector CPDP endorsed several recommendations for good practices, mainly related to the practical implementation of the methodology for carrying out these inspections.

Other ongoing inspections of more significant public interest carried out for the first time in 2017 with such subject matter are the inspections are related to inquiries received in 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 January 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 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, Item 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.

During the period January – December 2017 CPDP received 14 such requests. In the course of their consideration and of the actions taken by CPDP, 7 responding letters were received in which persons requesting access to the databases declare that they withdraw their

requests. In the course of the 6 inspections carried out, existence of measures for 'high level of protection' was established in 4 PDCs, 1 PDC withdrew its request in the course of the inspection, and 1 PDC did not provide the required assistance. Currently 1 legal entity is being inspected and the measures for protection of personal data undertaken by it will be established.

1.3. Ex-post Inspections

The third type of inspections are those under Article 12(4) of the PDP Act, namely 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).

Fifty-seven ex-post inspections were carried out in 2017 (Figure 8). 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 basis on which they are carried out.

These inspections resulted in the issuance of 6 compulsory instructions.

The 35 follow-up inspections carried out following the decision of 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) RACPDPA, when a request does not contain details about violations of the applicant's right, action can be taken under Items 3, 5 and 6 of Article 10(1) and Article 43 of the PDP Act. In 2017, the Commission received 200 requests from individuals, including topical inquiries on personal data protection issues. Where necessary, inspections on the grounds of Paragraph (3) or (4) of Article 12 of the PDP Act are carried

out. As in 2016, most frequently alerts referred to the attention of CPDP unlawful actions relating to:

- processing of personal data of individuals without existing registration with CPDP;
- publishing of personal data in websites and possibility for unregulated access to such data;
- creating false profiles in websites;
- alerts against mobile operators;
- receiving unsolicited electronic communications;
- processing of personal data for direct marketing purposes without having requested the consent of the individual;
- requiring copies of identity documents at the time of conclusion of employment contracts;
- video surveillance carried out in condominiums or in public locations.

By the end of the reporting period, 177 requests were considered, 3 compulsory instructions were issued, 4 statements establishing administrative violations were prepared, and 7 requests were referred by competence to the Commission for Consumer Protection, the Ministry of Interior and the Sofia Regional Prosecutor's Office.

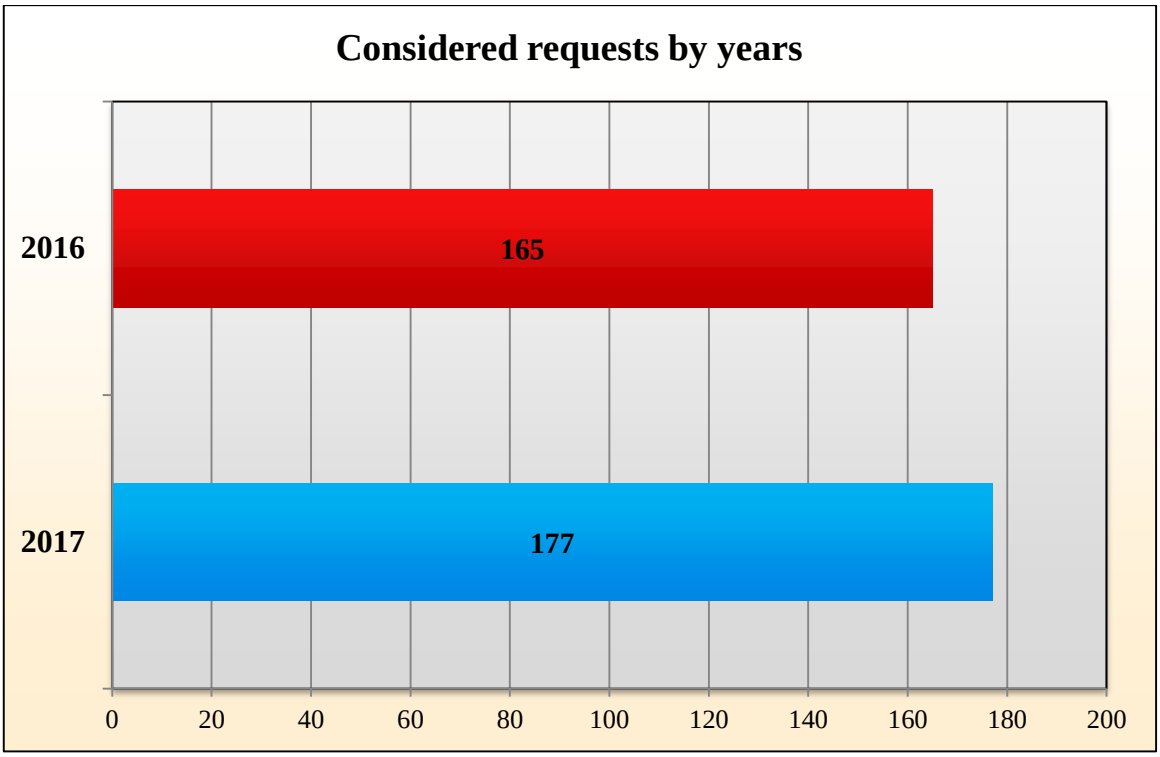

Figure 9

Comparative statistics from the previous year (Figure 8 and Figure 9) and the analysis of all types of inspections, including alerts and various inquiries, show a significant increase, both in absolute terms 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

2.1. Compulsory Instructions

On the grounds of Article 10(1)(5) of the PDP Act and in connection with the control activity under Article 12(1) of the PDP Act, 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 current and the previous reporting period.

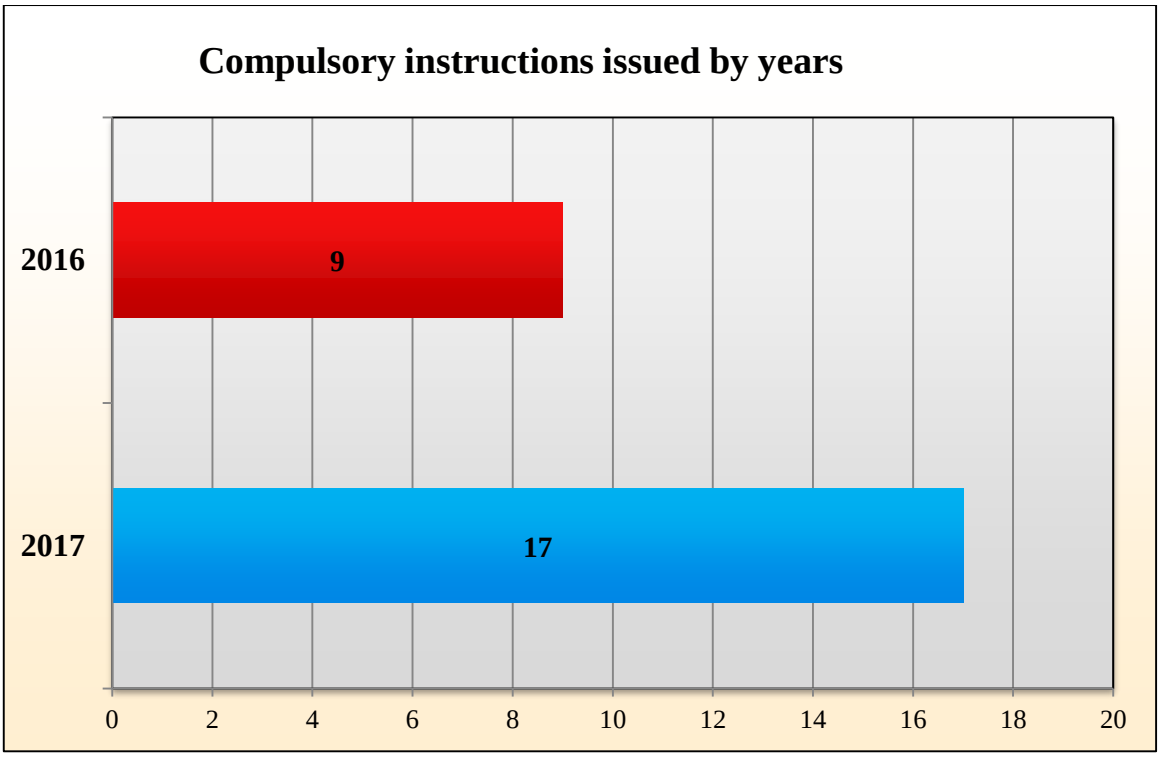

Figure 10

Nine of the 17 compulsory instructions issued in 2017 were complied with within the time-limits set by CPDP, and the other 8 CIs are under implementation. The compulsory instructions were issued in connection with:

- the processing of documents containing 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 updating of the Instructions on personal data protection measures under Article 23(4) of the PDP Act and in accordance with the provisions of the Ordinance.

-

2.2. Administrative-penal Proceedings

Article 43(4) of the PDP Act provides that the determination of the violations, the issuance, the appeal and the execution of the penal decrees (PDs) shall be carried out in compliance with the AVP Act.

Statements establishing administrative violations (SEAVs) of provisions of the PDP Act are issued by a CPDP member or by officials authorised by the Commission according to the requirements of Article 43(1) of the PDP Act, and penal decrees are issued by the Chairperson of the Commission in accordance with Article 43(2) of the PDP Act.

In connection with established violations of different provisions of the PDP Act, 11 SEAVs were issued in 2017. Based on these, the Chairperson of CPDP issued 16 PDs, 7 of which on the grounds of SEAVs from the end of 2016.

Similar to previous years, in 2017 the Commission continued to encounter major difficulties in delivering the issued SEAVs to addressees via municipal administrations in various parts of the country, in accordance with the provision of 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 CPDP, which is sometimes explained by objective reasons – lack of sufficient staff and large volumes of proceedings. In some cases, SEAVs are served to 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, CPDP seeks and receives assistance from the MoI authorities in the country. A frequent practice is statements and decrees to be served on the spot by the employees who prepared the corresponding statement or the draft of the PD.

The distribution of the PDs by type of the violation to be remedied is presented on the next chart (Figure 11).

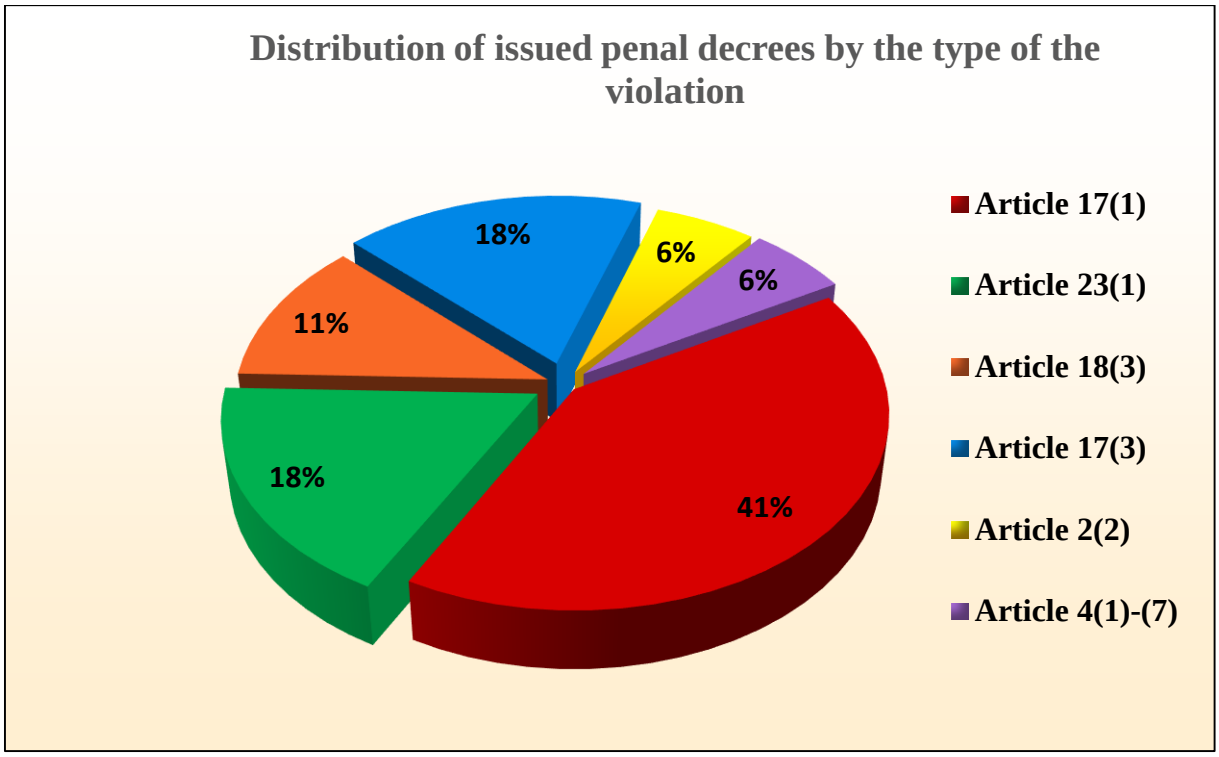

Figure 11

A natural continuation of the findings regarding the most frequent violations found in completed inspections is the failure of PDCs to submit applications for registration at CPDP before they begin any processing of personal data, as required by Article 17(1) of the PDP Act. For such violations, 7 PDs were issued. For failure of PDCs to fulfil their obligation under Article 18(3) of the PDP Act to notify CPDP of any alteration in the initially declared data, entered in the register under Article 10(1)(2) of the PDP Act, 3 PDs were issued. 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, 2 PDs were issued.

Next come the 3 PDs issued for non-compliance with the provision of Article 23(1) of the PDP Act regarding the obligation of PDCs to take appropriate technical and organisational measures to protect data against accidental or unlawful destruction, or against accidental loss, unauthorised access, alteration or dissemination, as well as against other unlawful forms of processing.

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 CPDP acting as a collective body.

In 2017, the penalties imposed amounted to BGN 34,500, the amounts collected totalled BGN 39,500 (including in relation to previous years), and BGN 2,500 of these were collected coercively by the National Revenue Agency (NRA).

Eighteen PDs are in a trial phase – 5 PDs issued during the year and 13 PDs issued in prior years. In 2017, 12 PDs with a total amount of imposed penalties of BGN 11,800 were paid without being contested, and most of the penalties imposed were in the minimum amount envisaged in the PDP Act or slightly above it.

The penal decrees issued for violations comprising unlawful processing of personal data of a large number of individuals and failure to take action for personal data protection in large commercial companies, which were confirmed by the court in 2017 and the pecuniary sanctions under which were paid, were of greater factual and legal complexity and of significant public interest. Examples include PDs against a telecommunication operator for a violation of Item 3 of Article 2(2) of the PDP Act in the amount of BGN 10,000 and against a bank for a violation of Items 1–4 of Article 4(1) of the PDP Act in the amount of BGN 10,000. The PD issued against a company conducting marketing activities with a total imposed penalty of BGN 17,000, returned for consideration by a different court panel, and against a sports association with a penalty of BGN 11,000 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. At present, enforcement proceedings have been instituted for enforced collection under 47 PDs, including from previous years.

In 2017, the outcomes of the court cases initiated on appeals against PDs issued in previous years were as follows: 3 PDs were rescinded in their entirety, and 10 PDs were confirmed. It shall be noted that 4 of the PDs confirmed with a final judgement of the appellate instance were rescinded by the court of first instance.

In the court cases initiated on appeals against PDs and appeals against CIs issued during the year, CPDP had procedural representation in 49 court hearings.

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

In the court proceedings continuing in 2017, 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, 2 PDs issued against political parties were confirmed, 1 PD is still in a trial phase, and under 5 PDs the NRA is collecting the receivables. Out of the total of 18 PDs issued at the end of 2016 and the beginning of 2017 against political entities that issued nominations for President and Vice President in the elections of 6 November 2016 and registered for participation in the information campaign of the national referendum held on 6 November 2016, 1 PD was finally rescinded, 9 PDs are in a trial phase, 5 of which were revoked at first instance. The main reason for rescinding of PDs is that the coalition of parties, respectively the initiative committee, which are entities under the Electoral Code, against which the PDs have been issued, are not legal entities and do not have legal personality. The Court points out that the interpretation of the provisions of the Political Parties Act and the Electoral Code implies that only the political parties and not the coalitions in which they are involved are PDCs, and therefore the administrative and penal liability shall be borne by the individual parties forming the coalition, and not the coalition itself.

Currently 1 PD against a coalition of parties and 8 PDs against initiative committees are in a trial phase.

The 1 PD issued against an initiative committee approved with a final judgement by the SCAC was sent to NRA – Smolyan for collection of the pecuniary sanction imposed. In a letter it is stated, that the NRA refuses to initiate enforcement proceedings in accordance with the procedure established by the TSIPC because the initiative committee has no BULSTAT identifier. The opinion requested and received from the NRA headquarters stated that the initiative committee is not a legal entity, has no legal personality and therefore against it no enforcement proceedings can be initiated regardless of the enforced court judgement. The proceedings were archived.

In line with the ordinary practice, all court judgements and their reasons, especially the court judgements 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 for establishment of 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 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 punishment 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 and strict compliance with the law of the prepared SEAVs 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 growth, and 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.

VI. Analysis of Complaints and CPDP Practices in Connection with the Elections for President and Vice President and the Referendum Held

In 2017 CPDP received a total of 181 complaints in connection with the processing of personal data in lists of individuals supporting the registration of parties, coalitions or initiative committees for participation in the information campaign of the national referendum held on 6 November 2016 and in lists of individuals supporting parties, coalitions or initiative committees for participation in the elections for President and Vice President of the Republic held on 6 November 2016. Of these, 76 complaints were in connection with the processing of personal data in lists of individuals supporting the registration of parties, coalitions or initiative committees for participation in the information campaign of the national referendum held on 6 November 2016, and 105 complaints were in connection with the processing of personal data in lists of individuals supporting parties, coalitions or initiative committees for participation in the elections for President and Vice President of the Republic held on 6 November 2016.

Within its powers and in order to clarify from a legal and factual perspective the allegations in the complaint, CEC was required to submit and submitted relevant evidence, in particular certified copies of the lists of voters supporting the relevant political entities for participation in the information campaign of the national referendum held in 2016, and for participation in the elections for President and Vice President of the Republic held on 6 November 2016.

On the grounds of Article 49, in conjunction with Article 39 of APC, and in order to clarify all facts and circumstances relevant to the administrative proceedings initiated on the complaint, CPDP allowed the performance of a graphological assessment. This was brought to the knowledge of the complainants, indicating the possibility of providing comparative specimens of their handwriting and signature, indicating the procedure for doing so. However, some of the complainants did not submit comparative material or submitted it after the deadlines, which also led to a delay in the completion of part of the proceedings.

The provided comparative material was sent to the Research Institute of Criminology and Forensics (RICF) with the MoI for the preparation of the graphological assessments mentioned above.

Several meetings were carried out for considering the complaints received – meetings regarding the admissibility of the complaints and for scheduling open hearings, and open hearings with the participation of the interested parties.

As a result of the proceedings conducted, CPDP issued 33 resolutions (this is the number of the defendants of the relevant complaints in accordance with the requirement of Article 32 of the APC), whereby the following violations were ascertained:

- processing of personal data in lists of individuals supporting the registration of parties, coalitions or initiative committees for participation in the information campaign of the national referendum held on 6 November 2016. Thirty-seven complaints were accepted as well founded, fines in a total amount of BGN 192,500 were imposed on 19 members of initiative committees, and a pecuniary sanction in the amount of BGN 10,000 was imposed on one coalition of political parties;

- processing of personal data in lists of individuals supporting the registration of parties, coalitions or initiative committees for participation in the elections for President and Vice President of the Republic held on 6 November 2016. Forty complaints were accepted as well founded, fines in a total amount of BGN 30,000 were imposed on 3 members of initiative committees, and pecuniary sanctions in the amount of BGN 77,800 were imposed on 7 political parties and coalition of political parties.

With regard to the participation of the initiative committees in the information campaign of the national referendum it should be pointed out that the provision of Article 16 of the Direct Participation of Citizens in Government and Local Self-Government Act (DPCGLSG Act) states that the Electoral Code shall apply to the conducting of an information and communication campaign, thus ensuring equal opportunities for presenting different opinions on the subject of the referendum. Furthermore, pursuant to the provision of § 2 of the Transitional and Final Provisions of the DPCGLSG Act, the relevant provisions of the Electoral Code shall apply to all matters relating to the holding of national and local referenda and not regulated by the Act.

The Electoral Code regulates the process of registration of initiative committees with the CEC, and Article 320 in conjunction with Article 153(1) of the Electoral Code states that a list of voters supporting the registration of the initiative committee shall be submitted to the CEC together with the documents specified in Items 2 and 3 of Article 318(1) of the Code. In turn, the list shall contain the name, Personal Identification Number and signature of each person supporting the relevant registration.

Article 320(3), second proposal of the Electoral Code introduces a legal fiction assimilating the member of the initiative committee to a PDC within the meaning of Article 3(2) of the PDP Act. Furthermore, the member of the initiative committee bears responsibility as a PDC.

With the provision of Article 320(2) of the Electoral Code the legislator has introduced an obligation that the signatures of the persons supporting the participation of independent candidates in elections shall be affixed in the presence of a member of the initiative committee, who confirms this fact by affixing his/her handwritten signature under the corresponding page of the list. Pursuant to Article 320(2) in conjunction with Article 153(1) of the Electoral Code in conjunction with Article 16 and § 2 of the Transitional and Final Provisions of the DPCGLSG Act, the same obligation is introduced regarding the participation of initiative committees in information campaigns of the national referendum.

In view of the above, the administrative and penal liability for the processing of personal data of the complainants contrary to the PDP Act without the existence of any condition of admissibility of the processing (Article 4(1) of the PDP Act) shall be borne by the persons in whose patrimony the legislator foresaw the obligation for affixing the voter's signature.

Article 4(1) of the PDP Act states exhaustively the grounds for admissibility of the processing of personal data. The legislator has decided that the processing of personal data of individuals shall be made conditional on at least one of these conditions, which is a prerequisite for the lawfulness of the processing. In this connection, and provided that the existence of none of the grounds listed in Items 1, 3, 4, 5, 6 and 7 of Article 4(1) of the PDP Act, nor of the prerequisites for the admissibility of the processing set forth in the provision of Article 4(2) is established, the only possible prerequisite for admissibility of the processing remains the one stipulated in Article 4(1)(2).

The explicit consent of the individual to whom the data relate is one of the conditions for admissibility of the processing of personal data (Article 4(1)(2) of the PDP Act), which corresponds to the purpose of the law. While the PDP Act obligates all PDCs to conform in the processing of personal data with the prerequisites for its admissibility, legally enshrined in Article 4 of the cited statutory instrument, for the political entities the Electoral Code additionally imperatively mandates that in the processing and provision of the personal data of voters under Article 133(3)(5) of the Electoral Code the political entity must comply with the requirements of the PDP Act.

The conclusions above stem from the amendments to the Electoral Code adopted in 2016 and relating to the liability for collecting of personal data.

VII. Proceedings for Delivering Opinions and Participation in Coordination Procedures of Legislation on Matters Relating to Personal Data Protection

In 2017 CPDP responded to 88 requests by issuing official opinions pursuant to Article 10(1)(4) of the PDP Act. For comparison, requests for opinions on which CPDP ruled during the previous three years were as follows: 79 requests in 2013; 80 requests in 2014; 92 requests in 2015; 125 requests in 2016.

1. Practice Relating to the Delivering of Opinions

During the reporting year, a trend was observed of diverse data controllers approaching CPDP with requests for opinions regarding some topical issued from public life. The analysis that can be made with regard to the subjects of such opinions and the PDCs that requested them is that the subject of personal data protection becomes more relevant in all areas of society. An increasing range of PDCs approach CPDP for delivering opinions outlining the accurate direction for processing of personal data. This trend is also required by the new rules introducing the General Data Protection Regulation.

At the beginning of 2017 CPDP delivered an important opinion relating to users of digital/cable TV. CPDP was approached with alerts from citizens that they have been forced to send SMS containing information regarding their Personal Identification Numbers if they wish to refuse to use services. In connection with this CPDP delivered the opinion that the requirement for sending an SMS containing information regarding the Personal Identification Number as a condition for valid refusal to use a service is excessive and contrary to the General Terms and Conditions for the Provision of 'Digital Television' and the General Terms and Conditions for the Transmission of Radio and Television Programmes via Cable Networks. This requirement is also contrary to the principles of lawfulness, proportionality and appropriateness in the processing of personal data, as well as to the legal requirement that personal data shall be relevant and not excessive to the purposes for which they are being processed, as introduced in Article 2 of the PDP Act. In order to protect the rights of a large number of individuals – users of the above-described service under the PDP Act, the PDCs shall immediately terminate the practice in question. In the event of failure to comply, CPDP

will undertake with respect to the PDCs the appropriate measures provided for in Article 38 of the PDP Act.

During the reporting period CPDP received a request of significant public interest. The request is related to the increase of the drying forests in the regions of Pernik and Kyustendil, specifying that a working meeting was held with the Regional Governors of the two regions, representatives of the Regional Directorates of Agriculture, the directors of the Regional Forest Directorate – Kyustendil, of the Southwestern State Enterprise – Blagoevgrad, and of the state forestry and hunting farms in both areas.

In order to limit the spread of the woodworm beetle which is the cause of the drying of white pine coniferous trees, it is necessary to perform sanitary felling in the affected areas. In the state-owned forest territories, priority is given to the absorption of the damaged timber, but in the private forests there is a serious lag, as the felling should be done by their owners. In connection with this Territorial Unit 'Vitosha–Studena State Hunting Farm' requested from the 'Civil Registration' Department of the Municipality of Pernik to be provided with updated information about the owners and heirs of the properties according to the list attached to the letter.

The CPDP opinion in connection with the issues raised is that for the purpose of preventing the spread of the woodworm beetle which is the cause of the drying of white pine coniferous trees, and in connection with the performing of sanitary felling in the affected areas, on the grounds of Article 4(1)(5) of the PDP Act in conjunction with Article 106(1)(2) of the Civil Registration Act, the Municipality of Pernik can provide Territorial Unit 'Vitosha–Studena State Hunting Farm' with the personal data contained in the local database 'Population' (names and addresses) for the purpose of contacting the owners of private forests or the heirs of deceased owners of private forests. For the lawful and bona fide processing of the personal data, Territorial Unit 'Vitosha–Studena State Hunting Farm' shall not process the accessed personal data for other purposes. Territorial Unit 'Vitosha–Studena State Hunting Farm' shall provide the individuals whose personal data it will process with information in connection with its obligations under Article 20(1) of the PDP Act, as follows: data which identify the controller and its representative; the purposes for which the data are being processed; the categories of personal data relating to the respective individual; the recipients or categories of recipients to whom the personal data may be disclosed; information about the right of access to and the right to rectify the data collected.

In 2017 CPDP received another interesting request for opinion of significant public interest from the Head of the Department of Medical Genetics at the Medical University of Sofia and National Medical Genetics Consultant of the Ministry of Health, in the capacity of project leader of a scientific project funded by the Scientific Research Fund of the Ministry of Education and Science with the subject 'Characterisation of Longevity Genes by Genomic and Targeted Sequencing'. The project objective is to collect samples of buccal mucosa from the largest possible number of Bulgarian centenarians and to perform a thorough genetic analysis by genomic sequencing. The summary of the project states that the results of the study will be of great importance to the scientific community and to healthcare not only at national but also at European level. In its request the scientific team requests authorisation to be provided with data about the first name and address of living persons who have reached the age of 100 at the relevant date, in accordance with the PDP Act. After assessing the significance of the research, with its opinion CPDP allowed the provision of the requested data for the purposes of the project, while making recommendations on the conditions for the lawful processing of personal data as well as providing guidance on specific technical and organisational measures for protection.

In connection with a series of questions sent by financial sector companies, in 2017 CPDP expressed its understanding on the application of specific provisions of Regulation 2016/679 (the General Data Protection Regulation). In connection with this, the following conclusions were made.

The conditions for the emergence of the figure of the joint PDCs are exhaustively set out in Article 26 of the General Data Protection Regulation. However, the assessment of whether it is applicable to the particular case should be carried out by carefully reviewing the purposes and means of processing personal data.

The specificity, as a characteristic feature of the consent, excludes the expression of a general consent to the processing of personal data given in general and without specific parameters and limitations for any processing performed by a particular PDC or joint PDCs. The processing must always be in line with the 'need to know' principle and therefore there must be an appropriate common goal for joint controlling. For example, for general marketing

purposes there is no obstacle to a specific consent for the processing of personal data to be given to more than one PDC.

The minimum necessary content is determined by the specific PDCs and reflects their will for allocating all obligations and responsibilities set out in the General Data Protection Regulation. In the cases of joint controllers, the statement enclosed with the request is not contrary to the PDP Act.

As clarified above, general consent cannot exist. The consent shall be given for specific purposes. However, there is no obstacle to the executing as a single document of the separate consents expressed for a specific processing by a particular PDC for a specific purpose, provided that all conditions for the validity of the consent are met. It should not be forgotten that consent can be withdrawn only in relation to a particular type of processing for a particular purpose by a particular PDC. The clearer the form of giving consent is, the easier it is for the data subject to withdraw the consent to a specific processing. This approach is fully consistent with the principle of self-accountability introduced by the General Regulation.

The consent shall be specific. It cannot cover future presumed purposes or means of data processing.

A lawful transmission of data among the different companies exists if all legally required characteristics of consent are satisfied.

When developing the General Data Protection Regulation, the legislator sought technological neutrality of the legal instrument. This approach means a complete freedom as regards the means of processing of personal data, provided that the processing complies fully with the requirements of the Regulation. The technical and technological neutrality allow PDCs to make decisions and change them, but PDCs shall always fulfil the obligation under Article 24, paragraph 1 of the Regulation: ‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.’

Given that the consent cannot be general, the will of the individual PDCs shall be expressed in an agreement/arrangement or other instrument between them.

If the consent is given for specific purposes and to specific PDCs, it can be withdrawn in the manner in which it was given.

The joint PDCs shall be jointly liable with regard to the data subjects. For the purpose of clarity and transparency, the allocation of responsibilities shall be agreed in the relevant mandatory arrangement between the joint PDCs, if the prerequisites for the existence of such a figure exist.

For the sake of precision with regard to the preparation for the implementation of the new General Data Protection Regulation, the views of sole proprietors of capital should be sought, and the intentions of the financial group management as a whole for a common approach to the processing of personal data shall be explored.

The opinion delivered during the reporting period is preliminary, as the measures implementing Regulation No 2016/679 have not yet been adopted in national legislation. It should be borne in mind that the Regulation in question, despite its direct application, contains provisions which refer to the national legislation.

During the reporting period CPDP also delivered an opinion in connection with a request by the Manager of the National Health Insurance Fund (NHIF). The request states that, by a ruling of a five-member panel of the SAC, the collective complaint of several associations of patients founded as non-profit legal entities was granted and the provision of Article 2(5) of the Ordinance on Exercising the Right of Access to Medical Care, according to which: 'Each health insured person shall be issued with a unique identification number under Article 63(1)(1) of the Health Insurance Act through electronic identification. When receiving medical care, the person shall be authenticated by this number, confirming the received medical care.' was repealed. The ruling is final.

In connection with this, a request is made to CPDP to deliver an opinion as to whether the information collected in the Registration System for Health Insurance Events with Medical Care Providers via Biometric Identifiers of Patients shall be destroyed, and in accordance with what procedure. It is also added, that pursuant to Article 67 of the Health Insurance Act '[t]he particulars regarding the insured persons shall be preserved at the NHIF for a period of 5 years after termination of their health insurance, and the particulars regarding the providers shall be preserved for a period of 5 years after the termination of the relevant contract with the NHIF'. The question is asked if the data gathered as a result of the application of the Registration System for Health Insurance Events with Medical Care Providers via Biometric Identifiers of Patients shall be stored according to this procedure.

The CPDP opinion on this case is that the ruling of the SAC declaring null and void the provision of Article 2(5) of the Ordinance on Exercising the Right of Access to Medical Care results in abolishing the grounds for processing a Unique Identification Numbered (UIN) for patients in hospitals. Although the UIN generated in the Registration System for Health Insurance Events with Medical Care Providers via Biometric Identifiers of Patients does not constitute personal data within the meaning of the PDP Act, in the case at issue, in view of the broad public interest, the provisions of the law concerning the obligations of PDCs with respect to the data processed thereby can be applied by analogy.

After the entry into force of the ruling of the five-member panel of the SAC, the personal data controller – NHIF could apply by analogy Article 25(1), first proposal of the PDP Act – prior to the discontinuing of the processing, destroy the data collected in the registration system and notify CPDP. The law provides for freedom of choice as to the specific technological solution to carry out the destruction in question. In the specific case, the 5-year period for storage of data, provided for in Article 67 of the Health Insurance Act, is not applicable, as the health insurance of the persons subject to mandatory health insurance is not terminated.

An interesting opinion CPDP delivered in 2017 is about the interpretation of the legal framework relating to the provision of ESGRAON data to attorneys, lawyers and parents of adults.

The CPDP position on the case is that the birth certificate is an official written document which certifies the event of birth and the parents from whom the person originates. In connection with this, it contains the personal data (name, Personal Identification Number, place of birth) of the individual to which it relates, but also personal data of the mother and father. Account should also be taken of the relationship between children and parents, which is of a specific confidential nature. In this connection parents shall not qualify as third parties within the meaning of Article 88a(2) of the Civil Registration Act.

A lawyer without representative authority and without proper certificate of such authority shall not have access to material relating to third parties, in particular the personal data contained therein. If, in a particular hypothetical case, the provision of information is

subject to special rules for its provision, in particular a statutory requirement for a notarised explicit power of attorney, they derogate the general rule prescribed in Article 31(1) of the Bar Act.

In 2017 CPDP also ruled on a request for provision of personal data, contained in medical records, and in particular on the lawful performance of the obligation of a PDC – medical treatment facility in connection with the provisions of Article 28b of the Health Act, pursuant to which the patient is entitled to receive from the medical treatment facility information relating to his/her health condition, including copies of his/her medical documents. CPDP was requested to deliver an opinion on the following several questions.

In the case of an explicit request from the patient, is it permissible to send the copies of the medical documents to an address specified by the patient?

Shall the power of attorney under Article 28b(2) of the Health Act contain a certification of the signature by a notary public? Pursuant to Article 28b(2) of the Health Act, the patient has the right to authorise in writing another individual to become familiar with his/her medical documents and to make copies thereof.

Does the authorised person have the right to request that copies of the medical records be sent to a specified address?

Shall the right of access to the personal data of a deceased person be exercised jointly by all heirs referred to in Article 28b(3) of the Health Act, or is it permissible to be exercised only by one/some of them? Pursuant to Article 28(3) of the Health Act, in case of a patient's death, his/her heirs and lineal or collateral relatives up to four times removed from them inclusive shall be entitled to review the health information on the deceased, as well as to make copies of the medical records of the latter.

CPDP delivered an opinion as follows.

In the event that the patient or a person expressly authorised thereby requests that the medical records be delivered by mail to an address specified thereby, the PDC (the medical treatment facility) shall comply with the request.

The provision of Article 28b(2) does not require notarial form of authorisation by the patient of another person so that the latter person can see the medical records of the patient and make copies thereof, therefore the medical treatment facility does not have legal grounds to require a certification of the signature by a notary public.

In case of a patient's death, his/her heirs and lineal or collateral relatives up to four times removed from them inclusive are entitled to review the health information on the deceased, as well as to make copies of the medical records of the latter. Each of the heirs has the right to exercise the rights he/she has as an heir alone, including the rights provided thereto under Article 28(3) of the PDP Act, and also under Article 28b(3) of the Health Act, without the need for 'complicity' of the other heirs by law or by will or for prior consent from them.

In 2017 CPDP delivered an opinion in connection with a request from the 'Financial Investigation' Specialised Administrative Directorate at the State Agency for National Security. The request is related to the forthcoming implementation in the Bulgarian legislation of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Directive 2015/849). The request for opinion relates to questions arising in connection with the establishment of a central public register provided for in the Directive in which data shall be entered on natural persons who are the beneficial owners of legal persons and other legal entities in order to prevent the use of the financial system for the purposes of money laundering and terrorist financing – activities that have an extremely negative impact on society and the functioning of the financial system at both national and European level, and international level as a whole.

Pursuant to the requirements of the Directive, the personal data, which persons or organisations that can prove a legitimate interest shall access, shall include at least the name, the month and year of birth, the nationality and the country of residence of the natural person who is the beneficial owner of a legal person or another legal entity.

Where necessary, the information contained in the register shall be able to be the subject of international exchange of information between competent authorities and financial intelligence units of different countries for the purposes of preventing money laundering and terrorist financing.

The Directive explicitly requires Member States to ensure access to information regarding beneficial owners in accordance with data protection rules.

In view of the analysis of the extant legislation, CPDP is of the opinion that:

The law whereby Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC will be transposed shall contain an explicit provision on the supervisory function of CPDP with regard to the processing of personal data under Directive 2015/849.

The law whereby Directive (EU) 2015/849 will be transposed shall include an obligation for the Registry Agency, as a PDC keeping the register of beneficial owners, to ensure that beneficial owners are notified that a certain amount of their personal data is being processed for the purposes of the Directive and can therefore be provided to a certain number of persons.

The law whereby Directive (EU) 2015/849 will be transposed shall contain time periods for storage and rules relating to the destruction of the personal data accessed for the purposes of and processed under the Directive.

CPDP made important conclusions in connection with the information regarding the natural persons registered in the register of beneficial owners. This information shall be accessible to the competent authorities and financial intelligence units without any restrictions; shall be accessible to the obliged entities, within the framework of customer due diligence in accordance with Chapter II of Directive (EC) 2015/849 without restriction within and for the purposes of such due diligence; and shall be accessible to all persons or organisations that can prove legitimate interest, in a volume comprising only: the name; the month and year of birth; the nationality; the country of residence of the beneficial owner; the nature and extent of the beneficial interest held.

In connection with the annual publication of information by the National Audit Office, an opinion was expressed that under the extant law there are no legal grounds for public and publicly available disclosure of information about the Personal Identification Number or the date of birth of the persons liable to the NAO.

CPDP specified that the opinion shall be updated after the Directive amending Directive 2015/849 is finally adopted.

Another interesting opinion delivered by CPDP during the reporting period was in connection with a request made to the Appellate Specialised Criminal Court (ASCC) by an individual regarding the coinciding of his first and last name with those of a defendant in a case considered by the Specialised Criminal Court (SCC) and the ASCC. The coincidence was established in publications on scheduled hearings and considered cases on the official website of the court. On this request CPDP delivered the opinion that the provision of information in the form of press releases regarding scheduled hearings and considered cases under Article 64 and Article 65 of the Criminal Procedure Code, which ASCC publishes on its own website or sends to the mass media, shall be carried out in compliance with the PDP Act, applying by analogy Article 64 of the Judicial System Act. In cases where the published information on individuals cannot be presented in an anonymous form and the court is expressly informed by the person concerned that there is an infringement of his or her right to protection of personal data and privacy due to coinciding names, the court can indicate additional data, such as initials of the father's name, year of birth, respectively age, etc. to prevent misidentification of the person.

During the reporting period requests for opinions regarding the provision of personal data by ESGRAON were received. Diplomatic missions of EU Member States, through the Ministry of Foreign Affairs (MoFA), sent requests for information regarding permanent and current addresses of Bulgarian citizens in the Republic of Bulgaria. The requests are related to different obligations of the Bulgarian citizens in European countries.

In connection with the above, CPDP expressed the position that information about permanent and/or current addresses of Bulgarian citizens can be provided to foreign official missions in connection with verbal notes sent to the Ministry of Foreign Affairs on the grounds of Article 4(1)(7) of the PDP Act and Article 106(2) of the CReg Act. The requested information regarding a permanent and/or current address shall be provided through the MoFA after having informed the individuals in accordance with Article 20 of the PDP Act.

An interesting opinion delivered by CPDP in 2017 was at the request of a municipal commercial company in connection with the collection of personal data for the purposes of a game organised by the municipal company.

The request for an opinion states that the company has the idea to launch a game with citizens – users of public transport. The game will be open to all citizens who have purchased a ticket for one-way travel with ground transportation (ticket) with a price of BGN 1.60. In order to participate in the game, citizens will have to write their names and phone numbers on the back of the ticket and put it in specially designated boxes placed next to the sales points of the company in Sofia. Each participant will be able to join the game with an unlimited number of tickets. The company asks a question regarding the lawfulness of the planned collecting of data (name and phone number) for the purposes of the game.

The CPDP opinion on the case is that the municipal company as a PDC can process the data provided voluntarily by citizens – name and phone number – for the purposes of the game on the grounds of Article 4(1)(2) of the PDP Act while complying with the principles of processing stipulated in Article 2(2) of the Act. At the same time the PDC shall fulfil its obligation to inform the persons in accordance with Article 19 of the PDP Act, to take the necessary technical and organisational measures for data protection under Article 23 of the PDP Act, and to destroy the data within the meaning of Article 25 of the PDP Act after the purpose of processing has been achieved.

CPDP has always been particularly careful when deciding on issues relating to the processing of personal data of children. CPDP has a steady practice in supporting and protecting the interests of children relating to their personal data and privacy. As this is a highly vulnerable group, apart from expressing opinions, by conducting information campaigns and thematic competitions CPDP aims to inform children about the importance of their personal data and the ways in which they could avoid violation of their privacy.

During the reporting period CPDP ruled on a request for an opinion from a non-profit association concerning the granting of permission by the Social Assistance Agency to its regional and territorial structures to provide personal data of children placed in foster families

for the purpose of entering them in a Register of children placed in foster families – members of the association, kept by the non-governmental organisation.

The CPDP opinion is that there are no legal grounds for the provision of the requested personal data of children placed in foster families by the Social Assistance Agency to the non-profit organisation.

Another opinion of CPDP in 2017, related to the lawful processing of personal data of children, was in connection with a request for an opinion from the State Agency for Child Protection (SACP) in connection with an initiative of the Children's Council. The request states that in 2003 a Children's Council was established with SACP. This is an advisory body with members – one representative of the children from each administrative region, as well as representatives of the vulnerable groups. The total number of members is thirty-three, aged from 13 to 18 years. The Children's Council decided to prepare and distribute a petition regarding the right of children to work. The inquiry contains information, that the three names and the Personal Identification Numbers of the children who sign the petition will be requested. SACP requested CPDP to deliver an opinion on whether it is admissible for children to collect Personal Identification Numbers of other children.

CPDP is of the opinion that the legal capacity of the persons is the condition, which must exist in order for them to incur obligations arising from the PDP Act. Therefore persons without legal capacity cannot process personal data.

In view of the target group of the petition, in order for the collecting of personal data for the needs of the petition prepared by the Children's Council, which is a type of processing of personal data, to be lawful, the explicit informed consent of the legal representatives of the children shall be given in accordance with the provision of Article 4(1)(2) of the PDP Act.

Data shall be collected in accordance with the principles of relevance and proportionality – data shall be collected only for specific, precisely defined and legal purposes in the following volume: three names and school name. In the cases of possible publishing, the PDC shall undertake the necessary technical and organisational measures for protection.

Because of its status, the Children's Council could not perform the actions above on its own, but only through the personal data controller – SACP.

In 2017 CPDP delivered an opinion on questions relating to the disseminating of the results from different types of examinations and the volume of information to be published. In order for the public disclosure, which is a type of processing of personal data, to be lawful, the explicit informed consent of the legal representatives of the pupils shall be given in accordance with the provision of Article 4(1)(2) of the PDP Act.

With regard to publication, it must be done in accordance with the principles of relevance and proportionality – data shall be collected only for specific, precisely defined and legal purposes. Different approaches can be adopted, such as individual access to lists with grades or their publication on the school's website with access with an individual code and a password.

In connection with the opinion above, and in particular the non-observance and non-implementation of the recommendations expressed therein, more than 150 inquiries which raise questions related to the above were received in the CPDP.

As a result, in 2017 the CPDP issued an opinion which developed further the first opinion, namely: the contents of the lists allocating the children in the rooms of the building is a technical form of preparation for the competition/academic competition. There is no obstacle to placing such lists in the building of the educational institution. On the other hand, the lists of results from the corresponding competitions/academic competitions contain information regarding the demonstrated knowledge and level of preparation. In combination with the full name, this unambiguously identifies the specific individuals and comprises processing of personal data.

The existence of a declaration for public disclosure fully complies with the rules regarding the lawful processing of personal data.

It is lawful and acceptable to include public disclosure of the result in the rules for conducting of competitions and academic competitions. In the absence of a desire to disclose the three names, the regulation can stipulate that the person shall be identified using a number.

During the reporting period, CPDP issued a decision on a request for an opinion from one of the mobile operators regarding the admissibility of the implementation of a software product through which personal data are taken from identity documents.

The request for an opinion was in connection with a compulsory instruction issued on the grounds of Article 10(1)(5) of the PDP Act and in pursuance of a decision whereby CPDP explicitly instructed undertakings providing public electronic communication services: 'to discontinue the taking of a copy of identity documents of natural persons upon the conclusion of a contract for public electronic communication services, through which the purposes for the processing of personal data are exceeded (Article 2(2)(3) of the PDP Act), and to delete from the annexes to the contracts (an integral part thereof) the requirement for taking a copy of the identity document'. In connection with this, and given the desire of the mobile operator to ensure the speed of its employees in providing services to the users, while avoiding mistakes in capturing information from identity documents, the company reports that it intends to purchase a software product that, through a reader, collects from the Bulgarian identity documents of individuals only the personal data necessary for the conclusion of a contract, an annex or another document between the parties and/or for the provision of an electronic communication service, namely the data under Article 228(1)(1) of the Electronic Communications Act (EC Act). It is intended to retrieve the data through an OCR solution. OCR (Optical Character Recognition) is a technology for converting printed text in a text file. This method is different from the scanning, where the scanned document is saved as an image file, while in optical character recognition the information read is stored as a text file. Only the data retrieved and specified above are stored, and the technology does not allow scanning, copying or another visual reproducing of the document.

The CPDP opinion on this case is that the processing via technical means of personal data of users of the mobile operator in the volume specified in Article 248(2)(2)(a) of the EC Act (three names, Personal Identification Number and address) is admissible, provided that the technology used complies with the security requirements under Article 23 of the PDP Act and does not result in violation of the personal data protection principles under Article 2(2) of the PDP Act.

The processing by the company of the number of the identity document for the purposes of provision of an electronic communication service is contrary to the imperative requirement of the first sentence of Article 249(1) of the EC Act.

The company providing public electronic communication networks and services can use the publicly available electronic service 'Information about the validity of Bulgarian identity documents' offered by the MoI when concluding contracts with subscribers – individuals, but only provided that the technology used ensures that the number of the identity document will be used only for automatic verification in the MoI database and will not be recorded, stored or processed in any other manner for other purposes.

When introducing new technologies for processing of personal data the PDC shall take the necessary measures for providing the data subjects with clear and accurate information under Article 19 of the PDP Act, and this information shall be in a simplified and understandable form and in the most accessible form possible.

The PDC – the company providing public electronic communication networks and services shall comply with the general regime on the time limits for the storage of personal data and such data shall be kept in a form that permits identification of the individuals concerned for a period not longer than is necessary for the purposes for which such data are processed (cf. Article 2(2)(6) of the PDP Act). The legislator has provided that the time period for storage of personal data shall be proportionate and adequate to the objectives of their processing.

In 2017 the trend for CPDP to be approached with requests from operating companies for the provision of personal data of debtors contained in the NDB 'Population' continued.

The opinion of CPDP on the case is as follows.

Mayors of municipalities in their capacity as civil status officials can provide operating companies with the permanent and current address of individuals – subscribers of the companies on the grounds of Article 4(1)(7) of the PDP Act after the relevant evidence is presented that such individuals are parties to a contract for the provision of services.

Under the same conditions, upon a possible death of an individual – subscriber of the company, the mayor can provide the operating company with official information regarding this circumstance.

Mayors in their capacity as civil status officials cannot provide operating companies

with certificates of inheritance without a court certificate. The assertion that the heirs by law, listed in the certificate of inheritance of a particular individual – party to an agreement for the provision of a service, are debtors of the operating company is a fact which must be proved and the burden of proof is on the person making this assertion.

During the reporting period the trend of requests to CPDP for opinions regarding the provision of certificates of inheritance in the event of death of borrowers continued**.** In connection with the above and on the grounds of Article 10(1)(4) of the PDP Act in conjunction with Article 106(1)(3), CPDP has a steady practice according to which mayors of municipalities in their capacity as civil status officials cannot provide the bank with certificates of inheritance without a court certificate. As specified above, the assertion that the heirs by law, listed in the certificate of inheritance of a particular individual – party to a consumer loan agreement, are debtors of the company is a fact which must be proved and the burden of proof is on the person making this assertion.

In view of the increased frequency of requests for permission to provide certificates of inheritance of deceased clients, CPDP published on its website a summary of its practice with regard to decisions to refuse such provision. For the sake of clarity, this information is provided in the form of questions and answers and is published in the 'Get informed' section, 'Topical Issues of Public Interest' sub-section. References are also made to judgements of the Supreme Administrative Court confirming the CPDP practice regarding the refusals to the provision of certificates of inheritance of deceased debtors requested by banks/operating companies on the grounds of Article 106(1) of the Civil Registration Act.

One of the main problems raised before CPDP in 2017 was the provision of access to personal data to different banks and non-banking financial institutions which wish to use information from the Population Register – National Database 'Population'. In connection with this, CPDP issued a decision authorising the access to NDB 'Population' in accordance with its mandates. Later in 2017, requests for extension of the purposes of the access to Population Register – National Database 'Population' (NDB 'Population') were received from different banking institutions. The CPDP position is as follows.

The authorisation under Article 103(1)(3) of the CReg Act, given with a previous decision of CPDP, also covers the checks on creditworthiness in the Population Register – National Database 'Population' performed by banks pursuant to the Consumer Credit for Real Estate Act, as well as other statutory instruments, concerning the actions related to the creditworthiness check of customers of banks and non-banking financial institutions.

During the reporting period CPDP ruled again on a case relating to a request made to an investment firm by an official of a police department in the United Kingdom for the disclosure of personal data of a customer of the investment firm**.** In his request the police official requests that data regarding the transaction be provided. In line with its steady practice in this respect, CPDP delivered the opinion that there are no legal grounds for a Bulgarian legal entity – PDC to provide data regarding an individual who is its customer directly to a police department of another European Union Member State. The lawful exchange of information containing personal data for the purposes of preventing, detecting and investigating crimes shall be only among the competent authorities of the respective states. In the specific case, these are the MoI authorities, respectively the judicial system.

2. Coordinating Draft Legislation

In 2017 CPDP received a letter from the Ministry of Finance in connection with a coordination procedure under Article 32(1) of the Structural Regulations of the Council of Ministers and its Administration regarding the draft Act to Amend and Supplement the Tax and Social Insurance Procedure Code.

The main objective of the draft amendment is to introduce the requirements of:

Council Directive (EU) 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation;

Council Directive (EU) 2016/881 of 25 May 2016 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation;

Council Directive (EU) 2015/2060 of 10 November 2015 repealing Directive 2003/48/EC on taxation of savings income in the form of interest payments.

Following an analysis of the draft law, CPDP established that the listed legal instruments subject to transposition respect the main rules and comply with the principles recognised in particular in the Charter of Fundamental Rights of the European Union. Both pursuant to the extant PDP Act and pursuant to the General Data Protection Regulation (Regulation 2016/679), the implementation of which starts on 25 May 2018, the exchange of personal data with a European Union Member State and with another Contracting Party to the European Economic Area Agreement shall be carried out freely if a legal ground exists. Since in the specific case the exchange of personal data is concerned, there is a statutory ground for this in the law of the Member States regulating the powers of the national competent authorities which are bound by the mandatory exchange of information in the field of taxation.

In 2017 CPDP coordinated without comments the draft AASSANS Act prepared by the interdepartmental working group, whereby the provisions of 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 shall be introduced. CPDP experts participated in the work of the interdepartmental working group for the transposing of the Directive and bringing the extant provisions of the SANS Act in line with the new requirements of the European legislation.

During the reporting period CPDP received a letter from the Supreme Judicial Council (SJC) in connection with a draft Ordinance on the Keeping, Storing of and Access to the Register of Instruments Issued by Courts. The SJC letter specifies that in connection with the adopted Act to Amend and Supplement the Judiciary Act, and in particular in the provisions on the SJC in Section III of Chapter Eighteen ‘a’, as well as in the provisions concerning the issuance of instruments and the execution in an electronic form of all other procedural actions provided for in law, new obligations for the bodies of the judiciary have been introduced. Following the latest legislative amendments, the courts shall declare the instruments issued thereby in a single register immediately after their issuance and after exercising due care in compliance with the rules set by the ordinance, the requirements of the PDP Act and

the Protection of Classified Information Act. Court instruments for the administration of justice and instruments that end or hinder the further development of the proceedings before the relevant instance or are subject to an independent appeal shall be announced in the register of court instruments. Instruments that disclose a secret protected by law and the motives thereto, and other instruments determined by the SJC Plenum, are not subject to registration in the register. In connection with the obligations of the courts, the provision of Article 360s of the Judiciary Act provides that the SJC Plenum and the Minister of Justice shall adopt an Ordinance on the Keeping, Storing of and Access to the Register of Instruments Issued by Courts. In connection with this, a working group was established with the task to prepare a draft ordinance. The SJC letter states that, based on a decision of the working group drafting the ordinance, it was decided to request an opinion from CPDP on the texts of the ordinance published for public consultations.

In connection with the proposed draft ordinance, CPDP makes a critical assessment regarding the text of the provision of Article 14(5) of the draft, according to which the personal data described in Paragraphs 1–4 must be published where they were of substantial procedural or substantive importance for the outcome of the particular case and their deletion would lead to rendering meaningless of the content of the judicial instrument or would change the meaning of the instrument. In practice, worded like this, the text of Article 14(5) of the draft allows the publication of unanonimised judicial instruments which have not entered into force based on vague criteria, in particular the criterion of 'substantial procedural or substantive importance for the outcome of the particular case'. The review of the case-law shows that at present there is contradictory case-law in the process of law enforcement, interpretation and reference to facts and circumstances of substantial procedural or substantive importance for the outcome of the particular case. In the opinion of CPDP, the result would be announcing of many judicial instruments which have not entered into force without deletion of personal data, which in turn could lead to serious breach of privacy and irreparable injury to persons whose data have been made publicly available. The delivery of the judicial instrument implies the indisputable fact that, in order to rule on the particular case, the relevant court has had in its possession all the necessary information and evidence on the case under consideration without any deletions. This information is also available to both the parties and the other participants in the trial who/which, in accordance with the appropriate procedure, have the right to obtain copies of the judicial instrument in its entirety, without

anonymised personal data. In this sense, it cannot be concluded that the publication of certain judicial instruments in the electronic register of court instruments with deletion of personal data may lead to the meaning of the judicial instrument being rendered meaningless or to changing the meaning of such instrument. The persons who/which enjoy res judicata are aware of the reasons and circumstances under which the instrument was delivered. Therefore the publication of judicial instruments with deleted personal data without the possibility of having a subjective 'specific discretion' regarding the deletion of the personal data contained therein is in line with the principle of publicity of the trial and enabling the public to draw up its own assessment of the trends in litigation, without the need to identify specific persons and data relating to such persons in the texts of the published instruments.

Furthermore, the adoption of such texts will in practice significantly limit the right to protection of personal data of individuals due to the fact that the publication of judicial instruments without deleting personal data will be done based on subjective criteria and at the same time will rest on formal statutory grounds.

VIII. Provision of Personal Data to Third Countries

In 2017 CPDP delivered opinions on a total of 24 requests and notifications for the provision of personal data to third countries, as follows: **13** notification on the grounds of standard contractual clauses, **4** requests for authorisations based on compulsory company rules and **2** requests on the grounds of agreements between countries, **5** requests on the grounds of Article 36a(7) of the Personal Data Protection Act (the so-called derogations).

1. Authorisations for Transfers

In an effort to lower their administrative costs, companies are increasingly interested in the lawful processing of personal data that has become the subject of transfer under corporate company rules under the corporate links within a group of companies located in different countries. During the reporting period, on the grounds of Article 36b(1) of the PDP Act CPDP authorised four transfers on the grounds of compulsory company rules. Data of employees and clients are mainly transferred. Human resources management, employment and financial and accounting activities are stated as main objectives of transfers.

In addition to the above, during the reporting period CPDP also issued resolutions for transfer of data in connection with other requests.

On the grounds of Article 36b(1) of the PDP Act in conjunction with Article 85(1) of the Constitution of the Republic of Bulgaria and Article 26(2) of the International Treaties of the Republic of Bulgaria, and having verified that the data controller which provides the data (NRA) and the data controller which receives the data (the US tax administration – Internal Revenue Service, IRS) have provided sufficient safeguards for their protection, CPDP authorised the transfer of financial information containing personal data for the purpose of regular automatic exchange within the meaning of the Agreement between the Government of the United States of America and the Government of the Republic of Bulgaria to Improve International Tax Compliance and to Implement the Foreign Account Tax Compliance Act (FATCA) for the period of validity of this agreement.

On the grounds of Article 36b(1) of the PDP Act in conjunction with Article 85(1) of the Constitution of the Republic of Bulgaria and Article 26(2) of the International Treaties of the Republic of Bulgaria, and having verified that sufficient safeguards are provided for the personal data in question, CPDP authorised the transfer by the NRA of financial information containing personal data for the purpose of the regular automatic exchange within the

meaning of the Convention on Mutual Administrative Assistance in Tax Matters, as amended with the Protocol Amending the Convention on Mutual Administrative Assistance in Tax Matters in force as of 1 June 2011, as well as of the Multilateral Competent Authority Agreement for automatic exchange of financial account information for the respective periods of validity of the convention/protocol/agreement.

During the reporting period CPDP received a request for authorisation of the provision of personal data in third countries from a company providing tourist services for Bulgarian and foreign citizens in the country and abroad. The evidence enclosed with the request make it clear that when purchasing a product from the tourist company, tourists sign a tourist service contract and a declaration of consent for the use of their personal data to book and pay for all the basic and auxiliary services relating to their travel and chosen by them.

Following a review and verification, CPDP authorised the transfer and delivered the following opinion: the company can provide personal data of its clients (consumers) to third countries for the purposes of its operations, namely – booking of and payment for basic and auxiliary services relating to travels, on the grounds of explicit and informed consent from the data subjects (cf. Article 36a(7)(1) of the PDP Act) subject to compliance with the requirement for provision of information of Article 19(1) of the PDP Act. Also, after the purposes of the processing of the personal data are achieved, the PDC shall destroy the data (cf. Article 25 of the PDP Act).

Another authorisation for transfer issued by CPDP is related to a request for authorisation of transfer of personal data submitted on the grounds of Article 36a(7) of the PDP Act (so-called derogations). The company transferring the data provides services for collecting claims of consumers arising out of problems with air tickets. The processing of the personal data subject to the transfer is related to making claims and receiving, on behalf of the client, sums due in connection to problematic flights, making bank transfer of the said amounts into an account of the client, accounting purposes, marketing and statistics. The purpose of the transfer of personal data to third countries is to claim and receive on behalf of the client compensations payable by airlines as a result of problematic flights, including: long delay, cancellation, refusal of boarding an airplane and/or seating in a class lower than

the class paid. It should be noted that the countries to which the personal data above could be transferred depend on the location of the relevant airline, the alternative dispute resolution authority, the administrative body, including the national supervisory authority, the court, persons with which the company operates in order to perform its contractual obligations. Potential clients must make a user profile in the website of the company in order to use its services. Personal data are provided only after potential clients have given their explicit and informed consent.

In its decision CPDP states that the company can provide personal data of its clients to third countries for the purposes of its operations, namely – services relating to claims of consumers arising out of problems with air tickets, on the grounds of explicit informed consent from the data subjects. After the purposes of the processing of the personal data are achieved, the PDC shall destroy the data.

2. Notifications of Transfers

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 need not request an authorisation for such transfer. In these cases PDCs shall notify the forthcoming transfer to CPDP and provide evidence of concluded standard contractual clauses.

When considering the notification, 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

3. Review of the Compliance with the EU–U.S. Privacy Shield

On 18 October 2017 the European Commission published a report on the first joint review of the EU–U.S. Privacy Shield. Representatives of the US government, the European Commission, the European Data Protection Supervisor, the Article 29 Working Party and European supervisors took part in the joint review (18–19 September). The Chairperson of CPDP Mr Ventsislav Karadzhov in his capacity of Deputy Chairperson of the Article 29 Working Party was part of the team.

The report covers all aspects of the agreement – implementation, administration, supervision and setting up of the legal framework by the US competent authorities. The focus of the evaluation is to confirm that the mechanisms and procedures underlying it are fully implemented and function in the way set out in the adequacy decision.

The reviewing team collected information from stakeholders – companies certified under the Privacy Shield, and from NGOs working in the area of fundamental rights, and in particular digital rights and privacy.

The joint review showed that the US government has provided the required structures and procedures for the functioning of the Privacy Shield. According to the information provided, over 2,400 companies have been certified under the scheme. Furthermore, the US authorities have ensured a complaint mechanism and procedures for protecting the rights of individuals. These include remedies for EU citizens, such as arbitration and ombudsman.

Based on the results, it is established that the US continues to provide an adequate level of protection with regard to transfers of personal data from the EU to companies in the United States.

At the same time, the European Commission made the following recommendations:

- Companies cannot rely on the agreement before the process of certification by the Department of Trade is completed;
- Proactive and regular inspections by the Department of Trade for false statements by companies the certification process of which is not completed;
- Ongoing supervision for compliance with the legal framework;
- Raising awareness;
- Improved cooperation between the Department of Trade and European supervisors;

- Study of the automated decision-making;
- Presidential Policy Directive 28 (PPD-28) incorporated in the Foreign Intelligence Surveillance Act;
- Quick appointment of an ombudsman for the Shield;
- Quick appointment of PCLOB members;
- More timely and detailed reporting on developments by the US authorities.

IX. Preparation for the Implementation of the New EU Legal Framework in the Field of Personal Data Protection: General Data Protection Regulation and Personal Data Protection Directive

After four years of intensive negotiations, on 4 May 2016 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) and 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 were published in the Official Journal of the European Union.

The General Regulation provides for the deferred application of its provisions as of 25 May 2018. The deadline for transposing the Directive is 6 May 2018.

In principle, personal data protection policy is extremely horizontal in nature, affecting almost all areas of life and all business sectors. This fact was taken into account by European legislators when the General Regulation was adopted, resulting in a comprehensive and complex legal instrument. From the perspective of EU law, the regulation is a directly applicable statutory instrument, binding in its entirety. Its purpose is to ensure uniform application of the Union law in all Member States. The Regulation, unlike the Directive, does not need to be transposed. One of the challenges posed by the General Data Protection Regulation, however, is the heterogeneous nature of its provisions, which allow, and in some cases oblige, legislators in the Member States to adopt national implementing measures. In this respect it can be said that it has some of the characteristics of a directive.

Regardless of the different legal nature of the two legal instruments of the EU (regulation and directive), the analysis of their provisions shows that the national legislation synchronised with them shall be regulated in a single national legal instrument – in an Act Amending and Supplementing the Personal Data Protection Act (AASPDP Act). This approach is best suited both from the point of view of principle and in legal and technical terms.

In connection with the above, during the reporting period a draft AASPDP Act was prepared, accompanied by draft reasoning and a draft of a partial preliminary impact assessment.

In the part concerning the General Regulation, the draft AASPDP Act was developed at an internal expert level by CPDP. Measures for the implementation of the regulation are adopted with this part of the draft law. The draft law in the part concerning the Directive was developed by an interdepartmental working group chaired by the MoI, in which CPDP representatives participated.

The draft AASPDP Act sets out the national measures required for the implementation 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), and transposes 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 (the Police Directive).

Some of the national legislative solutions proposed in the AASPDP Act are as follows:

Updated system of concepts: the Regulation considerably expands the existing system of concepts in the field of personal data protection. The proposed changes to legislation update the terminology used in accordance with Regulation 2016/679 and Directive 2016/680.

Data Protection Officer: controllers and processors shall designate a data protection officer (DPO) in the three hypotheses of Article 37, paragraph 1 of the General Regulation (public authority or local government body; systematic monitoring of data subjects on a large scale; processing on a large scale of special categories of (sensitive) personal data). In addition to this, AASPDP Act proposes mandatory designation of a data protection officer where personal data of more than 10,000 individuals are processed.

Registration of PDCs: as of 25 May 2018, the obligation for registration of PDCs with CPDP is abolished. This circumstance is taken into account in the draft legislative amendments and supplements by proposing to repeal the existing texts regulating the mandatory registration as a PDC.

Special situations of processing of personal data: the draft law proposes a more detailed regulation of certain groups of public relations, such as exercising the freedom of expression and information, including for the purposes of journalistic, academic, artistic or literary expression; processing of personal data in the context of employment/official legal relationships; legal regulation of the public access to Personal Identification Numbers in special acts; excluding the data of deceased persons from the personal data.

Administrative sanctions of public bodies: no distinction is made between public and private PDCs in the sanctioning regime for breaches of the rules on the protection of personal data.

Secondary legislation: in view of the wide diversity of matters regulated by the General Regulation and the PDP Act respectively, the proposed changes envisage a legislative delegation for the adoption of secondary legislation such as an ordinance in the field of certification and of non-statutory instruments such as the minimum requirements for systematic large-scale video surveillance of publicly accessible areas, as well as with regard to the automated individual decision making, including profiling.

Pursuant to the requirements of Article 19(2) in conjunction with Article 20(2) of the Statutory Instruments Act, a partial preliminary impact assessment of the draft AASPDP Act was carried out. The draft AASPDP Act was sent to the Minister of Interior for taking action within his competence for the conducting of a public consultation and submitting the draft for consideration to the Council of Ministers.

In connection with the implementation of the new General Data Protection Regulation, in 2017 CPDP held a wide information and awareness campaign targeted at different groups of stakeholders:

- individuals – data subjects;

- representatives of government and local authorities;

- personal data controllers and processors in the private sector in connection with the implementation of the new EU legal framework in the field of personal data protection: General Data Protection Regulation and Data Protection Directive. During the reporting period CPDP representatives participated in different forums.

At the beginning of the reporting period CPDP commemorated the Day of Personal Data Protection for the 11th consecutive time. The focus of the celebrations for still another year is the CPDP dialogue with the citizens and the PDCs. The traditional 'Open day' and 'Open reception' were organised. In order to present personal data protection in a comprehensible and memorable way, short animated information and educational videos on 'Privacy in the Digital Age' were translated and adapted. Each of the 10 videos contains an important message relating to the behaviour of individuals on the internet, in social media and when using mobile devices, as well as easy-to-remember privacy tips. The information and educational videos are accessible on the CPDP website in Bulgarian and in English.

As the sole supervisor in Bulgaria, CPDP has an important engagement to conduct a wide-ranging awareness campaign in an accessible language to promote the fundamental stances of the new Regulation (EU) 2016/679 so that the messages reach the widest possible range of stakeholders. In connection with this, during the reporting period CPDP developed a manual – information material '10 practical steps for implementation of the General Data Protection Regulation', which was published on the official website of CPDP. The purpose of the document is to present in a synthesised form and in an accessible language the basic practical actions PDCs shall undertake in order to fulfil the obligations imposed on them by the provisions of the General Data Protection Regulation. With this information material CPDP supports the operations of PDCs through up-to-date advice on the implementation of their duties in practice.

X. International Activity

1. Preparation for the Bulgarian presidency of the Council of the EU

During the reporting period a team for the Bulgarian Presidency of the Council of the EU, comprising 8 people and headed by the Chairperson of CPDP and one of the CPDP Members, was set up. All team members attended specialised training in public administration, organised by the Ministry for the Bulgarian Presidency of the Council of the EU, the Diplomatic Institute and IPA. Thanks to the training, team members were able to develop their negotiating skills, including trialogues, communication skills, chairing of meetings of EU Council working parties, working with EU documentation and document flow, etc.

In addition, each expert in the team is specialised in specific legislative files and EU topics, on which CPDP will have a lead or supporting role: a proposal for a regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies, the modernisation of Convention 108 of the Council of Europe, the proposal for a Regulation on privacy and electronic communications (ePrivacy Regulation), storage of traffic data for the purposes of national security and the fight against crime, the legislative proposal of the Commission on electronic evidence (e-evidence) expected at the beginning of 2018, and other.

2. Hosting the 40th International Conference of Data Protection and Privacy Commissioners in 2018

In 2017 the approval of the joint application of the Commission for Personal Data Protection and the European Data Protection Supervisor (EDPS) for hosing the 40th International Conference of Data Protection and Privacy Commissioners in 2018 was officially announced. An official presentation video clip of the anniversary issue of the largest personal data protection and privacy forum, as well as a joint conference brochure were prepared during the reporting period. CPDP and EDPS are currently negotiating a preliminary programme for the conference. The plenary part of the forum is planned to be held in Brussels, with two of the panels held as open sessions from Sofia. Through videoconferencing and a balanced programme, it will be proved that with the help of modern technologies

professionals in the field of personal data protection are more united in their efforts than ever before. It is planned to implement in Sofia a programme aimed at businesses, the non-governmental sector, academia, as well as the public sector from Bulgaria, the Western Balkans and the Commonwealth of Independent States. The International Conference of Data Protection and Privacy Commissioners is an annual event dating back to 1979. It is the largest and most important forum for exchanging experience, good practices and analyses of trends in the personal data protection sector worldwide and brings together 115 accredited bodies from all over the world. The hosting of the conference is entrusted to countries with proven experience and capacity in the area of personal data protection and history of observing and respecting human rights and freedoms.

3. Participation in EU Working Formats

In 2017 experts from the administration of CPDP participated in working groups to EU institutions. The participation in the discussion of the Commission working group on the introducing of the measures implementing Regulation 2016/679 and the transposition of Directive 2016/680 into the legislation of the Member States during the reporting period contributed to the progress in the development of key provisions in the amendment of the Bulgarian Personal Data Protection Act.

In January 2017 the European Commission presented the proposal for a regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. The adopting in 2016 of the General Data Protection Regulation and the Police and Justice Directive results in higher standards for ensuring the protection of personal data, which necessitated amendments to a number of legal instruments, including Regulation (EC) No 45/2001. During the reporting period CPDP experts participated in the discussion of the new texts within the DAPIX (Data Protection) Working Party to the Council of the EU. In June 2017 the Justice and Home Affairs Council reached a common approach on the proposal for a regulation, and in November 2017 the Estonian Presidency opened negotiations (trialogues) with the European Parliament. At the beginning of December 2017 it became clear that the work on the legislative dossier will continue during the Bulgarian presidency of the Council of the EU.

In 2017 the European Commission presented its proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). In essence, the proposal is a review of Directive 2002/58/EC (Directive on privacy and electronic communications). It is precisely the reform of the data protection framework, in particular the adoption of Regulation (EC) 2016/679, which requires to update the legislation in this area. On the one hand, the purpose of the new legal instrument proposed by CPDP is to ensure a better protection of privacy in electronic communications by building trust in digital services and their security, and on the other hand – to open new opportunities for business in the context of the digital single market strategy. Due to the complex nature of the relationships it deals with, as well as because of the issues raised in the field of personal data, experts from CPDP support the leading experts participating in the discussions within the TELE (Telecommunications and Information Society) Working Party of the Council of the EU. It shall be noted that Maria Mateva, Member of CPDP, took part as a representative of CPDP in the joint meeting of the TELE Working Party and the DAPIX Working Party on the on maintenance of metadata for the needs of national security and for the prevention, detection and investigation of serious crime. The work on the dossier continues.

4. Participation in international data protection forums

In 2017 the participation of 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 Joint Supervisory Body of Europol, 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 2017 CPDP continued to provide assistance within its competence to the full accession of Bulgaria to the Schengen area. CPDP was able to fully implement its commitments stemming from the interdepartmental plan with measures on Bulgaria's readiness to fully implement the Schengen acquis. The practice of participation of CPDP members in Schengen evaluations in the field of personal data protection in other Member States continued. During the reporting period the Member States evaluated were Norway, Sweden, Iceland, Spain and Portugal.

5. Spring Conference of European Data Protection Authorities

On 27 and 28 April 2017 in Limassol, Cyprus, the Office of the Commissioner for Personal Data Protection of the Republic of Cyprus hosted the annual Spring Conference of European Data Protection Authorities.

The event was held in the context of the introduction of the new European rules on data protection – the General Data Protection Regulation and the Directive on the Protection of Personal Data in Police and Criminal Justice Activities, and the modernisation of the Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data. In the context of the new challenges for data protection authorities, the agenda of the conference covered a number of topics aimed to reach the widest possible range of delegates, namely the new data protection rules, the raising of the awareness of people and businesses, the transparency and accountability in clouds, the access of law enforcement authorities to personal data, the challenges for privacy with regard to genomes and databases.

The latest developments in the modernising of Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and the implementation of the General Data Protection Regulation and the Directive on the Protection of Personal Data in Police and Criminal Justice Activities were presented during the forum. In the meantime the Article 29 Working Party is developing manuals for personal data controllers and processors, and the European Commission shall prepare the regulating of some provisions of the Regulation and the Directive. As a result of the discussions, Resolution No 1 of the Conference was adopted.

The need for international cooperation in the fight against terrorism and other forms of organised crime was also taken into account while emphasising that it is essential for this cooperation to be based on mutual trust and respect for the right to data protection. Also, a number of legislative proposals and initiatives are being developed, which lead to a huge collection of personal data and to exchange of information among interoperable large-scale systems for law enforcement purposes. These include the Convention on Cybercrime of the Council of Europe, the package of proposals for smart border control of the EU, the EURODAC Recasting Regulation, the EU entry/exit system, the European Travel Information and Authorisation System, etc.

New accreditation rules were discussed and adopted within the Spring Conference. In accordance with the decision, a working group was set up with a mandate to draft and propose new rules to amend the rules existing since 2004. The new role of the conference was discussed and the general desire was expressed to transform it into the absolute annual event of data protection authorities.

6. 39th International Conference of Data Protection and Privacy Commissioners

The annual event is among the most important global fora for exchange of knowledge, experience and ideas for interacting and developing unified methods of action for data protection authorities around the world.

Delegates from around the world – personal data protection authorities, non-governmental organisations, the academia and the business – take part in the conference. In 2017 the conference was held in Hong Kong from 25 to 29 September 2017. Representatives of the Bulgarian supervisor were its Chairperson Ventsislav Karadzhov, the member of CPDP Tsvetelin Sofroniev and the General Secretary Desislava Toshkova-Nikolova. The conference was held under the motto ‘Connecting West with East in Protecting and Respecting Data Privacy’.

As a rule, closed sessions are held at the beginning of the conference. In Hong Kong the main topic of the conference was ‘Government information sharing: Protecting sensitive

data, preventing discrimination and managing risk'. Topics relating to the sharing of information, the role of government bodies, the public concerns in connection with discrimination and the protection of personal data were discussed.

The open sessions were devoted to the following main topics: 'Data Protection in Asia', 'Notice and Consent', 'Cross-border Data Transfer', and 'Challenges of New Technology'.

An emphasis was placed on the differences in the privacy culture of the West and the East, the changes in public perceptions of privacy and the applicability of Western data protection models in Asia and other parts of the world.

The requesting and receiving consent as a milestone in building the trust on which the information society is built, and the question if there is room for a new approach to building trust in the online economy and better data protection were broadly discussed.

In view of the importance of cross-border transfers of personal data, the condition of the global regulatory framework was widely discussed. One of the highlights was related to the data transfer mechanisms under the EU law and the European Commission's efforts to expand the privacy and data protection frameworks with Japan and South Korea, as well as with trade partners in Latin America and the neighbours of Europe.

The important topics of the ethical aspects of artificial intelligence, the strategies and priorities in the regulation of digital economy results, the impact of cyber security on data protection, the role of encryption in the digital age, and the management of digital identity were also not omitted.

Traditionally, alongside the main sessions of the Conference, a number of accompanying events took place. CPDP representatives took part in the seminar devoted to the Privacy Shield, organised by the US Department of Trade.

The anniversary 40th International Conference of Data Protection and Privacy Commissioners in 2018 will be organised jointly by the Commission for Personal Data Protection of the Republic of Bulgaria and the European Data Protection

Supervisor. In connection with this, in the last panel of this year's conference the Chairperson of CPDP Ventsislav Karadzhov and of the European Data Protection Supervisor Giovanni Buttarelli presented the main topics and events envisaged for the forthcoming conference, which will be held in 2018 in Brussels and Sofia under the motto 'Do we need ethics in the digital world?'.

7. Conference of the Data Protection Authorities from Central and Eastern Europe

The forum is an annual event of the data protection authorities from Central and Eastern Europe. The purpose of the event is to support the implementation of international data protection standards and to provide an opportunity to share the experience and best practices of the countries participating in the meeting. Data protection authorities take the opportunity to discuss different aspects of personal data protection, existing challenges and opportunities to ensure the implementation of international data protection standards.

The main topics discussed were related to the processing or personal data in the law enforcement sector, the achievement of balance between public safety on the one hand and the respect for the right to privacy and data protection on the other hand, the awareness-raising campaigns held (development of guides and conducting of training events). The internal rules, the role, structure of the event, and the accreditation rules were discussed. The need to adopt resolutions and declarations for subsequent submission to the European Commission and the Council was emphasised. The risks to privacy that accompany the large data exchange in the context of diverse online services, social networks, online transactions, and search engines were also discussed. The experience of participants in the field of promoting decisions and the scope of the personal data disclosed was shared.

The Bulgarian data protection authority was represented by Mrs Maria Mateva and Professor Veselin Tselkov, members of CPDP. The Bulgarian representatives made a presentation within the 'Data Protection in the Internet' panel.

8. Participation in the European Practical Case Seminar and the Meeting of the GPEN Supervisors Organized by the UK Data Protection Authority

At the European Practical Case Seminar, data protection supervisors from Europe (including non-EU countries) had the opportunity to present separate aspects of the General Data Protection Regulation and, in particular, how exactly they intend to do implement them in practice. CPDP representatives made a presentation in the 'Strategy of Supervisors for the Implementation of the General Regulation' panel and outlined the main measures and activities CPDP undertakes to ensure the adequate and smooth implementation of the Regulation in Bulgaria. The presentation was positively welcomed by the other participants, some of whom were interested in further exchange of experience with CPDP in order to acquire good practices from the Bulgarian supervisor.

During the meeting of the GPEN supervisors, representatives of authorities outside Europe (Japan, South Korea, Israel, Canada) were provided with the opportunity to present their activities and achievements. The Bulgarian participants used the occasion to make a preliminary and informal study of the readiness of some of the non-European authorities to participate with lecturers and panelists in the 40th edition of the International Conference of Data Protection and Privacy Commissioners in 2018.

9. Training in 'Internet Governance'

The Balkan School on Internet Governance organised with the support of the Council of Europe training on 'Internet Governance', held from 21 to 25 August 2017 in Saraevo, Bosnia and Herzegovina. The event was targeted at representatives of government institutions, academia, the civil society, the business and the media. The topic of 'Internet Governance' is extremely topical, especially with a view to the future implementation of the General Data Protection Regulation. The main objective of the training was to encourage representatives of the Balkan countries to participate and to engage with the topic at both regional and international level and to make the problems and the existing perspectives public. By raising the awareness of national and regional experts on the importance of Internet governance and the urgent problems associated with its implementation, motivation was created for further participation in forums and future processes, and different research and assistance in this area was facilitated.

The training programme included fundamental issues relating to Internet governance – how does the Internet work, critical infrastructure, essence and main principles of internet governance. The role of the different actors in the processes was examined. The issue of network neutrality and how this protects the right of access was discussed. With regard to cyber security and encryption, the strategic question if the right to encryption should be protected was discussed. Issues relating to cybercrime and the relevant response – global, regional and national policies (laws, strategies, action plans) as well as operational mechanisms (centres for dealing with information security incidents, stakeholder roles, public-private partnerships) were presented. The establishing of a balance between data protection and freedom of speech was a subject of discussion. Other topics, such as 'Copyright and internet intermediaries' and 'Jurisdiction in the internet space', were also included in the training. In order to illustrate the application of theoretical knowledge in practice, a simulation of an Internet governance process was carried out.

10. Other international initiatives

During the reporting period CPDP considered a letter regarding the request made through the Permanent Representation of the Republic of Bulgaria to the EU by representatives of the US Department of Homeland Security to the US Mission in Brussels regarding the possible interest of our country in the signing of a letter of intent to exchange information on travellers convicted of sexual abuse of children. In connection with the question raised for coordination, CPDP notes that Bulgaria participates in the Global Alliance Against Sexual Abuse of Children Online, established at the end of 2012 and aiming at uniting decision-makers around the world in view of more effective detection of and providing assistance to victims and of prosecution of perpetrators through enhanced international cooperation. The Member States and many third countries, including the USA, are among the participants in the initiative. The discussion of the possibility for Bulgaria to declare an interest in signing a letter of intent to exchange information on travellers convicted of sexual abuse of children shall be considered taking into account the following framework parameters.

- The letter of intent does not create a mechanism for possible future cooperation. Such a mechanism will be created with the signing of the relevant international agreement with reciprocal action.

- Bulgaria shall express an intention to exchange information only regarding persons convicted of sexual abuse of children but not regarding persons suspected of such a crime.

- Data within a possible future agreement shall be exchanged only between competent authorities.

The best interest of children shall be guaranteed in the exchange of information regarding persons convicted of sexual abuse of children.

Cooperation continues between experts from CPDP and MoI in the framework of the international cooperation within the Working Party on Personal Data Protection to the Police Cooperation Convention for Southeast Europe (PCC SEE), where the draft implementation agreement on the protection of personal data within the Convention is discussed. Work on the implementation agreement started in December 2016, and in 2017 CPDP expressed an opinion on the proposed version of the instrument. Constructive recommendations were made regarding the conformity of the agreement with the new legal framework in the field of personal data protection, and in particular 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, and the Commission communication relating to the exchange of data and their protection on a global scale (Communication from the Commission to the European parliament and the Council – Exchanging and Protecting Personal Data in a Globalised World; http://europa.eu/rapid/press-release_MEMO-17-15_en.htm). Accordingly, at a later stage CPDP experts offered specific texts that are largely in line with the text of the model agreement on judicial and police cooperation with third countries – the so-called EU–USA Umbrella Agreement. United by

the fact that some of the parties to the Convention are EU Member States and the other part are pre-accession countries – candidates for the EU, CPDP believes that the new legislation sets a high standard and is a common goal to which we all should aspire. The work on the agreement continues.

XI. Training in the Field of Personal Data Protection

CPDP is the only national authority in the Republic of Bulgaria with control and supervisory powers in the field of personal data protection and privacy. Pursuant to the PDP Act, the Commission exercises control of both private individuals and entities and public authorities that have the status of PDCs. One of the main tools for prevention and establishing uniform standards among PDCs from the private and the public sector is the holding of training events. This obligation has been entrusted to CPDP with the PDP Act (Article 10(13)).

The General Data Protection Regulation imputes CPDP, in its capacity of a supervisory authority, to 'promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing' (Article 57, (a)).

In 2017 an entirely new concept was developed for conducting training in the field of personal data protection. It sets out the different target groups of trainees (PDCs, data protection officers, data subjects interested in the matter), and for each type a training programme is proposed of different duration and content, tailored to their interests, wishes and to the challenges they could face in the processing of personal data.

The concept for conducting training in the field of personal data protection complements the efforts of CPDP within the launched procedure for the development of a national training centre which can provide data protection officers, PDCs and other stakeholders with the training they need. The plan is to conduct the training events provided mainly by electronic means. This project is implemented in several stages, and the first training events are expected to be held in 2018.

1. Development of a national training centre in the field of personal data protection

The new moments in the statutory regulation of the protection of personal data call for specialised and targeted training of PDCs to prepare them to meet the requirements of the General Regulation. This is especially valid for data protection officers (new legal figure under the General Regulation), who must be covered by the training held. Currently CPDP

does not have the resources required to cover the entire spectrum of PDCs needing training in the field of personal data protection after the start of the implementation of the new European legal framework in May 2018. At the same time, the inclusion of this highly specialised and large-scale training in the responsibilities of existing training structures would deprive them of their resources and would decrease the effectiveness of the training being conducted due to the fact that only the supervisory authority for personal data protection has the specific experience and knowledge to conduct such training adequately.

The analysis carried out by CPDP clearly demonstrates that the most effective way to respond to the training needs of the public and private sector in Bulgaria is to establish a national training centre for personal data protection within CPDP, which shall be adequately supported by human and financial resources and shall assume the responsibilities relating to the training of data protection officers in Bulgaria as well as supporting tasks relating to the accreditation and certification in compliance with the General Regulation.

In this connection, in 2017 CPDP carried out the following activities relating to the development of the national training centre:

1. All documents required for the issuing of a construction permit by Mladost Municipality were prepared. As a result, the chief architect of Mladost Municipality issued construction permit No 19/12 June 2017 for 'Reconstruction and internal reconstruction of the administrative building of the Commission for Personal Data Protection (CPDP)'.

2. A procedure for award of a public contract with the subject 'Reconstruction and internal reconstruction of the administrative building of the Commission for Personal Data Protection (CPDP)' was organised and conducted. As a result of the successfully conducted procedure, a contractor was selected to perform the construction and installation works required for the development of the national training centre. At present the development of the training centre has not started because of the lack of financial resources. CPDP has created the necessary organisation, so that when the State grants the required financial resources, the construction and installation works can start immediately.

3. The introduction of a Training Management System for the purposes of CPDP is an important part of the training conducted by the Commission. In this connection, terms of

reference for the introduction of a Training Management System for the purposes of CPDP were developed during the reporting period. Pursuant to the requirements of the EG Act, they were coordinated with the State e-Government Agency. When the required financial resources are received, CPDP is ready to conduct a procedure for award of a public contract with the subject 'Introduction of a Training Management System for the purposes of CPDP'. Through the system PDCs will have access to learning content and will be able to participate in interactive training in real time. The proposed system will create an opportunity to conduct courses (classes) in two languages. The training in a module can start with an entrance test for determining the entry level of the trainee, and end with an examination. The examination can be oral or written (test). In distance learning, there is no limit to the number of trainees in a class, as well as to the simultaneous training for different classes.

In order to achieve maximum readiness for the rapid start of the training events in the centre, at the end of the reporting period CPDP developed a curriculum and learning content oriented towards the different target groups and in particular to the data protection officers. Part of the training modules were developed jointly with international partners from supervisory authorities of other Member States, such as Italy, Spain, Poland, Croatia.

2. Participation in CPDP representatives in information and training forums

During the reporting period the Chairperson, CPDP Members and experts participated in seminars and round tables with the topic 'Regulation 2016/679 and the Obligations for PDCs Arising out of it'. CPDP mobilised its efforts to achieve broad public awareness on issues relating to the implementation of the new legislation.

On 26 June 2017 in 'St. Sofia' Hotel in Sofia a seminar on issues relating to personal data protection was held. The event was organised by the National Union of Legal Counsels in Bulgaria. CPDP lecturers made a comparative analysis of the administrative and penal provisions of the extant PDP Act and the corresponding provisions stipulated in the new Regulation 2016/679, with a focus in the envisaged maximum amounts of sanctions for administrative violations.

On 20 September 2017 a CPDP representative participated as a lecturer in a seminar with the topic 'Welcome the European Data Protection Regulation with Security Solutions from Oracle'. The event was organised in 'Sofia Hotel Balkan' and there was great interest in it. Possible financial sanctions of up to 4% of the annual revenues, the need to analyse and modify existing organisational processes, applications and systems, and the need to implement new compliance requirements were among the topics discussed at the forum.

An event organised by the international law firm Kinstellar was organised in Sofia on 27 September 2017. It was aimed at informing PDCs about the impact of the new legal framework in the field of personal data protection on them. Over 60 representatives of controllers in the areas of energy, information technologies, banking and financing, retail trade, consumer goods and telecommunications attended the seminar.

A forum 'Business Topic: New Rules on Personal Data' was held on 5 October 2017 with great interest. Over 130 participants attended, including representatives of banks, insurance companies, investment firms, non-banking lending companies, agencies for collection of receivables, IT companies, law firms, consulting firms, industrial companies, representative offices of foreign companies, small and medium-sized enterprises. Heads of different functional units, human resources management specialists, IT specialists, compliance and risk management officers participated in the forum.

The first national round table with the topic 'Certification for Personal Data Protection in Bulgaria and the EU pursuant to Regulation (EU) 2016/679' was held on 10 October 2017. Representatives of government institutions, non-governmental organisations, private businesses and academia took part in the event.

On 24 October 2017, in 'Varna' hall of 'Interpred' – STC, the CPDP Chairperson and CPDP experts participated in a forum with the topic 'GDPR – Are you ready?'. The German–Bulgarian Chamber of Industry and Commerce was a co-organiser of the seminar.

On 25 October 2017, in 'Sofia Hotel Balkan', at the invitation of MEP Eva Maydell the Chairperson of CPDP participated together with EU Commissioner for Justice and Consumers Vera Yorova in a round table with the topic 'What we need to know and how to meet the new requirements of GDPR'. The summit was organised in partnership with the Confederation of Employers and Industrialists in Bulgaria. The event provided an opportunity

to receive information directly from the EU Commissioner and to share opinions on the topic. The representatives of Bulgarian businesses present at the meeting highly valued the attendance and expertise of the CPDP Chairperson.

On 30–31 October 2017 CPDP representatives took part in the Fourth regional forum on cyber security for the countries from Southeastern Europe, organised by the International Cyber Investigation Training Academy, Chief Directorate 'Combating Organized Crime' and IDC Bulgaria. Over 300 experts in cyber security from the public sector and businesses, representatives of leading companies in the sectors of ICT, logistics, energy and utilities, pharmaceutical industry, financial organisations and banks, non-governmental organisations, educational institutions, law enforcement agencies from over 20 countries, international organisations, media and end-users participated in the forum. CPDP representatives took part in the panel discussion on 'Management and compliance with the new data protection regulation. Is outsourcing to third countries possible?'

On 23 November 2017 the Council for Information Security of DSK Bank organised the IV annual conference 'Compliance and information security: Cyber resilience to evolved cyber threats'. A representative of CPDP made a presentation with a subject 'Are we ready to cover the requirements of GDPR? DPO (Data Protection Officer) as a position in the organisation and the role of the human factor'.

On 1 December 2017 on the initiative of the Bulgarian Industrial Capital Association (BICA) a working meeting was held in the building of CPDP between the CPDP management and the management of BICA to discuss the implementation of Regulation (EU) 2016/679. The Chairperson and members of CPDP and experts from the administration of the Commission took part in the meeting, and on the part of BICA – Boyan Boychev, Member of the Management Board, Dobrin Ivanov, Executive Director, and Ivelin Zhelyazkov, Director for Tripartite Cooperation.

The practical implications for businesses of the entry into force of the GDPR (General Data Protection Regulation), such as the abolition of the obligation to register as PDCs and the subsequent responsibility for storing data, were discussed at the working meeting. The obligation to designate a data protection officer, the selection and training of such person,

the risk management with regard to personal data protection, the action plan, and the required documenting and reporting were also discussed. Special attention was paid to the awareness of data subjects, the transparency of the processing, and the practical exercising of rights. The CPDP representatives acquainted the business with their readiness to implement the requirements of the new Regulation and their resources for carrying out inspections for compliance with these requirements.

The parties agreed, in the spirit of cooperation, to avail of the opportunities for certification of companies under Regulation 2016/679. BICA will properly inform its members of the new requirements of the Regulation and their practical implications.

After the working discussion, CPDP received a letter of thanks from BICA expressing readiness for further fruitful cooperation.

On 14 and 15 December 2017 a working meeting of CPDP experts with representatives of the three mobile operators in the territory of Bulgaria – 'Vivacom', MobilTel' and 'Telenor' was held. The event was initiated by the mobile operators, and its objective was to discuss practical issues in their activities related to their preparation for the implementation of the new European General Data Protection Regulation as of 25 May 2018. The two-day working meeting was held in the form of dialogue, in which CPDP experts explained the main issues related to the implementation of the Regulation and the representatives of the mobile operators asked questions and discussed specific problems related to their work. The main topics of the meeting were: 'Consent of data subjects', 'Rights of data subjects – scope and exercising', 'General Rata Protection Regulation and sectoral rules in the field of electronic communications', 'Forthcoming national regulation and CPDP policy', 'Processors – instructions, monitoring and responsibility', and 'Certification, codes of conduct and training'. At the closing of the working meeting both sides expressed their satisfaction with the form of the meeting, the bilateral exchange of information and the willingness to continue the working dialogue in order to fulfil the requirements for protection of the personal information of citizens – customers of electronic communications services.

On 18 December 2017 CPDP hosted a practical training event for lecturers and students from the fourth year of the Bachelor's degree in Public Administration of the Academy of the Ministry of Interior.

On 19 December 2017, in the building of the Communications Regulation Commission (CRC), CPDP experts held a working meeting with lawyers from the Legal Regulation and General Legal Services Directorate of CRC. The topic of the meeting was the practical implementation of the requirements introduced by the new legal framework in the field of personal data protection. CPDP representatives made presentations on the topic 'Main provisions introduced in Regulation 2016/679, and ten practical steps for the implementation of the General Data Protection Regulation'.

After the meeting, CPDP received a letter of thanks for the interesting presentations and the answers to the many questions asked by CRC experts, as well as for the useful discussion on the subject of personal data protection in the context of the new requirements introduced by the General Data Protection Regulation.

XII The Commission for Personal Data Protection in the capacity of Data Security Supervisor under the Electronic Communications Act

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 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, received from undertakings providing 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.

Due to the legislative changes in the EC Act, amendments and supplements were adopted at the end of 2016 in the compulsory instructions to reflect the imperative requirements arising from the entry into force of the Counter-Terrorism Act and the supplements to the Disaster Protection Act. With a decision dated 1 February 2017 CPDP updated the compulsory instructions issued under Article 261a(3)(2) of the EC Act to the obligated entities under the Act. The compulsory instructions are intended to unify the practice of all institutions, bodies and undertakings providing public electronic communications networks and/or services involved in the process of requesting and providing access to stored traffic data under Article 251b(1) of the EC Act, in compliance with the requirements of EC Act and the PDP Act.

During the reporting period 104 undertakings submitted information to CPDP. They are with 27 more (about 30% more) compared to the previous year.

The number of cases of requested information was the lowest for the period 2011–2017. The reasons for these changes should be sought primarily in the amendment and supplement to the EC Act in 2015 and the ensuing higher requirements to authorities competent to obtain information, as well as in the increased judicial control.

Based on the information submitted by 104 undertakings providing public electronic communication services, the following statistics can be summarised:

- The total number of requests for access to traffic data was 65,505, which is a 10.67% decrease on the previous year.

- The cases where the request for provision of traffic data could not be responded to were 546, under 1% (0.83%), which was considerably lower compared to the previous year, when the percentage of these requests was 3.8%. Most of the cases were related to requests covering periods outside the statutory one – 6 months.

- The time elapsed from the initial date of storage until the date on which the competent authorities requested the transmission of data (age of data) was mainly up to 3 (three) months – in 66% of the cases (Figure 12).

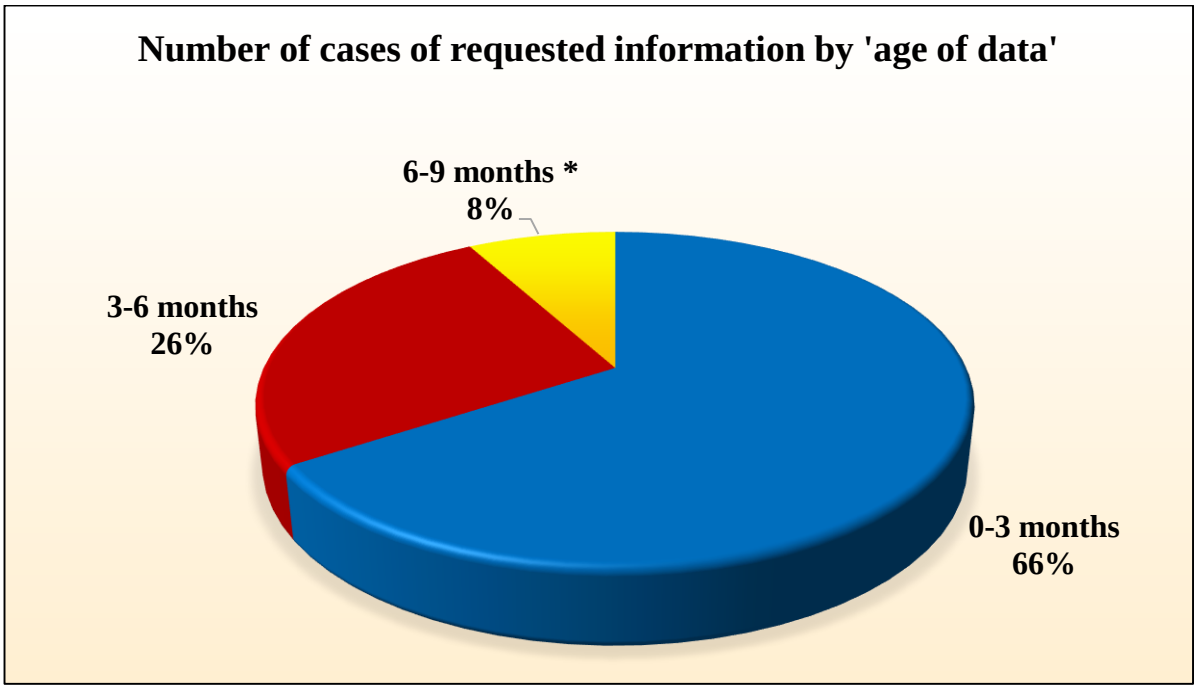

Figure 12

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

Statistics regarding the protocols received in 2017 is presented in Figure 13.

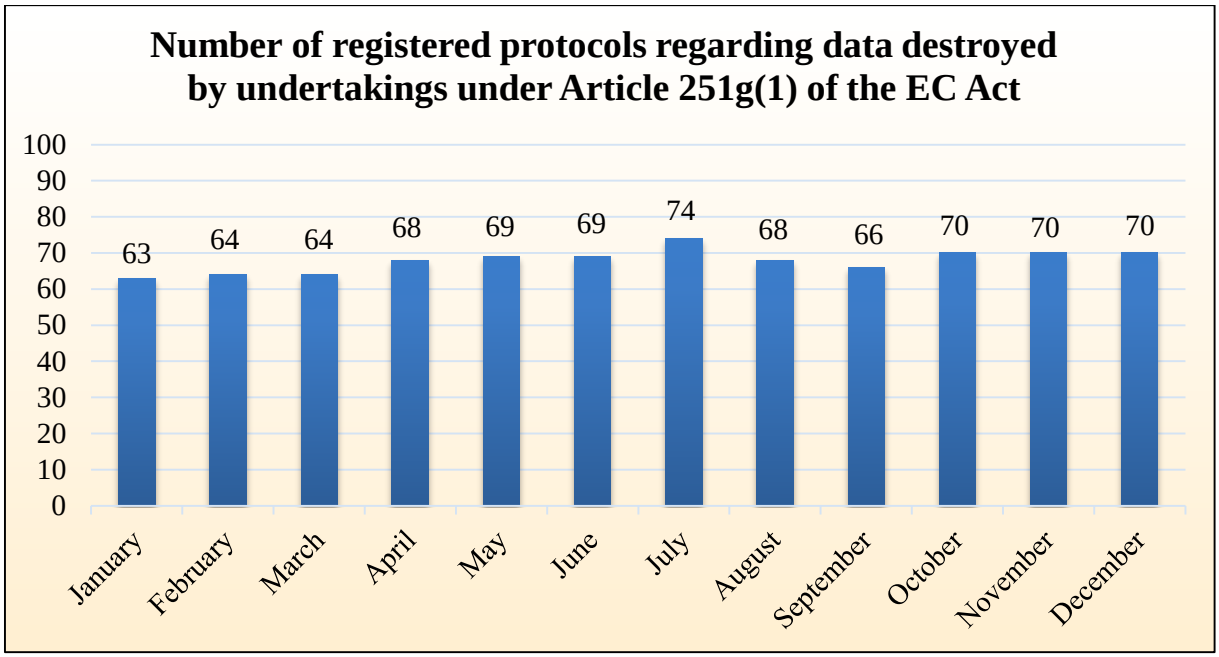

Figure 13

The number of undertakings that fulfil their obligation to provide monthly protocols regarding destroyed data under Article 251g(1) of the EC Act was 68 a month on the average.

XIII. CPDP Strategy for Development in the Field of Personal Data Protection (Horizon 2022). Preparation and Implementation of Nationally and Internationally Funded Projects

1. Strategy – General Information, Strategic Objectives, Targeted Policies, Action Plan for the Implementation of the Strategy

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).

Its development has also taken into account the experience accumulated by CPDP for 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 CPDP are defined.

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

- System implemented for the prevention and containment of the unlawful forms of personal data processing and violation 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, 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 the CPDP strategic objective can be achieved as effectively as possible. An interim evaluation and analysis of the implementation are envisaged. The strategic document sets out performance evaluation means and indicators. The Action Plan for the Implementation of the Strategy, which includes specific activities, indicators and responsible officials, is an integral part of the Strategy.

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. At the same time, considering the rapidly changing new trends in the area of personal data protection, the Strategy 'Horizon 2022' lays down a mechanism for a review to serve as a basis for its further development.

2017 was the first reporting period for the implementation of the Strategy. The individual administrative units provided information regarding the results achieved in the strategy implementation. The individual work plans of the officials in the administration for 2018 will take 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 2022’ and of the Action Plan for its implementation are accessible in the CPDP website.

2. Project Activities

- **Project Proposals Under Implementation**

At the end of 2015 a project proposal by 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 project value is 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 staff training to work with the platform and raising public awareness.

In 2017 CPDP participated actively in the implementation of the project activities. Based on the large-scale study of the attitudes of the academic community and employers in Bulgaria on the need to develop a postgraduate programme, a detailed curriculum was developed and proposed as a basis for a Master’s course. The project continues in the first quarter of 2018 with events promoting its results and with training of trainers.

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 project value is 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 (EC) 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. All administrative procedures relating to the signature of the contract were completed in 2017, so that the actual contract execution can start at the beginning of 2018. The project is envisaged to be completed at the beginning of 2020.

At the end of March 2017 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 project value is 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 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 to provide a collaborative environment and open, innovative and inclusive informal digital learning.

The first international project meeting was held, and the first activity 'Catalogue of Good Practices in the Field of Informal Adult Education' was launched during the reporting period. The planning of the work under two other intellectual products started during the same period: the 'Master Training Plan' and 'Open Learning Resources for Informal Digital Training in Data Protection'. The execution of the main volume of project tasks is planned for 2018.

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

Under the EU Instrument for Pre-Accession Assistance (IPA), representatives of CPDP support the implementation of the Support to Access to Right on Protection of Personal Data in FYROM project. They participate as key experts in a number of project activities, and a CPDP representative will be a project leader until the end of the execution of the activities. Since its inception, the Instrument for Pre-Accession Assistance has replaced a number of Community funding programmes and instruments, namely PHARE, PHARE CBC, ISPA, SAPARD, CARDS and the financial instrument for Turkey. IPA is the programme through which the EU supports reforms in candidates for membership in the Union by providing financial and technical assistance. The resources provided under IPA strengthen the capacity of countries during the accession process thus resulting in progressive positive development in the Western Balkan Region.

- **Project Proposals Under Preparation**

In August 2017, CPDP in cooperation with NGOs, research centres and universities from 11 EU Member States – Bulgaria, Germany, Spain, Austria, Ireland, Greece, Slovenia,

Lithuania, Estonia, Macedonia and Cyprus, prepared and submitted a project proposal under the largest European programme 'Horizon 2020' with a working title 'Data Security PPP: Pro-design: Protection of personal data through privacy by design'. The project proposal aims to support the implementation of the new EU legal framework in the field of personal data protection, and in particular the General Data Protection Regulation, by providing incentives and technological and organisational capabilities to PDCs to apply the 'privacy by design' principle in their daily operations.

The technological and organisational capabilities provided by the project proposal are related to the dissemination and use of a uniform set of criteria for the implementation of the 'privacy by design' principle, the development of technologies for clear and comprehensive framework for privacy as early as at the design stage, and the tools for evaluation of this process.

In addition, methods for raising awareness and promotion of new privacy concepts improving the privacy and data protection environment by creating a community that uses common and standardised tools and procedures for implementing the 'privacy by design' will be implemented among relevant stakeholders.

At the end of the reporting period, in partnership with the Union of Lawyers in Bulgaria and 'Apis Europe', CPDP started preparing a project proposal funded under the call for proposals 'Ensure the highest level of protection of privacy and personal data' of the EU Rights, Equality and Citizenship Programme. The lead partner and applicant will be CPDP. The project proposal aims at providing small and medium-sized enterprises with practical tools for achieving compliance with the General Data Protection Regulation. Following the implementation of the project activities, small and medium-sized enterprises 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.

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

XIV. Institutional Collaboration. Partnership with Media Representatives and Information and Educational Activity

1. Institutional collaboration

In the process of preparation of project proposals and subsequent implementation of the approved projects with EU funding, in 2017 CPDP expanded its partnership with the Sofia University 'St. Kliment Ohridski' and the International Cyber Investigation Training Academy (non-governmental organisation). In implementing the Erasmus+ e-OpenSpace project, CPDP is a partner not only of the oldest and most authoritative higher education institution in Bulgaria, but also of similar data protection authorities from Poland and Croatia as well as the oldest university in Poland – the Jagiellonian University. In the preparation and implementation of the approved project proposal under the EU Rights, Equality and Citizenship Programme, CPDP is a partner of the data protection authorities of Italy, Spain, Poland and Croatia. The two projects contribute to the development of partnerships with Italian NGOs.

By means of the prepared project proposals under the EU programmes Horizon 2020 and Rights, Equality and Citizenship, in the second half of the reporting period partnerships were established with the Union of Bulgarian Lawyers and with more than 10 NGOs, research centres and universities from different European countries.

In pursuance of its power to keep a register of PDCs and the registers kept thereby, in 2017 CPDP continued its interaction with Chief Directorate GRAO at the Ministry of Regional Development and Public Works with regard to the granting of access to personal data from NDB 'Population' regarding specific individuals in their capacity as PDCs. This information is required for maintaining the register under Article 10(1)(2) of the PDP Act.

In the spirit of good interinstitutional collaboration, in 2017 CPDP experts took part in an interdepartmental working group on the transposition in the SANS Act of 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, and in an interdepartmental group for the transposition of 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.

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

CPDP is constantly striving to ensure transparency and openness of its activity relating to the protection of personal data of individuals. By applying these principles, it provides information about its work in an easy and accessible for the society language. Because of the rapid development of the communications and high technology sector due to the digital evolution, CPDP seeks partnership and interaction with other government bodies, representatives of public and private sector organisations, and with civil society organisations. Comprehensive communication with these sectors and the media in Bulgaria is a guarantee of fruitful cooperation and good coordination of the efforts of the institutions related to the protection of personal data. All this is done by respecting the legitimate interests of stakeholders and seeking pragmatic solutions that benefit citizens and businesses.

In 2017 CPDP commemorated the Day of Personal Data Protection, 28 January, for the 11th consecutive time. The idea for celebrating this day was initiated by the Council of Europe and it was first celebrated in 2007. Today, 28 January is celebrated in a number of countries, both in Europe and around the world.

CPDP is a government institution with a mission aligned with citizens and their rights. For this reason, the focus during the reporting period continued to be on the dialogues with citizens and PDCs. Traditionally, an Open Day was organised, when the Chairperson and the members of CPDP and the Chief Secretary accept anyone wishing to visit them, get familiar with the atmosphere of their work, ask them questions, receive up-to-date information, and share ideas and suggestions.

A Reception for PDCs and citizens where experts from the administration received visitors, listened to their problems and answered their questions was opened on the Data Protection Day. CPDP believes that raising public awareness is a key preventive measure in safeguarding security in modern society.

During the entire day, short animated video clips with the subject ‘Privacy in the digital era’ were shown on the ground floor and in the conference room of CPDP. These video clips are also accessible on the official website of CPDP (www.cpdp.bg) and in the YouTube channel of CPDP.

CPDP also selects this day for submitting to the National Assembly its Annual Activity Report for year 2016.

On the occasion of the Data Protection Day, an annual prize for journalism is announced, which is awarded annually based on the following criteria:

- genre (investigative journalism);

- active and well-intentioned coverage of events;

- significance;

- timeliness;

- objectivity and truthfulness of information;

- interesting and accessible material;

- media with national coverage.

In 2017 the prize was awarded to the journalist from ‘Monitor’ newspaper Maria Kadiyska for the greatest contribution to journalism in 2016 in promoting the activities of CPDP and citizens’ rights to protection of their personal data and their privacy. The Chairperson Ventsislav Karadzhov personally presented the diploma and the plaque.

Another initiative of public interest was announced on the Data Protection Day – a competition with awards for children’s and pupils’ creative works (drawing, essay, poem) under the motto ‘What others know about me?’

Children and the protection of their personal data are always in in the focus of CPDP’s attention. The adolescents are the most vulnerable group in modern society in terms of privacy abuses, especially when communicating on the Internet. Besides the proven benefits, the broad capabilities offered by new technologies enable serious intrusion into the personal

space. For this reason one of the extremely important tasks of CPDP of high priority is to promote among children in school age the basic rules for safe communication in the social environment, especially through information technologies and the internet. The issue of privacy in all aspects of life is becoming increasingly relevant, and the responsibilities of CPDP as an independent supervisory body include active actions to clarify the activities of CPDP and the measures it takes to protect personal data.

With the assistance of the MoES through the regional education departments, 2,000 posters with information about the competition, as well as an information and education clip were distributed in schools throughout the country in February 2017.

The competition for children's creative works is held by CPDP for a second time. The interest in it was big, and more than 250 children aged 7 to 18 years from all over the country submitted their works. Children compete in 5 categories – poem, story, essay, drawing and song. The work of the Commission for the evaluation of creative works is extremely challenging, as each work deserves an award. The main criteria for the evaluation of works are as follows:

- correct interpretation of the topic;

- artistic value;

- correspondence of the artistic value with the age of the pupil.

Awards to the distinguished participants were presented on 19 May 2017. The event was attended by more than 70 people, including the ombudsman of the Republic of Bulgaria Maya Manolova, representatives of the Ministry of Education – 'Contents of Pre-school and School Education' Directorate, the civil society sector and businesses.

'Thank you for the invitation! This competition is a wonderful initiative on the occasion of the 15th anniversary of CPDP, which I intend to 'steal'. The idea to inform the young generation about their behaviour in sharing personal information on the Internet is very good. This is a cause I support, and the Commission can rely on me for future initiatives', Mrs Maya Manolova said.

The winners in the individual categories – poem, story, essay, drawing and song – received awards. Children received mobile phones, tablets, rucksacks, drawing sets, honorary diplomas and presents from sponsors and CPDP.

Over 30 letters of thanks were sent to the MoES and to all schools which assisted children in their preparation for participation, as well as in the sending of their works.

The initiatives for protecting the personal data and privacy of citizens were also supported by maintaining sustainable and beneficial relationships with the Bulgarian media. In 2017, due to the already established and facilitated personalised contacts between the Commission and media representatives, over 100 interviews and materials were realised with the participation of the Chairperson, members and experts from CPDP. The activities of the institution were reported in a number of publications in central daily newspapers and the main weekly newspapers. Electronic newswires and electronic media regularly cover the activity of the institution. CPDP responded to topical public issues and interviews on different topics in the Bulgarian National Television, bTV, Nova TV, 'Bg On Air' TV, BI TV, TV+, Bloomberg TV Bulgaria, Channel 3, the Bulgarian National Radio, bTV Radio, '168 Hours' newspaper, 'Monitor' newspaper, 'Economist' Magazine, Mlex market insight and other media.

The abuse by unauthorised use of personal data by political entities in collecting signatures of people supporting them for the parliamentary elections, and the preparations for the entry into force in 2018 of the new General Data Protection Regulation were among the topics of greatest public interest during the reporting period. In this connection, the Chairperson of CPDP took part in a series of broadcasts on all national televisions and was also a lecturer in business conferences of national and international significance.

CPDP provides promptly information to journalists on their written or oral request. This resulted in the publication of a significant number of information materials and journalistic investigations concerning various aspects of the protection of personal data. 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 institution to achieve publicity, transparency and open dialogue with the Bulgarian society.

3. The Website of CPDP – an Important Information Tool

The official website of CPDP is a basic information tool for creating maximum visibility for the society of both the CPDP activity and the overall developments in the topic of personal data protection. Three main improvements were made in the CPDP's website in 2017.

- A responsive design of the website was developed, making it accessible and convenient for use on devices with different resolutions, in particular mobile devices with small screens (tablets, mobile phones). This corresponds to the ever-increasing tendency for access to information from anywhere and at any time and to the CPDP's strategic goal of raising citizens' awareness and the policy for accessibility of information and services.

- A third language version of the website is already maintained – in French (in addition to the Bulgarian and English version maintained from the very beginning of the website's functioning). With this, the awareness of the institution's activities and the new developments in the field of personal data protection extends its scope and becomes available to a French-speaking audience.

- In order to modernise and improve the vision of the site, a slider was developed. Its purpose in not only to refresh the appearance of the website, but also to create a tool for focusing on important and up-to-date topics. Currently the main topics emphasised on with the help of the slider are:

    - the General Data Protection Regulation – the awareness of citizens and PDCs of the new European legal framework for personal data protection was a priority for 2017;
    - the forthcoming 40th International Conference of Data Protection and Privacy Commissioners – the preparation for hosing the conference was one of the CPDP objectives in 2017;
    - the Strategy of CPDP for Development in the Field of Personal Data ('Horizon 2022'), adopted and published in 2017.

In line with the Plan for the implementation of Strategy 'Horizon 2022' (item 7 – 'Advanced openness and transparency processes', 'Sustainable-development and management-of-change policy'), as well as due to the increased volume and scope of the information published over the years, in 2017 steps were taken to enhance the internal organisation for maintaining the information on the website. Owners were designated in the individual administrative directorates and departments, and they are responsible for regular reviews of the published information corresponding to the activity of the respective department and, if necessary, for making proposals for supplementing and updating the content or removing any outdated information.

The regular reporting through the website of national, European and international events and initiatives in the field of protection of personal data continued in 2017. The promotion in the maximum volume possible of information on the institution and its activities, the publication of information, educational and explanatory materials in various areas of personal data protection continued. The main international and Bulgarian statutory instruments in the area of human rights and protection and privacy (laws, regulations, directives, rules) are published and maintained up-to-date. The activity of the Commission and the work of European and global forums and initiatives are presented, and public documents of European supervisors and groups are published.

Extremely detailed and up-to-date information about the Schengen area is provided. This is in line with the permanent priority for full accession to the Schengen area, as well as the continued participation of CPDP in Schengen evaluation missions.

In pursuance of the strategic goal for advanced openness and transparency processes, the practice of CPDP is presented in large volumes – anonymised decisions on complaints, opinions, compulsory instructions, decisions of SAC and SCAC on appeals against CPDP decisions are published.

In 2017 the website continued to be part of the means to engage in active dialogue with citizens and PDAs through the forms for submitting complaints through the CPDP's website and the forms for asking questions. Access to standardised forms of communication and interaction with the institution is provided, clear guidelines are 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. Complete and detailed information about the administrative services CPDP provides to citizens is also published.

The CPDP's website provides citizens and PDCs with access to the CPDP information system for registration of PDCs (eRALD). The access is mainly for the purpose of making an electronic registration and for searching the public registers for a specific PDC. For the purposes of group inquiries and re-use of public information from the register, CPDP provides information to the Open Data Portal.

The regular publishing of financial information about the institution (budget; information from the annual financial statements; monthly and quarterly reports on the cash implementation of the budget, the resources from the European Union and other person's resources; information about the payments made by CPDP in the system for electronic budget payments) continued in 2017.

The information bulletin which is issued by CPDP and has its own ISSN 2367-7759 is among the means for public awareness. Six bulletins were issued in 2017. 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 2017, 85 new subscribers subscribed, and the number of subscribers reached 690.

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, which started during the previous year, continued in 2017. As CPDP is a public sector organisation, pursuant to the Access to Public Information Act (API Act) it is obliged to publish the public information it collects, creates and maintains in an open machine-readable format allowing re-use. In 2017 CPDP continued to publish regularly in the Open data portal the following information extracted from the eRALD information system:

- list of PDCs entered in the register pursuant to Article 10(1)(2) of the PDP Act (BULSTAT code/UIC, name of the data controller, type of entity, identification number in the register of PDCs and personal data registers kept thereby);
- list of PDCs exempted from the obligation for registration (BULSTAT code/UIC, name of the PDC, type of entity);
- list of PDCs with denied registration (BULSTAT code/UIC, name of the PDC, type of entity).

Where the PDC is a natural person, his/her PIN is not provided in the lists above.

In 2017, 63 datasets comprising 147 files were published in open machine-readable format CSV. Currently the Open Data Portal does not have a functionality providing information about the number of downloaded public documents.

XV. Administrative Capacity and Financial Resources

1. Administrative Capacity

The ability of 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.

CPDP employs 51 members of staff under civil service relationships and 18 under employment relationships (including the Chairperson and the members of CPDP).

Fife members of staff, of which 3 under civil service relationships and 2 under employment relationships, were appointed during the reporting period. The employment relationships with 10 members of staff were terminated. During the period January–December 2017, 33 members of staff were promoted in rank, and 9 members of staff were promoted in position.

Six competitive procedures for filling vacancies in the CPDP administration were held, 3 of them were completed with appointments, and another 3 were terminated because there were no applicants satisfying the conditions for appointment.

For CPDP, staff training is an important element of the human resources management function. During the reporting period 42 employees increased their professional qualifications by participating in training courses on the Annual Training Plan for 2017, conducted mainly by the Institute for Public Administration. One newly appointed civil servant passed mandatory training.

The analysis of the employees' participation in training workshops revealed that absence from the work process has not affected the performance of the employees' duties. The effectiveness evaluation of the trainings demonstrated a correlation between the training process and the performance of the CPDP's tasks, objectives and priorities.

2. Requests for Access to Public Information and Requests for Re-use of Information

In compliance with the requirements of the API Act, a section 'Access to Information' (subsection of the 'Administrative Service' section) is included in the CPDP's website. It contains:

- Procedure for consideration of requests for access to public information and provision of information for re-use;

- Description of the unit accepting 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 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.

A report on the requests for access to public information and requests for re-use of information received at CPDP in 2017 is presented in the following table:

Total number of received requests for access to information:	**11**
- from citizens of the Republic of Bulgaria;	9
- from foreign citizens;	0
- from media;	1
- from NGOs;	1
- from private individuals.	0
Total number of decisions granting access to public information:	**2**
- full access to public information granted;	2
- 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
Forwarding the request where CPDP does not have the requested information but knows where it is located	**2**
Information provided under the procedure for providing administrative services or in accordance with the procedure of the APC	**6**
Requests which do not comply with Article 25(1) of the API Act in conjunction with Article 2(1)	**1**
Total number of received requests for provision of information for re-use	**1**

In 2017, a total of 11 requests for access to public information were received. Of these, 10 were in writing, and 1 was oral, and an acceptance protocol was prepared. Of the 10 written requests, 5 were received in a hard copy, and 5 were submitted by electronic means. Out of the 11 requests, in 3 a request was made for the information to be provided electronically; in 4 – on a physical carrier; in 1 request three forms of provision were listed, and 3 requests did not contain a specified form for providing the information. CPDP responded to requests in accordance with the requested form of reply, and 2 of the requests were referred to other authorities according to their competencies.

A journalist (Maria Kadiyska from 'Monitor' newspaper) requested wide-ranging information on the CPDP practice in 2017 in relation to the processing of complaints and alerts from citizens as well as on the opinions issued by CPDP – how many complaints and alerts have been received in CPDP; how (letters, by phone, electronically); how many decisions CPDP has taken; how many have entered into force; statistics of received complaints and alerts by settlements; which are the biggest offenders in the processing of personal data; interesting cases; existence of alerts regarding trade in personal data and misuse of personal data; opinions of CPDP in 2017 – in connection with what issues they were issued and what they say.

A representative of an NGO ('Programme Access to Information' Foundation) requested to be provided with information regarding a List of the categories of CPDP information to be published on the Internet and the formats in which this information is available.

Natural persons filed requests:

- to be provided with a certified copy of the CPDP opinion regarding the deletion of names and signatures of employees of administrative structures when published for free access on the Internet;

- to be provided with an uncertified copy of an order of the Chairperson of CPDP for selecting a tenant of a part of a real estate – public State property;

- to be provided with information on the acquisition of a permanent address by CPDP;

- to be provided with information regarding a label, plaque, medal of CPDP – how, when and why they were made, adopted and approved, for what purposes, at what price, how many times they were given, existence of designs, etc.;

- to be provided with information in writing regarding personal data processed by a collection company. The individual was informed of his right under the PDP Act to receive this information from the PDC – the relevant collection company;

- to be provided with information regarding the number of men and women working in CPDP.

The following two requests for provision of information under the API Act, filed by individuals, were referred to other authorities according to their competencies:

- request for access to public information concerning a recording by a video surveillance camera taken by the Municipality of Varna. The recordings made by a specific camera over a specified period were requested. The request was referred to the Mayor of the Municipality of Varna.

- request to be provided with information regarding the transportation of unclassified information and shipments by 'Special Courier Service', as well as clarification which shipments and information are classified and which are unclassified. The request was referred to the State Commission on Information Security (SANS). SANS sent feedback that the request of the citizen was honoured and he was provided with the relevant information.

One request for access to public information from an individual did not comply with Article 2(1) of the API Act, i.e. the requested information was not public.

3. Public Procurement

In order to provide resources for the activities of CPDP in 2017, public procurement procedures were awarded through the collection of tenders with announcement, as follows:

– ‘Reconstruction and internal reconstruction of the administrative building of the Commission for Personal Data Protection (CPDP)’;

– ‘Provision of air and bus tickets for the carriage of passengers and baggage for the business trips abroad of the Chairperson and the members of the Commission and the administration staff, as well as provision of additional travel-related services’;

– ‘24-hour physical security of the building of the Commission for Personal Data Protection, Institute of Defence ‘Prof. Tsvetan Lazarov’, and the parking lot in front of it’, situated at 2, ‘Prof. Tsvetan Lazarov’ Blvd., Sofia, Sofia Municipality, Mladost District;

– ‘Delivery of a new 14+1 seat minivan’;

– ‘Delivery of fuel and accessories for vehicles owned by CPDP through charge cards for cashless payment’;

4. State of Play of the Implemented Information and Communication Systems in CPDP in 2017

Due to the increased volume of document circulation and the need to improve the interaction between different administrative units and the administrative services in CPDP, an upgrade of the existing System for management of documents and workflows in CPDP and control of decisions is carried out. The system was developed and successfully introduced in 2017. Specific functionalities specially tailored to and related to the CPDP needs became operational. As a result, we can point out the significant increase in employee productivity, as well as the possibility of faster and more efficient processing of the documentation. It is important to emphasise on the possibility of ongoing and timely control over the fulfilment of the tasks, in compliance with the necessary measures for preservation of the confidentiality of documents. The additional registers introduced and the easier access to information greatly facilitate the work of the individual units as well as the communication between them.

The drastic reduction of paper documents, the reduction of the time required for performing tasks, and the acceleration of the information flows can be emphasised on as long-term advantages of the electronic document circulation system adopted by the CPDP.

The electronic document circulation system is expected to be brought in line with the uniform technical protocol for exchange of documents in the state administration, approved by the Chairperson of the State e-Government Agency, by May 2018.

The contracts for maintenance of the information systems critical to the activities and processes of CPDP were renewed in a timely manner. Some of the systems were replaced by new ones, and the new systems were commissioned without interruptions to the provided services.

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

During the reporting period, 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).

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

5. Financial resources

The operating budget of CPDP in the amount of BGN 2,450,000 was approved with the 2017 State Budget of the Republic of Bulgaria Act. The CPDP budget was not amended during the year.

The operational expenditure of Commission for Personal Data Protection and its administration amounted to BGN 2,424,562, or 98.96% 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 service contracts	1,207,267
02-00	Other remunerations and staff payments	69,513
05-00	Mandatory social insurance contributions paid by employers	310,019
10-00	Running costs	671,982
19-00	Taxes, fees and administrative sanctions paid	10,485
46-00	Expenditure on membership fees and participation in non-commercial organisations and activities	250
52-00	Acquisition of long-term tangible assets	104,014
53-00	Acquisition of long-term intangible assets	51,032
	Total budget expenditure	**2,424,562**

XVI. CPDP Goals and Priorities in 2018

Given that the new European legal framework on personal data protection applies from 25 May 2018 and taking into account the commitments of CPDP, the Commission for Personal Data Protection sets the following objectives and priorities for the forthcoming reporting period.

1. Successful fulfilment of the commitments related to the Presidency

The international activities of CPDP during the next reporting period will start with the intensive and successful fulfilment of the tasks stemming from the Bulgarian Presidency of the Council of the EU. The most important of these tasks is the conclusion of the negotiations with the European Parliament on the legislative proposal for a new regulation on the protection of personal data in the EU institutions and bodies.

2. Complete readiness for practical application of the new standards in the field of personal data protection

Following the entry into force of the amendments and supplements to the PDP Act, by May 2018 CPDP will focus on developing and/or updating the necessary regulations, which arise from Regulation (EC) 2016/679 of the European Parliament and of the Council and the national legal framework.

In 2018, the work on the development and deployment of an information system for keeping registers in line with the requirements of the General Data Protection Regulation and the changes in the national data protection legislation will continue.

As a continuation of the work on the development of a national training centre, the efforts of CPDP over the next reporting period will be focused on the development of specific training modules for data protection officers, tailored to the specifics of the sectors in which the controllers and processors of personal data perform their activities and the requirements that the new European legal framework places before them. In addition, work on a broad information and awareness campaign on the new regulatory requirements for businesses and public authorities will be intensified.

3. Enhanced international activity at different levels for further reinforcing of the reputation of the Republic of Bulgaria and the Bulgarian supervisor in the field of personal data protection

CPDP will actively focus its efforts on the process of the institutionalisation of the European Data Protection Board established with the General Regulation. The policy of increased involvement of the Bulgarian supervisor in leadership positions in the EU supervisory and coordination structures in the area of personal data protection (Article 29 Working Party/European Data Protection Board, Europol, Eurodac, SIS 2, VIS, Customs Information System) will continue in 2018. To this end, CPDP intends to continue its proactive position on all topical issues of public interest in the field of personal data protection. Adequate administrative and expert resources are required to achieve this. CPDP will continue its efforts in this area.

4. Intensive preparation and successful hosting of host the 40th International Conference of Data Protection and Privacy Commissioners

The intensive preparation and successful hosting of host the 40th International Conference of Data Protection and Privacy Commissioners is another important direction in the forthcoming activities of CPDP. During the forthcoming reporting period CPDP will focus both on formulating topics of present interest in the international context, which will be included in the programme of the event in Sofia, and on providing financing for the event through various partner initiatives.

5. Enhanced assistance and support to data protection supervisors in the Western Balkan countries

CPDP intends to continue in 2018 the process of sharing experience with and supporting the institutional strengthening of the data protection supervisors in the Western Balkan countries.

6. Continuing the work of CPDP for full accession of Bulgaria to the Schengen area

CPDP focuses its efforts on reinforcing the established reputation of the Bulgarian experts in the field of personal data protection by continuing the participation of its representatives in Schengen evaluation missions in other Member States.

7. Creating the necessary conditions for conducting effective control activity in accordance with the enhanced standards in the field of personal data protection at European level

For the purposes of exercising its controlling power, CPDP plans for 2018 activities in two main directions:

- developing up-to-date supervisory mechanisms in the light of the new Regulation 2016/679, including developing different methodologies in line with the current priorities in the control activity;

- effective and efficient supervisory activity, including through validation of professional experience in carrying out sectoral inspections.

The Annual Report of the Commission for Personal Data Protection for its activities in 2017 was adopted by a Decision of the Commission at a meeting held on 10 January 2018 (Protocol No 2).

CHAIRPERSON:

Ventsislav Karadzhov (signed)

MEMBERS:

Tsanko Tsolov (signed)

Tsvetelin Sofroniev (signed)

Maria Mateva (signed)

Veselin Tselkov (signed)