



REPUBLIC OF BULGARIA
COMMISSION FOR PERSONAL DATA
PROTECTION

ANNUAL ACTIVITY REPORT

of the Commission for Personal Data Protection
for 2016

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

TABLE OF CONTENTS

I.	Introduction	5
II.	Analysis of the Degree of Achievement of the Objectives and Priorities of the CPDP set in the 2016 Annual Report	6
III.	Registration of Personal Data Controllers and of Registers Maintained Thereby	11
IV.	Protection of the Rights of Individuals in Relation to the Processing of Their Personal Data	14
V.	Control and Administrative-penal Activity	34
VI.	Personal Data Protection in the Conducted Presidential/Vice Presidential Elections and the Referendum. Analysis of Proceedings	53
VII.	Proceedings for Issuing Opinions and Participation in Legislative Coordination Procedures on Matters Relating to Personal Data Protection	57
VIII.	Provision of Personal Data to Third Countries	70
IX.	New EU Legal Framework in the Field of Personal Data Protection: General Data Protection Regulation and Personal Data Protection Directive	74
X.	International Activity	76
XI.	Training in the Field of Personal Data Protection	82
XII.	CPDP in the capacity of Data Security Supervisor under the Electronic Communications Act	87
XIII.	Institutional Collaboration. Partnership with Media Representatives and Information Activity	91
XIV.	Administrative Capacity and Financial Resources	98
XV.	CPDP Goals and Priorities in 2017	105

List of the acronyms used in this document

PDC	–	Personal data controller
APC	–	Administrative Procedure Code
AC	–	Administrative Court
SCAC	–	Sofia City Administrative Court
SEAV	–	Statement establishing an administrative violation
SAC	–	Supreme Administrative Code
GD GRAO	–	Chief Directorate of Civil Registration and Administrative Services
SAR	–	State Agency for Refugees with the Council of Ministers
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
TSIPC	–	Tax and Social Insurance Procedure Code
PIN	–	Personal Identification Number
EDPB	–	European Data Protection Board
EDPS	–	European Data Protection Supervisor
eRALD	–	CPDP's electronic system for registration of personal data controllers
AVP Act	–	Administrative Violations and Penalties Act
API Act	–	Access to Public Information Act
EC Act	–	Electronic Communications Act
PDP Act	–	Personal Data Protection Act
AASEC Act	–	Act Amending and Supplementing the Electronic Communications Act
MI	–	Mandatory instruction
PACI Act	–	Prevention and Ascertainment of Conflicts of Interest Act

Acc Act	–	Accountancy Act
SF	–	Statement of findings
EWRC	–	Energy and Water Regulatory Commission
QES	–	Qualified electronic signature
CPDP	–	Commission for Personal Data Protection
MoI	–	Ministry of Interior
MoES	–	Ministry of Education and Science
NRA	–	National Revenue Agency
NDB “Population”	–	National Database ‘Population’
RICF	–	Research Institute of Criminology and Forensics
PD	–	Penal decree
CrPC	–	Criminal Procedure Code
RACPDPA	–	Rules on the activity of the CPDP and its administration
RC	–	Regional Court
UniBIT	–	University of Library Studies and Information Technologies
CEC	–	Central Electoral Commission
CFTC	–	Center “Fund for Treatment of Children”

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 1 January 2016 — 31 December 2016.

The Report presents information on the main areas of the activity of the Commission for Personal Data Protection in the reporting period with a focus on the implementation of tasks of major public interest, including registration of personal data controllers (PDCs), control and administrative-penal activities, protection of the rights of individuals, and preventive events and measures. Due attention is paid to activities relating to international cooperation and the new European legal framework in the field of personal data protection. The degree of achievement of the objectives and priorities set for year 2016 is analysed, and the administrative capacity and financial position of the CPDP are reported.

II. Analysis of the Degree of Achievement of the Objectives and Priorities of the CPDP set in the 2016 Annual Report

The main objectives of the Commission for Personal Data Protection and the related priorities for 2016 are arranged in three groups:

- Increased international activity at all levels and in all areas as well as ensuring the fulfilment of international obligations;
- Coordinated approach in areas of high public importance;
- Policy of active dialogue with citizens and personal data controllers.

In 2016, serious progress was achieved in all formulated priority areas under the first objective related to the international activities of the CPDP.

The preparation for the introduction of the new European personal data protection legal framework at national level and the synchronisation of the national legislation with it began immediately after the publication of the General Data Protection Regulation and the Directive on Data Protection in Police and Criminal Justice Activities in the EU Official Journal in May 2016. A detailed action plan of the CPDP with clearly defined tasks, deadlines and responsibilities was adopted as well as an interdepartmental working group was established. The extant legislation which will be affected by the implementation of the new European legal framework was reviewed and the external stakeholders were identified. The CPDP representatives are actively involved in the EU working formats discussions on the preparation process of Member States for the implementation of the new rules.

In order to fulfil the obligation to introduce the figure of the data protection officer in the Bulgarian legislation, on the initiative of CPDP the position ‘Data Protection Officer’ has already been introduced in the Classifier of the Positions in the Administration (State Gazette, No 76 of 30/09/2016). Similar amendments of the National Classification of Occupations and Duties were initiated and expected to be adopted in 2017. In 2016, special attention was also paid to the establishment of necessary conditions for the training and preparation of data protection officers within personal data controllers. In view of the scale of this task, during the reporting period CPDP started the development of a specialised national training centre.

Another important statutory amendment relating to the introduction of the position of the ‘Data Protection Officer’, also implemented on the initiative of the CPDP, is the requirement, set out in the Rules on the Implementation of the Electronic Identification Act, that each entity registered in the Register of electronic identity controllers and centres for electronic identification shall designate a data protection officer pursuant to Articles 37—39 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) (OJ, L 119 of 4.5.2016).

The CPDP representatives are actively involved in the discussions of the Article 29 Working Party (European advisory body for data protection) and the expert subgroups thereto on the implementation of the new EU legal framework and the establishment of the future European Data Protection Board (EDPB) — a new EU body, which will become operational in May 2018, with its own legal statute and power to adopt binding decisions. The Chairperson of the CPDP, who is also a Vice-Chairman of the Article 29 Working Party, is also a member of the management team monitoring the implementation of the action plan for the establishment of the EDPB.

The preparation of the members and employees of the CPDP for the successful implementation of the tasks related to the Bulgarian Presidency of the Council of the EU in the first half of 2018 continued. During the reporting period, the Presidency team members were included in different training programmes, and three employees participated in one-week internships in EU institutions and bodies — the General Secretariat of the Council of the EU, the European Commission and the European Data Protection Supervisor. In addition to getting acquainted with the working processes in these institutions, the representatives of the CPDP received valuable information about the expected legislative programme of Working Party on ‘Information Exchange and Data Protection’ (DAPIX) for the first six months of 2018.

In September 2016 the Commission for Personal Data Protection and the European Data Protection Supervisor officially submitted a joint application to host the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2018. The proposal to host the event included two aspects: a plenary part of the forum planned to be held in Brussels, and two regional meetings in Sofia for the data protection authorities of the Western Balkan countries and the Commonwealth of Independent States. The two capitals and the upcoming events as part of the international conference are planned to be connected through a video conference.

In 2016 the CPDP continued to contribute within its competence for the full accession of Bulgaria to the Schengen area. The Commission was able to fully implement its commitments stemming from the interdepartmental Action Plan on the preparedness for full application of the provisions of the Schengen acquis. The practice of participation of the CPDP members in Schengen evaluations in the field of personal data protection in other

Member States continued. Italy and Malta were the Member States evaluated during the reporting period.

The main group of priorities for achieving the second annual objective of the CPDP operations, namely coordinated approach in areas of high public importance, was related to the control activities of the CPDP.

Primary role among these has the a sectoral inspection of the Education sector carried out in accordance with the Methodology for Carrying out Sectoral Inspections, adopted with a CPDP decision, as well as creating of conditions for uniform application of the data protection rules and formulating good practices in this sector. In the final report on the inspection, specific recommendations for the sector were elaborated and a deadline of 6 months for their implementation was set.

The next priority for the reporting period is related to the implementation of active work for monitoring and supporting the operation of the system for registering refugees and asylum seekers EURODAC in connection with the extremely increased refugee flow across the country. Therefore, in order to evaluate the compliance of the operations of the National EURODAC System with the PDP Act as well as drafting a report to the European Commission, during the reporting period the CPDP conducted inspections at the Research Institute of Criminology and Forensics at the MoI (RICF) and the State Agency for Refugees with the Council of Ministers (SAR). The inspections were closed with the issuing of mandatory instructions.

A detailed analysis of the implementation of these two priorities is included in Section V of the Report.

The CPDP decision for establishing clear rules for the processing of personal data in the course of video surveillance, respectively creating safeguards for individuals — subjects of surveillance had an important point among the priorities in 2016. For this purpose, draft rules prepared by an interdepartmental working group, which aim at establishing common requirements for all entities that process personal data via video surveillance, were being finalised.

Another priority area during the reporting period was the publishing and updating in the Open data portal of public information of public interest collected, created and maintained by the CPDP, the reuse of which has high added value. Amendments and supplements made in 2015 to the Access to Public Information Act introduced an obligation for public sector organisations to publish the public information they collect, create and process in an open machine-readable format allowing reuse. Since October 2016 the CPDP started to publish

regularly in the Open data portal the following information extracted from the eRALD information system:

List of data controllers 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 personal data controllers and personal data registers kept thereby);

List of data controllers exempted from the obligation for registration (BULSTAT code/UIC, name of the data controller, type of entity);

List of data controllers with denied registration (BULSTAT code/UIC, name of the data controller, type of entity).

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

The information published in the Open data portal is updated every two weeks.

One of the CPDP priorities for 2016 under the third thematic area is the implementation of a policy of active dialogue with citizens and personal data controllers. The Commission outlined children as a priority target group for its information activities in 2016, decision based on the sociological survey conducted at the end of 2015 in the field of personal data protection, which demonstrated that there is much to be desired for greater communication coverage of the CPDP among different target groups in society with different social and educational status and age. An information and education short movie for children and adolescents with 10 Internet safety tips was created for the purpose of preventive training on data protection. The information campaign was accompanied by a competition for children's creative works under the motto 'What others know about me?' Detailed information about this initiative is presented in Section XIII of the report.

Other priority areas of active dialogue with citizens and personal data controllers are related to the adoption of the new European personal data protection legal framework. In 2016 the first information and explanatory materials under the General Data Protection Regulation, designed for data controllers and citizens, were prepared and published in the institutional website of the CPDP in different thematic areas, as follows: regarding the rights of individuals, respectively the obligations of data controllers, the consent of individuals and the figure of data protection officers. Training programmes for training events organised by the CPDP already include a separate topic dedicated to the new requirements in the field of personal data protection.

In order to enhance the quality of administrative services provided by the CPDP and its administration after the adoption of the new European personal data protection legal

framework, and in response to the new requirements of Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and the Council, in 2016 a training seminar for the CPDP employees was held. In order to increase the level of competence of the employees of the administrative services units for citizens and administrators, additional specialised training was organised last year. The training provided employees with detailed information regarding the new elements in the amended legislation, the main aim of which is to modernise data protection rules with a view to the rapid development of information technology.

For the purpose of providing active contribution to the successful completion of the initiative of the Bulgarian government for introducing complex administrative services nationwide, during the reporting period Internal Rules on the Administrative Services at the CPDP that fully reflect the new functions of the specialised and general administration of the Commission were adopted. In connection with the amendments to the Access to Public Information Act, a new Procedure for reviewing applications for access to public information was adopted. The Customer Charter was also updated.

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

Pursuant to Article 10(1)(2) of the PDP Act, the CPDP keeps a register of personal data controllers and the registers of processed personal data kept by controllers. The PDC Register is public and is maintained electronically.

The CPDP's activity for maintaining the PDC Register is with the e-Government concept and aims to provide citizens with a highly efficient and user-friendly service based on the 'single window' technology. This activity is performed based on the CPDP's electronic system for registration of personal data controllers (eRALD). The system is a web-based application accessible from the CPDP's website, which supports all PDC registration functions. It enables personal data controllers 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 data controllers.

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

The system is also accessible via the Single Portal for Electronic Administrative Services.

In 2016 the trend of data controllers registering via the Internet, including using a qualified electronic signature (QES), continued.

Between the inception of eRALD in 2009 and 31 December 2016 the number of system users reached 359,048, of which 327,860 applied for PDC registration and 31,188 requested an exemption from the registration requirement (Figure 1).

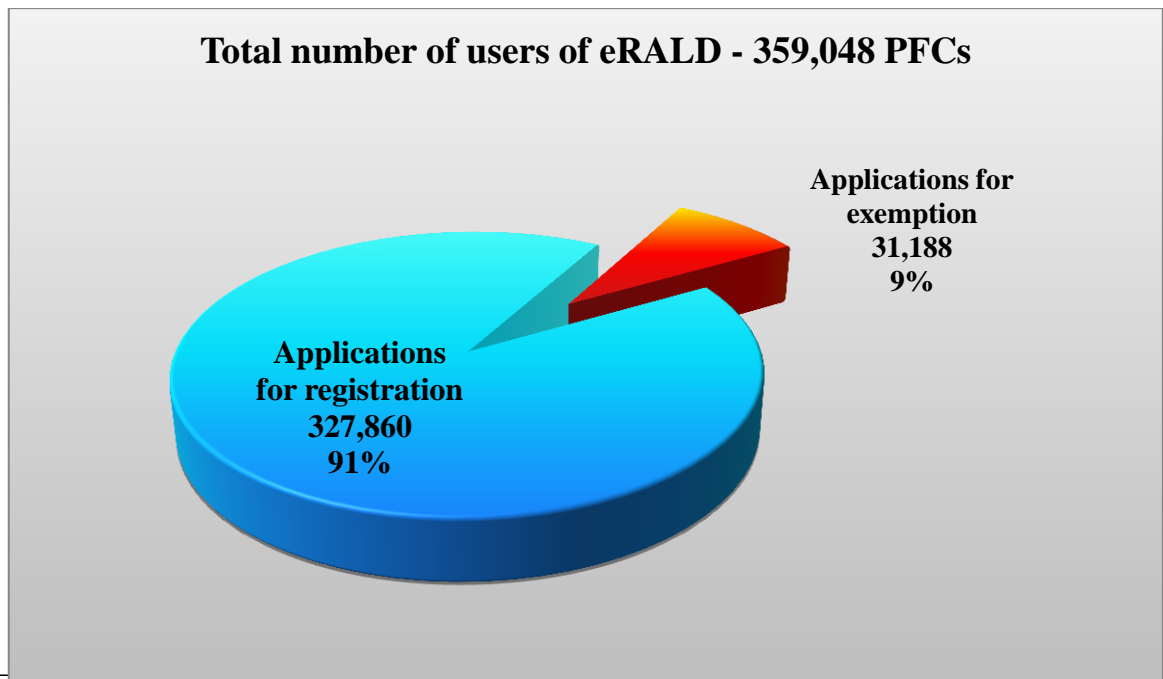


Figure 1

In 2016 CPDP registered 6,176 new personal data controllers. Thus, the overall number of PDCs entered in the register became 284,592 (Figure 2).

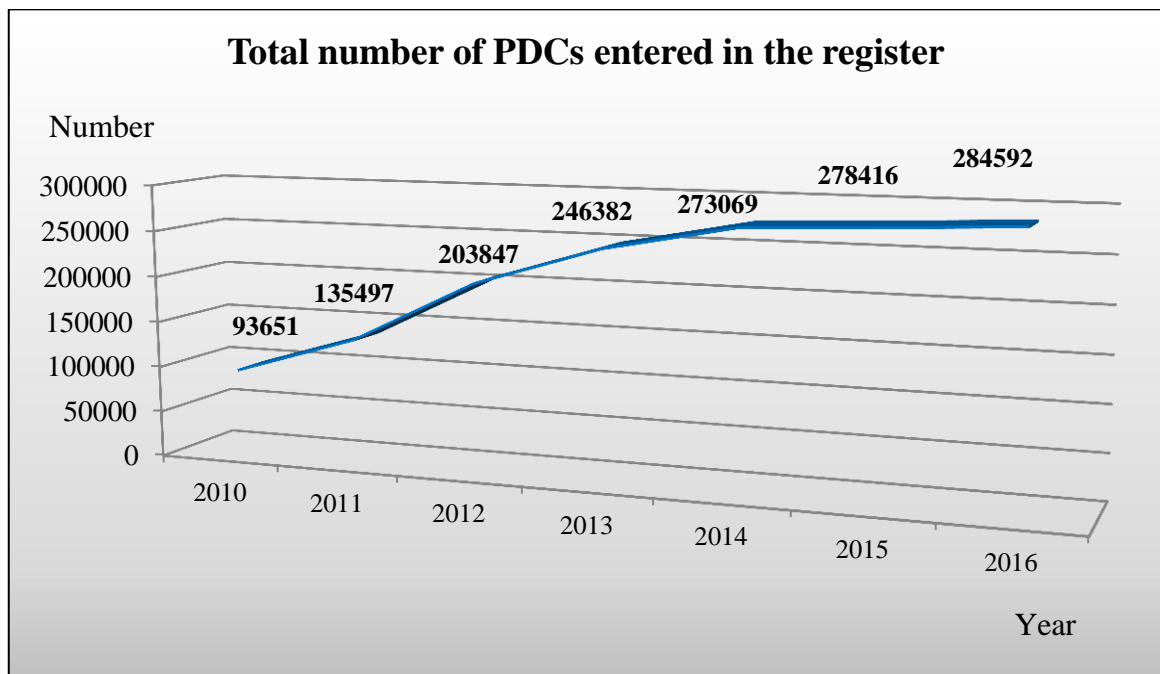


Figure 2

During the reporting period the Commission exempted from the obligation to register 364 PDCs, and their total number as of 31 December 2016 reached 28,035 (Figure 3).

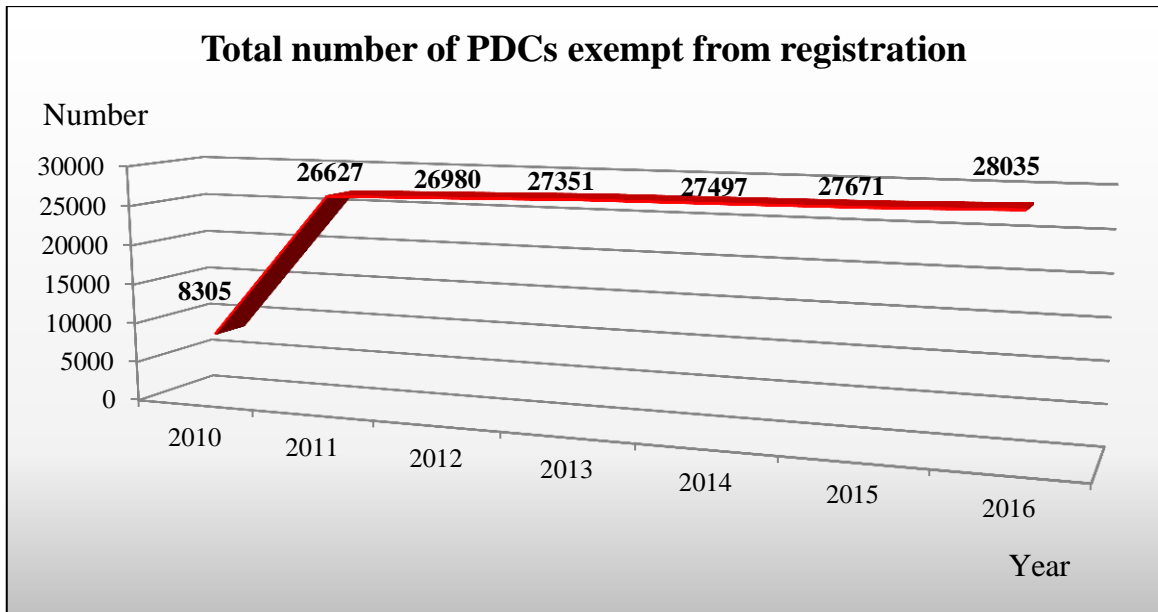


Figure 3

In 2016 CPDP deregistered from the register 70 PDCs, and the total number of deregistered data controllers reached 371.

Where a PDC applies for processing of data falling within the scope Article 5(1) of the PDP Act or in the case of data the processing of which according to a CPDP decision endangers the rights and lawful interests of individuals, the CPDP always performs an ex ante inspection in accordance with Article 17b of the PDP Act before entering the applicant in the PDC Register. During the reporting period, 743 controllers were subjected to ex ante inspections before entry in the PDC Register under Article 10(1)(2) of the PDP Act. As a result of the completed inspections and on the grounds of Article 17b(3)(3) PDP Act, in 2016 CPDP by its decision refused to enter 102 controllers in the PDC Register.

Statistics relating to the registration of personal data controllers and registers kept thereby in 2016 confirms the conclusions made during the previous year, in particular:

- The processes relating to the registration of data controllers 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

General Statistics

The Commission for Personal Data Protection is the only independent government authority in the territory of Bulgaria competent to consider complaints filed by individuals, claiming violation of rights in relation to the processing of their personal data. This competence and jurisdiction stems from the provisions of Article 10 and Article 38 of the PDP Act.

A complaint can be submitted only by an individual claiming violation of his/her rights. In the event that an individual reports violated rights of a third party or of any other violations in relation to the processing of personal data, an inspection according to the procedure established by Article 12 of the PDP Act, can be conducted in connection with the request.

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

No fees are payable for considering complaints by the Commission and in this connection the legal possibilities for protection of rights, provided for in the PDP Act, are available to all individuals.

In recent years a constant upward trend in the number of complaints filed with the Commission is observed.

The total number of complaints filed in 2016, which were considered by the Commission and on which the Commission delivered a decision in the form of an administrative instrument, was 430. The total number of complaints filed with the CPDP during the reporting period was 650. Of these, 220 were related to the Presidential/Vice Presidential elections and the national referendum held during the year. In addition, the Commission reconsidered 9 complaints returned by the court with instructions regarding the application of the law.

Each administrative proceeding for consideration of complaints filed by individuals has the following stages:

- Assessing the regularity of the complaint.

Each request submitted to the Commission shall have the requisites envisaged in law: author, i.e. the individual whose data have been unlawfully processed, and a request addressed

to the Commission in accordance with its competence. Authorship means that the complaint shall be signed and shall contain information about the individual who filed it, including contact information.

During the reporting year the Commission terminated the proceedings on 99 complaints, submitted (including during the previous year) without the mandatory requisites for regularity. It should be pointed out that when an irregular complaint is received, a letter to the complainant with instructions for removing the irregularities is prepared. The instructions are sent to the complainant in the manner in which the respective complaint has been received at the Commission. Only after the instructions are not acted upon within the deadline, the Commission adopts a decision to leave the complaint without consideration due to failure to comply with the requirements of the law.

A trend is observed for filing complaints by electronic means without an electronic signature, as required by the law. Out of the total of 134 complaints filed by electronic means in 2016, only 20 were filed using an electronic signature. It should be noted that the regularity at the time of filing the complaint determines the legality of the administrative instrument issued by the Commission and making a decision on the merits of the complaint.

- Assessing the admissibility of the complaint.

After a regular request is received at the Commission, it is assessed for admissibility of the complaint. To be admissible, a complaint shall be filed by an individual alleging violations of his/her rights under PDP Act, within one year of becoming aware of the violation, but not later than five years of its commitment. It is important for the complaint to be directed against a person having the capacity of data controller. Frequently the Commission receives complaints with allegations of violations made by individuals who do not have the capacity of personal data controllers — neighbours, strangers, ‘enemies’ and others with whom the individual submitting the complaint is in personal conflict. It should be noted that the PDP Act does not apply to the processing of personal data by individuals for their personal or household activities. The number of complaints in this category was significantly lower in 2016 compared to previous years.

In 2016 the Commission left without consideration 89 complaints, including complaints filed during the second half of the previous year, due to their inadmissibility, and in three proceedings the complainants withdrew their complaints thus de-seizing the Commission.

Every admissible complaint is subject to actions for clarifications of the facts and circumstances concerning the violations alleged by the individual by requiring evidence and

opinions from the persons involved in the administrative proceedings, including by carrying out inspections where necessary. Admissible complaints are referred for consideration on their merit in an open hearing and the parties are notified. In the open hearing of the Commission each party involved in the administrative proceedings can provide information and additional evidence and can make evidentiary requests.

- Assessing the merits of the complaint.

After having clarified the facts and circumstances relating to the complaint, the CPDP delivers a decision in the form of an administrative instrument, which is subject to judicial review.

In its decision the Commission could provide mandatory instructions (MIs), set a deadline for eliminating the violation or impose an administrative penalty.

The complaints considered on their merit in 2016 were 206. Of these, 79 were justified and 127 were unjustified.

During the reporting period the Commission imposed 61 administrative penalties for violations established in the course of administrative proceedings and issued 32 MIs to the relevant personal data controllers.

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): 9 violations were established, in respect of which CPDP imposed sanctions in the total amount of BGN 105,500;

- Processing of personal data in the absence of a lawful reason for the data processing operation (Article 4 of the PDP Act): 11 violations were established, in respect of which CPDP imposed sanctions in the total amount of BGN 126,000;

- 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): 26 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 17,400;

- Non-compliance with Article 20 of the PDP Act — failure of the PDP to provide information to an individual where personal data have not been collected from the individual to whom they refer: 3 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 4,500;

- Non-compliance with Article 32 of the PDP Act — the personal data controller failed to respond within the deadline to a request for access to personal data: 1 violation was established, in respect of which the CPDP imposed a sanction in the amount of BGN 1,100;

- Failure of a PDC to assist the CPDP in exercising its supervisory powers (Article 22(5) of the PDP Act): 9 violations were established, in respect of which CPDP imposed sanctions in the total amount of BGN 10,500.

In its practice, the CPDP also rules on resumptions of administrative proceedings and stays of proceedings in view of the existence of preliminary proceedings brought by another body on the same complaint.

Resumption is ruled on complaints which have been stayed with an administrative instrument issued by the Commission.

In 2016 the administrative proceeding on one complaint was resumed, and the complaint was assessed on its merit. The resumption was made at the request of the complainant after the completion of the proceedings by the prosecutor's office.

In the presence of the prerequisites laid down in Article 54(1)(5) of the Administrative Procedure Code (APC) (where other administrative or judicial proceedings were initiated and the instrument cannot be issued before their completion), the CPDP stays the administrative proceedings instituted before it.

During the reporting period the Commission stayed 36 administrative proceedings.

It shall be pointed out that the statistics above included in 2016 proceedings initiated on 9 complaints from individuals concerning the processing of their personal data for registration with the Central Election Commission of political parties and coalitions of parties for their participation in the 2015 elections for municipal councillors and mayors. Two of these complaints were found to be irregular and the administrative proceedings instituted on them were terminated. The administrative proceedings on five of these complaints, considered on their merit in open hearings of the Commission, were closed with decisions declaring them to be unfounded because they were unsubstantiated. The proceedings on one complaint were not completed in view of the applicant's wish, expressed at a meeting of the CPDP, to provide comparative material for the preparation of a signature expert assessment.

Key areas of public life where violations in the field of personal data protection are most frequently observed

The sectors of operation of personal data controllers, against which complaints from individuals were most frequently received in 2016, were as follows:

Political entities — 220 complaints
Telecommunications — 146 complaints
Banks and credit institutions — 62 complaints
Video surveillance — 30 complaints
Judicial and executive authorities — 19 complaints
Electronic services — 15 complaints
Employment and social security services — 14 complaints
Media — 13 complaints
Postal and courier services — 8 complaints
Insurance services — 8 complaints
Provision of services (intermediation, utilities, commerce) — 8 complaints
Healthcare — 5 complaints
Local authorities — 4 complaints
Education — 3 complaints

Specific cases and case-law of the Commission

Video surveillance

Video surveillance as a form of processing of personal data of individuals, regulated by the provisions of the PDP Act, shall be distinguished from the video surveillance as part of security activities pursuant to the rules of the Private Security Industry Act.

The Private Security Industry Act regulates public relations connected with private security, its administrative regulation and control.

The provisions concerning the processing of personal data of individuals through video surveillance are contained in the PDP (Personal Data Protection) Act.

Pursuant to Article 1(1) of the PDP Act, the Act shall govern the protection of rights of individuals with regard to the processing of their personal data.

Pursuant to Item 1 of § 1 of the PDP Act, within the meaning of the Act ‘processing of personal data’ shall mean any operation or set of operations which can be performed with respect to personal data, whether by automatic means or otherwise, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, provision, transfer or otherwise making available, updating or combination, blocking, deletion or destruction.

In this connection, processing of personal data through video surveillance shall be an operation performed with respect of personal data of individuals by technical means.

The powers of the CPDP are set out in a systematic way in Article 10(1)(1) — (13) of the PDP Act. In the specific case, the competence of the CPDP set out in Item 7 of the quoted provision is relevant and is stated, as follows: handle complaints against acts issued or any actions of data controllers, which violate the rights of individuals under this Act.

It is necessary to correctly constitute the parties to the administrative proceedings — complainant and personal data controller.

As far as the complainant is concerned, it is important for the complaint to include alleged infringements of the rights of the individual filing it.

The figure of the personal data controller, as a party to the proceedings before the Commission, shall take into account the provision of Article 3(1) and (2) of the PDP Act and the legal definition of the term, as follows: personal data controller shall refer to any individual or legal person, or a central or local government authority which determines separately or jointly with another person the purposes and means of personal data processing, including where the type, purposes and means of processing are determined by law.

In view of the above, it shall be concluded that the lawful referral of the CPDP shall be in view of the factual processing of the personal data of an individual by a data controller specified in the complaint, with contact details about it.

In addition, the contents of the provision of Article 4(1) of the PDP Act are indicated. Pursuant to this provision, personal data may be processed only in cases when at least one of the conditions set out in Items 1 — 7 of the PDP Act is met.

With regard to the subject of complaints to the CPDP containing allegations of illegal processing of personal data of individuals through video surveillance, the following two factual situations can be distinguished: video surveillance carried out in condominiums, and video surveillance carried out by an individual for personal and household activities.

Video surveillance carried out in condominiums

This hypothesis covers the provisions of the Condominium Management Act, which regulate the powers of the General Meeting as a management body of the condominium.

The General Meeting adopts decisions regarding the costs that are necessary for maintaining the common areas, including the placement of advertisements or installing technical facilities in the building.

The lawful holding of general meeting of condominiums is guaranteed by the requirement for a certain quorum, i.e. if owners of at least 67 per cent of the shares of the condominium are present personally or through representatives.

In this sense, the necessary presence of the owners in view of the regularity of the General Meeting is established.

In relation to the matters to be resolved on by the condominium, the decisions shall be adopted by a majority of more than 50 % of the represented shares of the common areas of the building or by a qualified majority for some decisions, the subject of which is not related with the installation of video cameras.

It is noted that the authentication of documents, such as the minutes of the General Meeting, together with the list of residents certifying their presence by their signatures, as in the case, is outside the competence of the administrative body and is within the jurisdiction of the respective court.

Video surveillance carried out by an individual for personal and household activities

Pursuant to Article 1(9) of the PDP Act, the Act does not apply to the processing of personal data by individuals for their personal or household activities.

In this connection, the judgement of the Court of Justice of the European Union in case C-212/13 — Reference for a preliminary ruling regarding the interpretation of Article 3(2) of Directive 95/46/EC — Concept of ‘in the course of a purely personal or household activity – recording with a video surveillance camera of the entrance to home of the individual using the recording system, the public footpath and the entrance to the house opposite’, as formulated in the conclusion of the Attorney General, is relevant.

In view of the fact that this judgement of the Court of Justice of the European Union is binding upon the national court that referred the specific case to it, the EU institutions and Member States, and that all of the above are obliged to interpret the legal norm exactly in the sense of the judgement of the Court of Justice of the European Union, the CPDP has considered that the following opinion is applicable: ‘The second indent of Article 3(2) of 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 must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of

protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision”.

The CPDP practice in relation to the hypothesis considered corresponds to the meaning of the aforementioned judgement of the CJEU, i.e. in a factual situation where the captured space is outside the property of the individual who installed the video cameras and covers public spaces or common areas of a condominium, it is assumed that video surveillance is unacceptable.

The reasons of this conclusion are related to the principle of relevance, connectivity and not exceeding the purposes for which personal data is processed, which is violated in this case.

In the event of establishing a violation of the rights of an individual, the CPDP shall issue a decision and can give mandatory instructions, set a time limit for the removal of the violation or impose an administrative penalty.

According to its competence and exercising its powers in the conditions of operational autonomy, the administrative authority is of the opinion that the purpose of the law is achieved by issuing mandatory instructions for dismantling the respective video surveillance cameras within a certain period (usually 14 days) from the date of entry into force of the decision, for which the personal data controller shall provide relevant evidence.

In connection with the entry into force of the decisions of the CPDP as administrative instruments it is noted that they enter into force if they are not appealed within 14 days of their receipt by the parties to the proceedings or after they are confirmed by the courts, which are two — the Sofia City Administrative Court (SCAC) and the Supreme Administrative Court (SAC).

Processing of personal data for the purposes of journalism

As far as the law does not contain a legal definition of journalism, the practice assumes that it is an activity aimed at gathering the necessary information on cases of public interest, checking its credibility and informing members of the public about them.

The PDP Act allows the assessment of the existence of ‘processing of personal data for the purposes of journalism’ to be made by the personal data controller or the data protection authority — the CPDP, respectively the administrative court, insofar the CPDP decisions are appealed before the latter. This is the case because the regulations do not provide for specific criteria to determine the extent, to which the processing of personal data

is for the purposes of journalism, and where these purposes are exceeded. The only condition is that such processing shall not violate the right to privacy of the person to whom such data refer. This makes it necessary to make an assessment on a case-by-case basis so that the processing of personal data is lawful.

The main issues to be addressed when assessing the lawfulness of the processing of personal data for the purposes of journalism are whether the published information constitutes personal data and whether the processing of such data in the specific case constitutes a violation of the law, also taking into account the provision of Article 4(2) of the PDP Act.

The requirements for a good quality journalistic investigation involving publication of verified information shall comply with the provisions of Article 2(2)(3) of the PDP Act, pursuant to which processed personal data shall be relevant, proportionate to the purposes for which they are being processed and not exceeding their scope.

The **publishing of documents** is one of the forms of visualising journalistic articles. The practice of the CPDP, confirmed by the case law, clearly imposes upon publication of documents containing personal data of the individual — subject of journalistic investigation the deletion of data that exceed the needs of journalism. For example, when investigating participation in commercial companies or ownership of real estate, it is not necessary to disseminate personal identification numbers, addresses, ID card numbers, etc. contained in the relevant documents. The existence of personal data in a volume exceeding the journalistic purpose entails administrative and penal liability for violation of the principles of processing of personal data, specified in the provision of Article 2(2) of the PDP Act.

The **publishing of photographs of individuals** as a journalistic method for visualisation is also subject to assessment of the existence of personal data processing and of the compliance with the requirements of Article 4(2) and Article 2(2) of the PDP Act.

It is an established practice that the use of information relating solely to displaying the appearance of an individual not accompanied by additional information does not make such individual ‘recognisable’ to an indefinite circle of persons, since the presentation of the person’s appearance shall not be treated as information relating to his/her personal and intimate life the access to which can be regulated. The social life and contacts of each individual in themselves imply access to this information of an unlimited number of persons. At the same time, the fact that relatives and friends of the individual recognise him/her does not lead to the conclusion that such personal data regarding him/her have been used, that would lead to his/her indisputable identification in the public domain by all other persons outside his/her acquaintances, family, friends, and colleagues.

To identify an individual, the presentation of certain personal data about him/her shall be in such a volume as to allow his/her identification, and the presentation of only certain attributes such as two names or the image of the face of a non-public person is not sufficient.

Processing of personal data of officials

In the practice of the CPDP, it is often necessary to assess the extent to which the processing of information related to the position and official duties shall be penalised.

An example of this is the case of publishing the name and position of an individual in a 'Reports of completed cases', maintained by an administrative court, where the three names and the abbreviated position of the individual are published and freely accessible. At the same time the personal data of other parties — complainants and respondents on other cases, are anonymised, and such individuals are shown in the report with their initials.

In view of the specificity of the particular case concerning a person holding a public position — a public enforcement agent, the processing of personal data is lawful within the hypothesis of Article 4(1)(5) of the PDP Act, namely the processing is necessary for the performance of a task carried out in the public interest.

The public enforcement agent is a public authority and the public must be informed exactly to whom the state has assigned the respective functions and how they are implemented. The assignment of each function of state authority requires identification of the individual to whom it is assigned. In this connection, the names of public enforcement agents are published in the website of the relevant regional court.

In view of the nature of the position occupied by the individual, to which the case at stake in which the complainant is referred to as a party is related, it is concluded that the data regarding the full name and position are information based on which the public is to reach an opinion on the activity of the institution — public enforcement agent, by identifying the individual performing it.

The balance between the right to information and the public interest, on the one hand, and the protection of personal data, on the other hand, is also assessed. The role of a person in public life justifies the priority interest of the public in having access to information relating thereto, and individuals in the capacity as state bodies shall be subject to more transparency and criticism. The case law of the Constitutional Court of the Republic of Bulgaria is along these lines. According to it, the protection of the personal data of persons occupying public positions, including enforcement agents, is much lower compared to the protection of the rest of the citizens. In this regard, the processing of their personal data, individualising them as

authorities, in particular the information regarding their names and the positions they occupy, is necessary so that citizens can reach an opinion on the activity of the entities obligated by law.

Access to documents containing personal data

Frequently the exercising of the right under Article 38(2) of the PDP Act to approach the CPDP is used to obtain access to documents, respectively the personal data contained therein, created for the exercise of powers of state bodies.

The provision of Article 28(1) of the PDP Act specifies the objective limits of the right to access under Article 28(1) of the PDP Act. None of the three hypotheses exhaustively defined by the legislator provides for an obligation of the personal data controller to provide copies of instruments drawn up within the framework of its statutory activity.

The access to any other information, including documents, shall be provided in accordance with the special law based on which such information has been created, for example the Child Protection Act and the Implementing Regulation of the Child Protection Act. In the specific case it shall be emphasised that the official documents drawn up during the work of the relevant authorities are not independent in their nature and that the term ‘copy of personal data’ is not identical to the term ‘copy of documents’.

The aforementioned is supported by the manner in which the obligation of the personal data controller to provide information is stipulated in Article 31(1) of the PDP Act. The latter states that the information subject to access to personal data ‘may be provided as an oral or written reference, or in the form of the data review by the individual concerned or by another explicitly authorised person’.

The issue with the right to access to personal data, regulated in this way, stems from the provision of Article 31(2) of the PDP Act, which states that: ‘The individual may request a copy of the personal data processed on a preferred carrier or by electronic means, unless this is prohibited by law’.

According to the CPDP opinion No D-283/2013, the term ‘copy of personal data’, interpreted as a ‘copy of documents’, practically does not correspond to the idea of the nature of the information subject of access, as defined in Article 28(1) of the PDP Act.

Based on the legal definition of ‘personal data’ in Article 2(1) of the PDP Act and § 1, Item 16 of the Additional Provisions of the PDP Act, it shall be stated that the term ‘copy of personal data’ shall not be treated as identical to the term ‘copy of documents’.

Numerous statutory instruments dealing explicitly with the term ‘copy of documents’ and respectively regulating the access to them are in place, and in this respect copies of documents shall be provided by the personal data controller in accordance with the procedure provided for their creation, storage and access.

2. Case law relating to appealed decisions of the CPDP

In 2016, the Sofia City Administrative Court (SCAC) initiated 59 cases on appeals against administrative instruments issued by the CPDP. The Supreme Administrative Court (SAC), in the capacity of appellate court, dealt with fifty-seven (57) cases.

During the reporting year, sessions of panels of the SCAC were scheduled for 73 cases, of which 14 cases initiated in 2015 and 48 cases initiated in 2016. It shall be noted that 11 of the cases initiated before the SCAC in 2016 were scheduled for consideration in 2017.

A total of 105 cases, initiated in prior years, were finalised in 2016 by the SCAC with a court judgement.

The information available shows that 72 judgements confirmed the appealed administrative instruments of the CPDP. In 12 of them the court decreased the penalty imposed by the Commission. In 32 judgements the instruments issued by the Commission were cancelled.

The figure (Figure 4) shows the number of confirmed and cancelled decisions of the Commission:

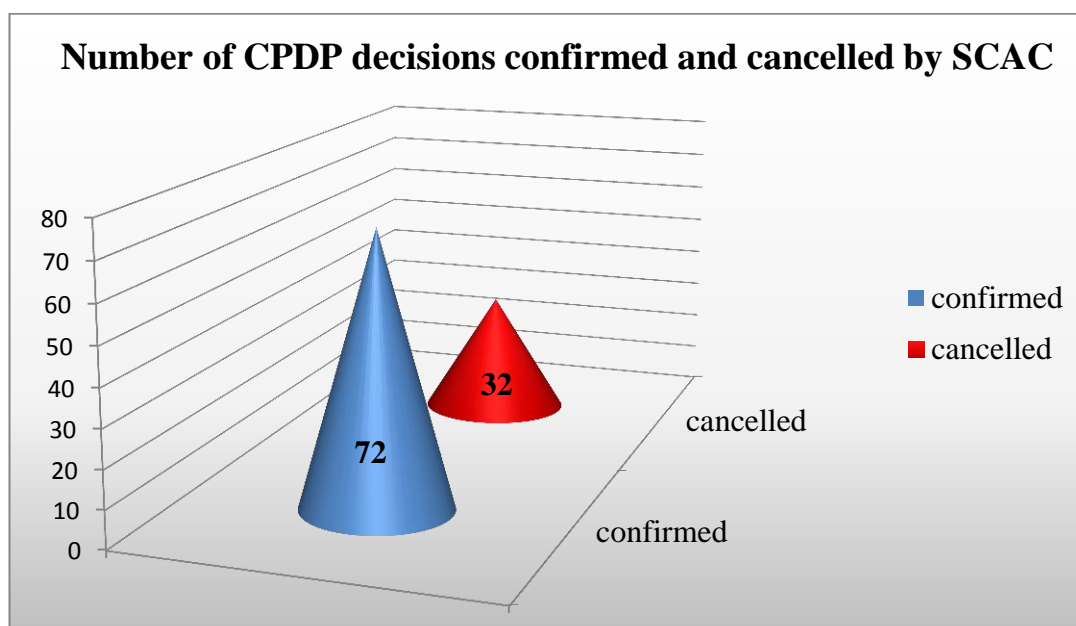


Figure 4

In 2016, the SAC held sessions on 39 cases, of which 38 cases initiated in 2015 and only 1 case initiated in 2016. All remaining cases initiated in 2016 were scheduled for consideration by the end of 2017 and 2018.

In 2016, the SAC ruled on 37 cases, initiated in 2016 and prior years. As a result of the two-instance judicial review, 22 decisions of the CPDP were confirmed, and 15 decisions were cancelled.

In view of the final result, the practice of the SAC with regard to instruments issued by the CPDP can be expressed graphically as shown below (Figure 5):

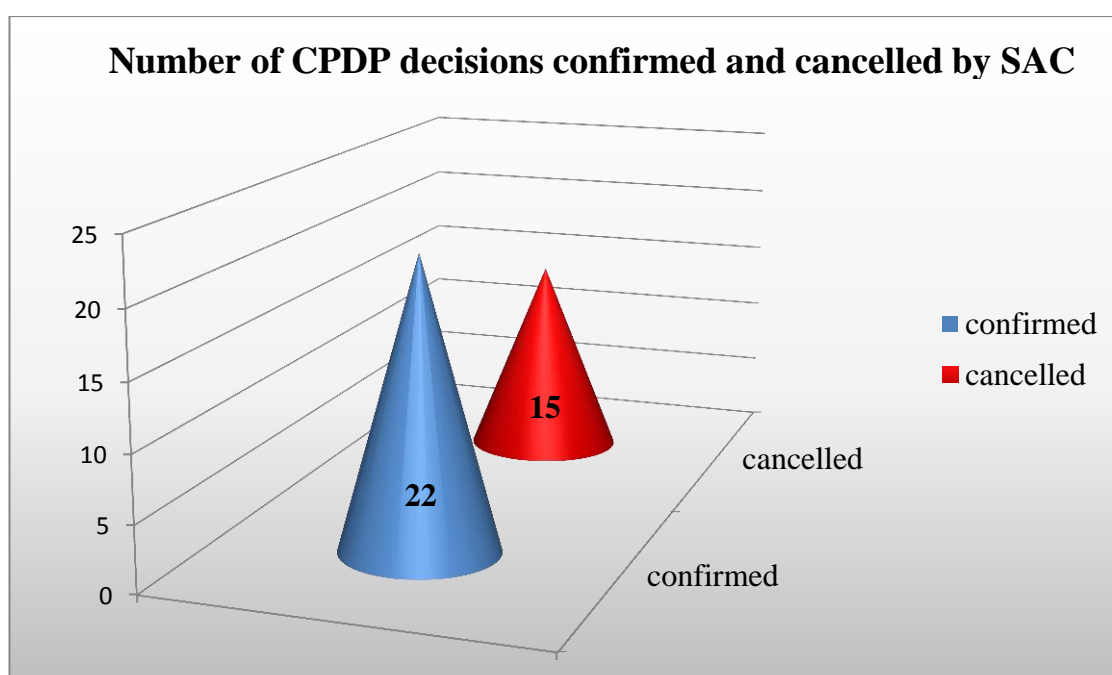


Figure 5

Statistics of the imposed and collected public receivables stemming from the CPDP decisions

The penalties imposed by the CPDP decisions in 2016 amounted to BGN 265,000. The amounts collected pursuant to the CPDP decisions in 2016 came to BGN 150,270.50, of which BGN 10,687.50 were collected coercively by the NRA.

Consultations provided to citizens

The CPDP has provided different opportunities for consultations with experts from its administration. This makes it easier for citizens to address the Commission even when matters are not within its competence and authority. In such cases files are forwarded to the relevant institutions so that they can take action according to their competencies.

Experts are available for communication via e-mail, by phone and in the building of the Commission. The most common matters in 2016 were related to the provision of personal data by data controllers to foreign natural persons and legal entities or foreign state bodies. The emphasis is mainly on the provision of personal data of individuals where an adequate level of protection and standard contractual clauses exists. Questions are related to the procedure to be followed and the requirements to be met by data controllers when providing the data.

Multitudinous inquiries received in writing related to the scanning of identity cards by banks as well as to the obligation of Internet merchants to register in the Register of Personal Data Controllers and the Registers Kept Thereby.

During the reporting period the CPDP received a written inquiry relating to the development of spyware collecting information from phones, such as: contacts, calls, SMS, browsing history, etc. The question concerned ways of legalisation the software. The response of the CPDP stated that pursuant to Article 32 of the Constitution of the Republic of Bulgaria, privacy of citizens is inviolable. Every individual has the right to protect against unlawful interference with his/her personal and family life and against encroachment on his honour, dignity and reputation. No one can be followed, photographed, filmed, recorded or subjected to any other similar actions without his/her knowledge or despite his/her explicit disagreement except in the cases provided for by law. All data relating to a particular individual, whether individually or in a particular set, fall within the definition of “personal data” within the meaning of the PDP Act if they lead or could lead to a unique identification of the particular individual. Personal electronic communication (e-mail, chat, SMS) is correspondence and its secrecy is inviolable, unless otherwise provided for in a court ruling.

The trend continues to be the same both in 2014 and 2015, and in 2016: a large group of questions are 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 Commission’s position on these cases is related to the accounting for this service as a basis for admissibility of personal data processing. Article 7(1) of the Accounting Act defines the scope of information required for primary accounting documents. Article 7(1)(3) of the Accounting Act specifically provides that primary accounting documents must contain the issuer’s and the recipient’s name, address and identification number referred to in Article 84 of the Tax and Social Insurance Procedure Code (TSIPC). Pursuant to Article 84(2) of the TSIPC, individuals who are not registered in the Commercial

Register or in the BULSTAT register are identified by their Personal Identification Numbers if they are Bulgarian citizens or Foreigner Identification Numbers if they are foreigners.

In 2016, there were numerous inquiries related to the provision of personal data by mobile operators to the so-called 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.

Questions related to the functioning of websites known as online gaming sites, which require registration of pre-purchased tickets, continue to be raised.

Most frequent questions concern the lawfulness of the mandatory fields in registration forms, where users are required to fill in their personal data such as full name, address and PIN. Following each particular inquiry, provided that the inquiry contains sufficient information, the CPDP experts in the first place check the online game operator in the Electronic register of the CPDP.

If the operator is registered in the eRALD, the citizens are informed that the required entry of PIN during the user registration in the website constitutes 'processing of personal data' on the part of the PDC in accordance with the legal definition in § 1(1) of the Supplementary Provisions of the PDP Act. Each data controller has a duty to process the personal data lawfully and in accordance with the provisions of the PDP Act, wherein Article 4(1) the Act defines exhaustively the situations in which personal data of natural persons can be processed. Item 2 of the said Article 4(1) of the PDP Act provides that it is lawful to process personal data when the natural person, whom the data relates to, has explicitly given his or her consent. By the mere entry of his/her PIN, the online gamer is assumed to have given the required consent. It is also important for citizens to know that Article 23(1) of the PDP Act requires the PDCs to apply appropriate technical and organisational measures in order to protect the data against accidental or illegal destruction, or against accidental loss, unauthorised access, modification or dissemination, or against other illegal processing.

If the ex-officio check establishes that the operator is not registered as a personal data controller or has not applied to the CPDP for registration in the electronic register, the case is referred to the Legal Proceedings and Supervision Directorate for them to take appropriate steps.

The questions relating to the registration of personal data controllers were the most numerous in 2016 as well. From the perspective of the PDP Act, when a person conducts commercial operations in the territory of the Republic of Bulgaria, collects and processes personal data of individuals and keeps registers, containing personal data, such person falls within the scope of the definition of personal data controller set out in Article 3(1) of the PDP Act.

All persons that process personal data and keep registers of information constituting personal data are obliged to register as personal data controllers. 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 file containing personal data of former employees. If the personal data controller is already registered, the registration shall be updated upon each change in the circumstances relating to the person.

In 2016, a large number of questions from citizens and legal entities were received at the CPDP via different channels. The questions relating to the implementation of the obligations of personal data controllers prevail – for registration, for providing technical and operational measures for protection, for provision of the required information, and for safeguarding the rights of data subjects.

The CPDP frequently receives questions relating to the competencies of the Ministry of Interior (MoI) authorities and the processing of personal data in connection with the performance of their duties.

For example, inquiries were received from citizens regarding the competence of the police to summon people by phone, including through their relatives.

The MoI authorities process personal data pursuant to the provisions of Article 4(1)(6) of the PDP Act, i.e. where the processing is necessary for the execution of competences vested by law in the data controller or in a third party to whom the data are disclosed.

The Ministry of Interior Act (MoI Act) regulates the principles, functions, activities, management and structure of the MoI and the status of its employees. Pursuant to Article 4 of the MoI Act, state bodies, organisations, legal persons and citizens shall be obliged to provide assistance and to comply with the instructions of the MoI bodies issued in the course of or in

connection with the exercise of their legally assigned functions. Pursuant to the provisions of Article 69 of the MoI Act, the police bodies may summon to the official premises citizens in order to exercise the legal powers, assigned to them by the Act. The police bodies shall inform the citizens in writing about the summons. The summons shall state explicitly the purpose of the summoning, the time and the place of appearing.

Paragraph (3) of the same Article 69 provides that **in urgent cases, summoning may be made by telephone or fax**. Summoning by telephone or telefax shall be attested in writing by the official who has done it.

During the reporting period, the number of received inquiries by citizens regarding the storage of and access to medical records, as well as the choices in the exercise of patients' rights, increased considerably. Difficulties arise from the fact that there is a wide variety of legal instruments governing the protection of medical records and the data on the health of individuals contained therein. An interesting inquiry was made by a foreign partner in connection with a request of an airline operator (employer) to access the results from the medical tests of crews (employees and workers).

An analysis of the applicable legislation revealed the existence of a special ordinance issued in accordance with Commission Regulation (EU) No 1178/2011 of 3 November 2011, providing for an explicit procedure for access to medical records in files of pilots and crew. The Ordinance provides for the establishment of the Aeromedical Section (AMS) to General Directorate 'Civil Aviation Administration', competent on matters of aviation medicine and aviation personnel. Access to records, containing medical information about aviation personnel, is made through the Aeromedical Section in compliance with the rules explicitly set out in the ordinance. The persons entitled to direct access do not include employers. With regard to the employer (the airline operator), the general provisions of the PDP Act for access to medical records apply. The employer has the right to receive information regarding the health of an employee only to the extent necessary to fulfil its obligation to ensure health and safety at work as well as its obligations under the labour and social security legislation.

Copying of identity cards is a problem that does not lose its relevance. It shall be noted that no explicit provision exists in this respect and each inquiry is considered on its merits. However, there is no clear, explicit ban on the copying of identity documents either. On the contrary, certain statutory instruments expressly stipulate the copying of identity documents as part of the facts and circumstances of a particular administrative or another procedure (for example, the Measures against Money Laundering Act). This is necessary

because the identity document identifies individuals in an indisputable manner and in the cases prescribed by law guarantees the security of the civilian turnover.

The CPDP frequently receives letters containing questions regarding the revealing the secret of adoption. Bearing in mind that the process is related to access to the National Database 'Population' (NDB 'Population'), kept by Chief Directorate of Civil Registration and Administrative Services at the Ministry of Regional Development and Public Works (GD GRAO), in certain cases the CPDP gives permission for access to such information. One particular case is different, as there are special provisions restricting access. The provision of Article 105(1) of the Family Code states that adoptive parents or adopted children who have reached the age of sixteen years may ask the district court which has passed the decision to grant adoption to be informed of the parentage of the adopted person when important circumstances so require. In a closed court session, after hearing the birth parents of the adopted person and the prosecutor's conclusion, the district court makes a ruling. Therefore it is the court that, by its ruling, allows the provision of information regarding parentage. Currently, proposals for amendments to the Family Code, which envisage easing the procedure in question, are being discussed, and experts from the CPDP follow the discussion.

The questions received by the CPDP in 2016 were many and of diverse nature. Citizens have been actively seeking assistance and explanations in relation to the application of the PDP Act. This is equally confirmed by the statistical analysis of the 370 answers given by the Commission.

An important communication channel for direct communication with citizens and improving the quality of services is the Centre for Information and Contacts (Call Centre) of the CPDP. Its goal is to satisfy inquiries by providing as full information as possible from the very first call. In 2016, 5,926 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 centre as an opportunity for direct contact with the Commission experts. The average monthly number of calls to the Centre for Information and Contact is approximately 494, with a large percentage of inquiries being related to the registration of data controllers. A major problem with registration is that applications for registration are often not properly filled in. In such cases support from the operators in the Centre for Information and Contact is required.

Frequently asked questions are whether the data controller can begin processing personal data of individuals after making a registration with the CPDP. Another frequent

problem is the signing of the so-called confirmation sheet with a qualified electronic signature (QES). Such a problem arises most frequently from a discrepancy between the data signed with an electronic signature and the data filled in the application for registration. This shows that a significant part of the data controllers are not adequately informed about the registration process despite the efforts made by the CPDP to provide the necessary instructions on its website.

Next is the issue of processing of data under Article 5(1) of the PDP Act, which by virtue of the law is subject to a preliminary inspection prior to entry into the register by the Commission. Frequently errors are made in this respect as well.

Recently, there was a boost of online marketing, and this year inquiries continued regarding whether companies that sell online products over the Internet shall be registered as data controllers, and if they can provide personal data in the European Union and in third countries. In such cases inquiries are referred to the experts in the specialised administration of the Commission.

The Centre for Information and Contacts receives calls relating to difficulties in the drafting of the Data Controller Instructions in accordance with the requirements of the Commission. Applicants request an example of instructions and criteria for defining different levels of personal data protection.

The issues concerning the misappropriation of personal data in the lists submitted to the Central Election Commission (CEC) by initiative committees and parties in connection with the Presidential/Vice Presidential elections of Bulgaria in 2016 and the national referendum are equally important. A large part of the inquiries to the call centre concern the procedure for filing complaints with the CPDP, and the average weekly number of inquiries relating to the matter was 160.

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

- Regarding the registration of personal data controllers, 1,464 inquiries with a frequency of approximately 122 inquiries a month were received;

- Regarding the issuing of certificates to personal data controllers — 1,356 inquiries with a frequency of approximately 113 inquiries a month;

- Regarding the signing of the confirmation sheet with an electronic signature — 650 inquiries with a frequency of approximately 54 inquiries a month;

- The inquiries regarding user names and passwords for logging into the system of the electronic register — 455 inquiries with a frequency of approximately 38 inquiries a month;
- The inquiries regarding changes in personal data registers — 355 inquiries with a frequency of approximately 30 inquiries a month;
- Regarding the registration as PDCs of companies selling online products over the Internet — 310 inquiries with a frequency of approximately 26 inquiries a month.

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 Rules on the activity of the CPDP and its administration (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 the CPDP and specially authorised officials from the specialised administration — Control and Administrative-Penal Proceedings Department of the Legal Proceedings and Supervision Directorate. Where necessary and depending on the subject and the tasks of the inspection, employees from other departments/directorates of the Commission are additionally authorised and take part. The activity relating to this type of control includes inspections of personal data controllers 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.

Inspections end by the issuance of a statement of findings, and depending on the findings therein, a proposal for issuing a mandatory 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 2016, 844 inspections were initiated, of which:

- 750 ex-ante inspections;
- 26 ongoing inspections;
- 68 ex-post inspections;

The total number of inspections carried out (Figure 6), including finalised inspections initiated in 2015, was 712. Of these:

- 609 ex-ante inspections;
- 29 ongoing inspections;
- 74 ex-post inspections.

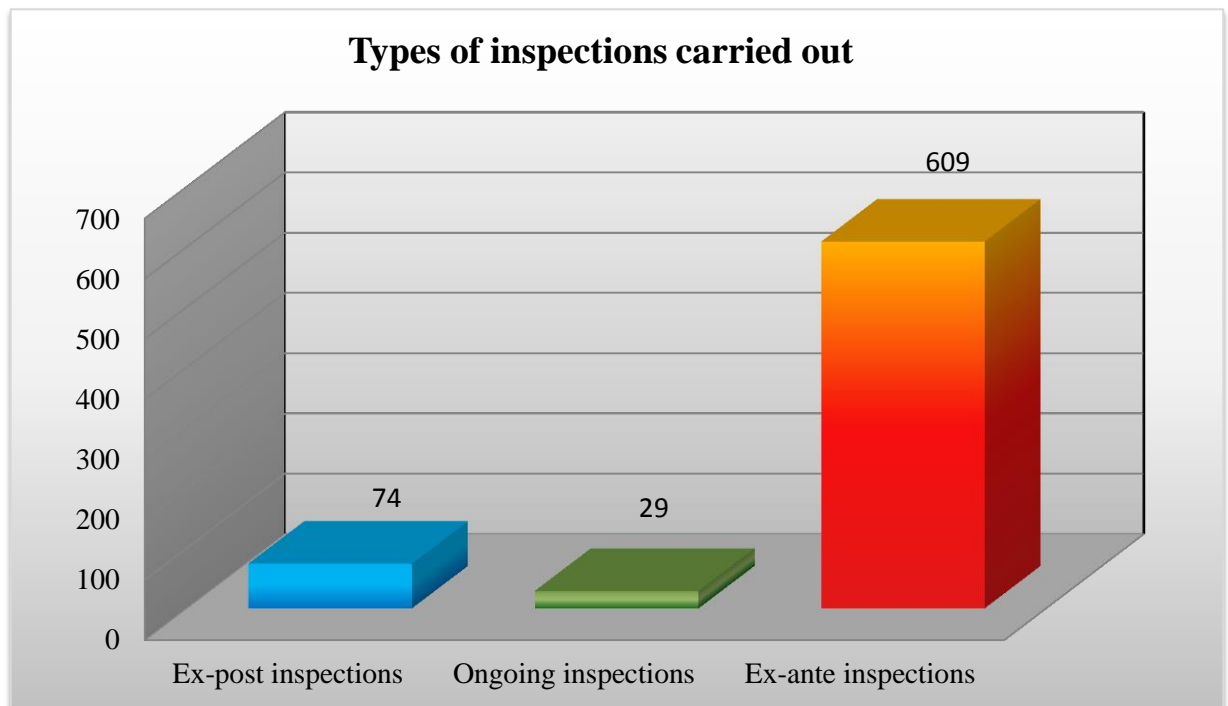


Figure 6

The 712 inspections carried out resulted in the issuance of 674 statements of findings and 6 mandatory instructions, and 50 inspections were completed with the issuance of statements establishing administrative violations.

Comparative statistics of assigned and completed inspections (ex-ante, ongoing, ex-post) is presented in the following figures (Figure 7 and Figure 8):

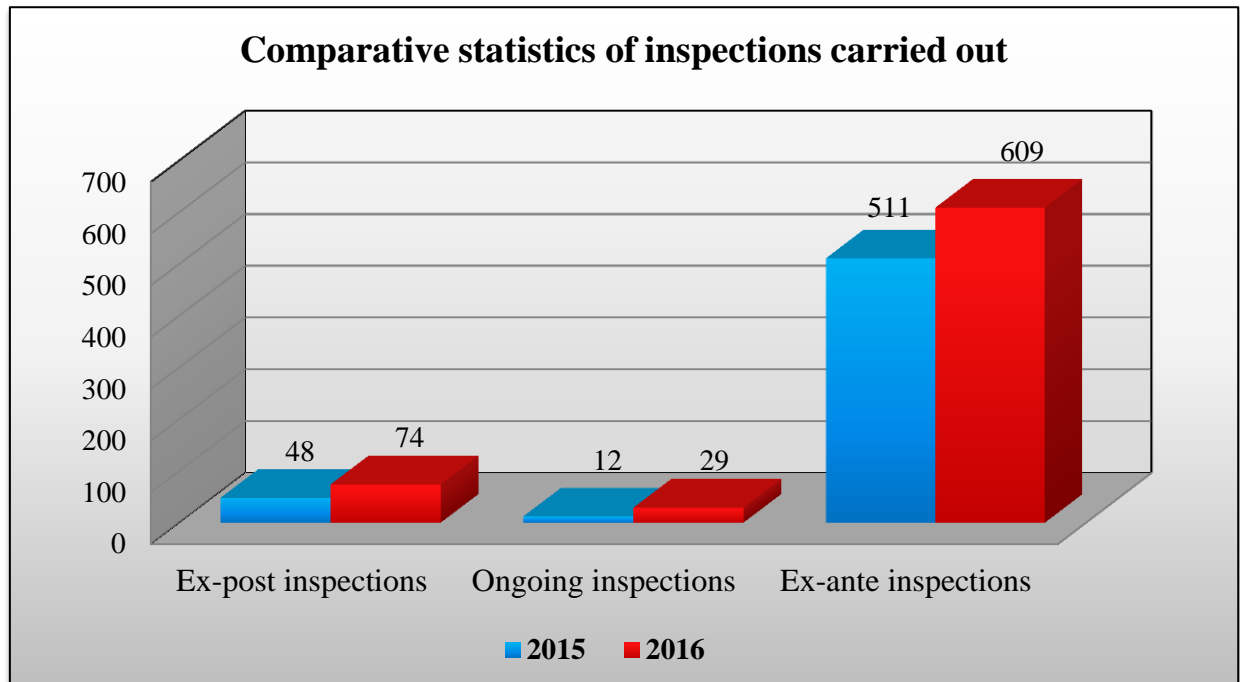


Figure 7

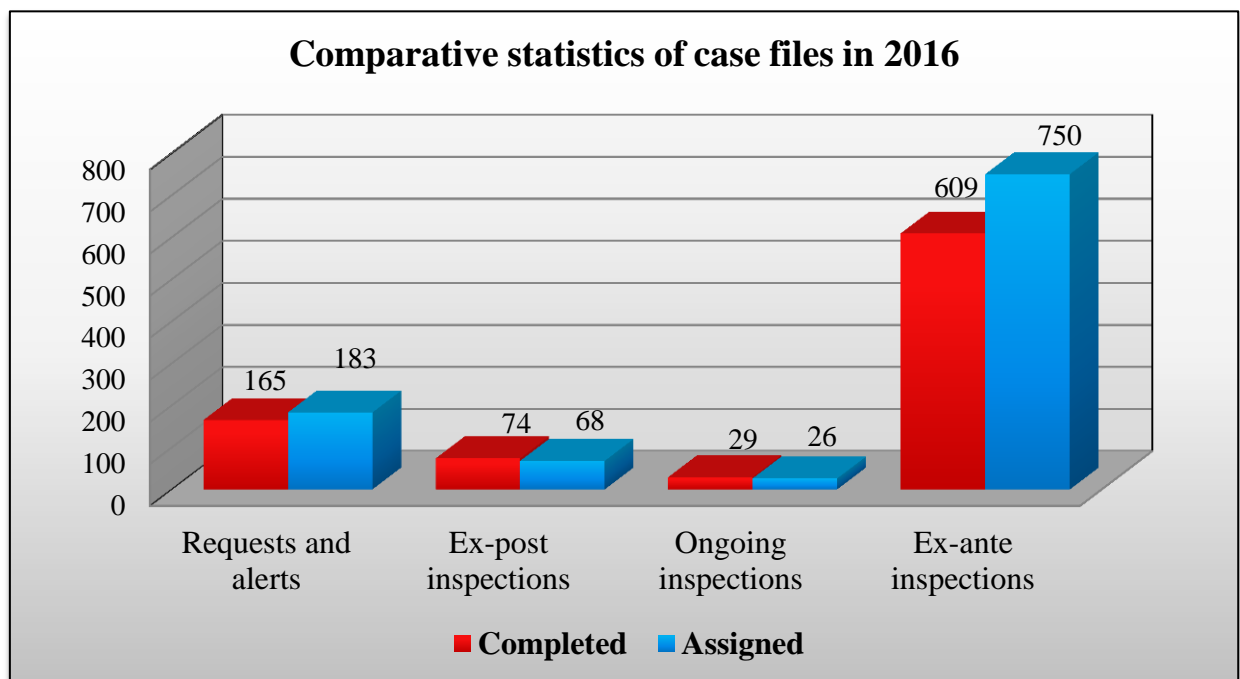


Figure 8

The comparative statistics above 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 of speed and timing in dealing with them. 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 2016, CPDP carried out inspections in the following sectors and areas:

	SECTOR/AREA	NUMBER
	Healthcare	266
	Commerce and services	145
	Education and training	86
	Non-profit organisations	44
	Video surveillance	26
	Politics	25
	Internet	21
	Public administration	19
	Industry and trade	18
	Transport	18
	Consulting activities	17
	Legal services	13
	Human resources	12
	Telecommunications	12
	Insurance	12
	Financial and accounting services	11
	Information technologies	11
	Hotels and restaurants	11
	Social activities	10
	Regional and local authorities	9
	Banking	7
	Media	6
	Real estate transactions	5
	Security	4
	Justice / Law enforcement	4

	Construction	4
	Gambling	4
	Other	57

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 life 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 mandatory instructions regarding the conditions of personal data processing and the keeping of a personal data register, or refusal of registration.

In 2016, a total of 609 ex-ante inspections were carried out, including 20 inspections of PDCs with regard to which a refusal of registration was ruled in CPDP decisions in previous years.

The main problem with these inspections, similar to previous years, was the communication with the data controllers 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 by the PDC. Regardless of the efforts made by experts, often involving repeated correspondence due to impossibility to complete these inspections in 2015, the CPDP made a decision and in early 2016, on the grounds of Article 17b(3)(3) of the PDP Act, refused to register 102 personal data controllers in the Register of Personal Data Controllers and the Registers Kept Thereby. Following the publication of the decision on the CPDP's website, 14 PDCs submitted the documents required to finalise the check, statements of findings were issued, and as a result the PDCs were entered in the register referred to in Article 10(1)(2) of the PDP Act.

Another important issue in these inspections is the often poor quality of the personal data protection instructions that data controllers 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 inspection carried out during the reporting year in the Education sector. In addition to the sectoral trainings that the Commission 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 monthly control plans adopted by the Commission. It is a good practice to plan the inspections for the entire current year and accordingly to publish the plan on the CPDP website in order to inform the personal data controllers in due time and to take the necessary actions for preparation and carrying out the inspections.

29 ongoing inspections were carried out in 2016 (Figure 6). They resulted in the issuance of 12 statements establishing administrative violations (SEAV) and 3 mandatory instructions (MI).

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

- unlawful processing of personal data of customers/patients;
- 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 2016 in the field of personal data protection in the activity of personal data controllers in the sector of Education (Sectoral inspection), including the administration of the Ministry of Education and Science (MoES), was the inspection with the greatest factual and legal complexity and of significant public interest.

The planned and conducted sectoral inspection was the first of its kind in the activity of the CPDP. It resulted from the implementation of the main priority in the control activities of the CPDP adopted in 2015, i.e. carrying out of sectoral inspections. The main reason for this decision is related to the need for changing the approach for the selection of personal data controllers to be included in the scope of statutory inspections, as well as for a more global identification and solving of major problems of compliance with the PDP Act by large groups of controllers with similar activity.

In this connection, at the end of 2015 and the beginning of 2016, a working group of experts from the administration of the Commission prepared a draft Methodology for Carrying out Sectoral Inspections, and the Commission adopted it. With another decision, the sector, tasks and time period for conducting the inspection were determined. Mr Tsvetelin Sofroniev, Member of the CPDP, was appointed as a leader, and Mr Tsvetan Ivanchovski, Head of Control and Administrative Penal Procedures Department – as a coordinator.

For the purposes of the inspection, 4,611 educational institutions were selected, including 2,006 kindergartens with 232,600 children, 2,554 schools and vocational colleges with 761,990 pupils, and 51 higher schools with 218,398 students. In addition, administrative structures were included as subjects of the inspection – the MoES and 29 regional departments of education. In compliance with the methodology, the sectoral inspection was completed with a summary report to the CPDP.

At a regular meeting held on 30 November 2016 the Commission adopted the report and decided that a short version thereof shall be sent to the MoES for information and dissemination via appropriate channels to its structures. A period of 6 months was given for implementing the recommendations made in the report. Pursuant to the CPDP decision, educational institutions and the respective administrative structures having the quality of personal data controllers shall take the following actions within 6 months of the date of receipt of the attached report:

1. Request/update registers related to the processing of personal data of pupils/students and, if necessary, of parents.
2. Request/update in the relevant register mandatory data on the health of pupils/students.

3. Prepare/update Instruction on personal data protection within the meaning of Article 23(4) of the PDP Act on technical and organisational measures taken to protect personal data in accordance with Ordinance No 1/2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection.

4. Discontinue the collecting of copies of birth certificates of children and personal documents of parents as an appendix to Applications for Admission of Children according to the requirements of Ordinance No 5 of 3 June 2016 on pre-school education. In order to observe the principles set out in Article 2 of the PDP Act, the necessary data can be collected, for example, by a declaration or comparing with the original by the respective official. To this end, the MoES shall make the necessary amendments in the by-law, Ordinance No 5 of 3 June 2016 on pre-school education.

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

Another important ongoing inspection the CPDP planned as one of the priorities of its control activity in 2016 was related to the compliance with the PDP Act in the operations of the National EURODAC System and the preparation of a report to the European Commission. To this end, inspections at the Research Institute of Criminology and Forensics at the MoI (RICF) and the State Agency for Refugees with the Council of Ministers (SAR) were carried out. With a decision, the Commission appointed Ms Mariya Mateva – Member of CPDP, as a team leader with the following tasks:

- The new legal framework of the EURODAC System;
- Examination of the rules and procedures concerning the processing of personal data;
- Establishing the technical and organisational measures taken to protect personal data;
- The ways of exchanging information from the system with other authorities in the country and with countries in the European Union.

As a result of the inspections, on the grounds of the proposals made in the statements of findings, with a CPDP decision mandatory instructions were issued to the Research Institute of Criminology and Forensics at the MoI (RICF) and the SAR with the Council of Ministers.

The mandatory instructions to the RICF were as follows:

- For the purpose of ensuring the security of EURODAC data and providing an opportunity for data recovery where necessary, at least one backup copy of all the information in the system shall be stored on a separate server located outside the building of the RICF at the MoI;

- To provide authorised persons from law enforcement authorities with a technical possibility for direct electronic access to dactyloscopic data contained in fingerprint identification system EURODAC. Using a dedicated journal entry section (in log files), to provide an opportunity for full identification of the persons who received and processed these data;

- To synchronise the time periods for storing dactyloscopic data of individuals in the EURODAC system with the time periods for storing the same data in the AFIS system.

The mandatory instructions to the SAR were as follows:

- To restore video surveillance of security areas where fingerprint scanners are located;

- To provide metal lockable cabinets for storing the operational working archive with case files of foreign citizens;

- To issue an order authorising the persons concerned to work with the workstations of the EURODAC system.

Other ongoing inspections of greater public interest were the inspections of the following personal data controllers:

- United Bulgarian Bank AD the inspection resulted in the issuing of a SEAV to the PDC;

- ‘Customer Care BG’ OOD – the inspection resulted in the issuing of a SEAV;

- State Enterprise ‘Bulgarian Sports Lottery’ — the inspection started at the end of 2015 and was finalised in 2016 with the issuing of mandatory instructions.

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 the CPDP’s decisions or mandatory instructions as well as inspections undertaken at the CPDP’s own initiative upon receipt of irregularity reports (alerts).

74 ex-post inspections were carried out in 2016 (Figure 6). 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 2 mandatory instructions and 30 statements establishing administrative violations.

The ex-post inspections carried out following a CPDP decision of 21 political entities registered in the CEC for participation in the elections for President and Vice President of the Republic of Bulgaria and in the information campaign of the national referendum on 6 November 2016 attracted the most significant public interest. The main objectives of these inspections were to discontinue the possible misuse of personal data of citizens participating in subscription lists and to verify whether the political entities comply with the PDP Act. Based on the official checks in the website of the CEC and the public register of the CPDP it was established that some of the entities which submitted documents for registration in the CEC for participation in these elections and in the information campaign of the national referendum, including subscription lists with personal data of individuals supporting the registration, namely 6 parties, 3 coalitions of parties and 12 initiative committees, have not submitted applications for registration or for updating in accordance with the requirements of Article 17(1) or Article 18(3) of the PDP Act. In the course of these inspections, the experience from the inspections of political entities in connection with the participation in the elections of members of the European Parliament from the Republic of Bulgaria, held on 25 May 2014, were also used.

Among the remaining ex-post inspections carried out during the reporting period, the inspections of the following personal data controllers were of greater public interest:

- ‘Toplofikacia Sofia’ EAD, closed with the issuing of a mandatory instruction to the PDC;
- Central Cooperative Bank AD, closed with the issuing of a SEAV to the PDC;
- Registry Agency at the Ministry of Justice, closed with the issuing of a mandatory instruction to the PDC.

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 2016, the Commission received 183 requests from individuals, including topical inquiries on personal data protection issues. The consideration

includes getting acquainted with the relevant laws and regulations, requesting written answers and/or opinions from the corresponding PDCs, giving instructions for certain actions, consultations, etc. Where necessary, inspections on the grounds of Paragraphs (3) or (4) of Article 12 of the PDP Act are carried out.

Most frequently, alerts refer to the attention of the CPDP unlawful actions relating to:

- processing of personal data of individuals without existing registration with the 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;
- ability to generate a PIN on a website and learn the names of individuals from health insurance reports;
- requiring copies of identity documents;
- making copies of identity cards for issuing a European Health Insurance Card.

By the end of the reporting period, 165 requests were considered, 1 mandatory instruction was issued, 8 statements establishing an administrative violation were prepared, and 2 requests were referred by competence to Chief Directorate 'Combating Organized Crime' at the MoI, and 1 — to the Regional Police Department of the town of Slivnitsa. Appropriate replies were returned to the senders.

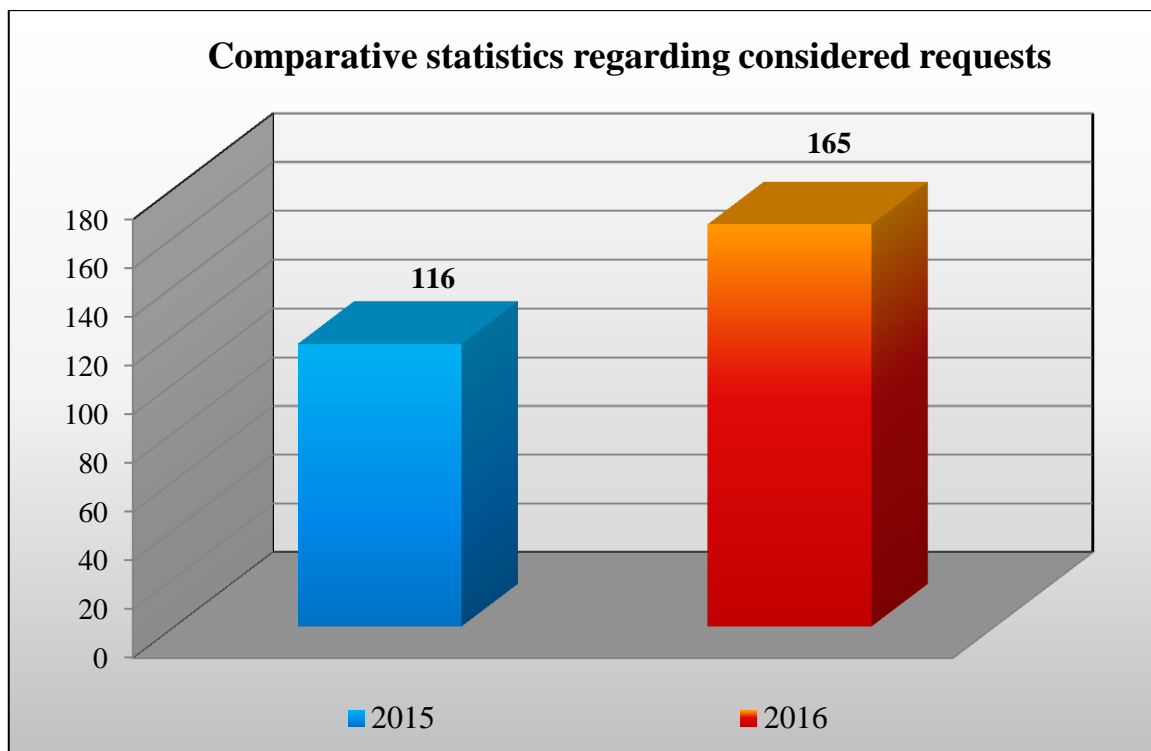


Figure 9

Comparative statistics from the previous year (Figure 9) and an 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. Mandatory 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 mandatory instructions (MIs) to PDCs regarding the protection of the personal data processed.

The MIs 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 Ordinance No 1 of 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection. Instructions put the personal data controller 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.

Four of the 9 mandatory instructions issued in 2016 were complied with within the time-limits set by the CPDP, and the other 5 MIs are under implementation. The mandatory instructions issued were addressed to the following personal data controllers:

- State Enterprise ‘Bulgarian Sports Lottery’;
- Executive Agency ‘Military Clubs and Recreation Centers’;
- Registry Agency (RA);
- Ministry of Foreign Affairs;
- ‘BDZ Passenger Services’ EOOD;
- ‘Alpico Publishing’ EOOD;
- ‘Oriflame Bulgaria’;
- Research Institute of Forensic Science and Criminology – MoI;
- State Agency for Refugees with the Council of Ministers (SAR).

Instructions are issued with regard to:

- the processing of documents containing personal data, where the volume required is bigger than the volume necessary to identify the individual and 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;
- taking of specific measures to ensure the required level of protection of personal data, including taking special measures when transferring personal data electronically.

In view of their factual and legal complexity, longer time periods for implementation were given in instructions issued to the Ministry of Foreign Affairs regarding the operation of the Visa Information System; to the RICF at the MoI and the SAR at the CoM with regard the operation of the National EURODAC System; and to the Registry Agency at the Ministry of Justice in connection with the access of third parties to the optional fields in the forms for registration of circumstances in the Commercial Register and to scanned documents, as well as with the taking of the necessary measures for regulating the technological interaction between RA and the portal <https://opendata.government.bg>.

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, 50 statements establishing administrative violations were issued in 2016. Based on these, the Chairperson of the CPDP issued 45 penal decrees, 4 of which on the grounds of statements establishing administrative violations from the end of 2015.

Similar to previous years, in 2016 the Commission continued to encounter major difficulties in delivering the issued statements establishing administrative violations 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 the CPDP, which is sometimes explained by objective reasons – lack of sufficient staff and large volumes of proceedings. In some cases, statements establishing administrative violations are served to persons without representative powers, or the receipt whereby the personal data controller 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 statements establishing administrative violations and penal decrees, the 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 employee of the Commission who has prepared the corresponding statement or the draft of the penal decree.

The distribution of the penal decrees by type of the violation to be remedied is presented on the next chart (Figure 10)

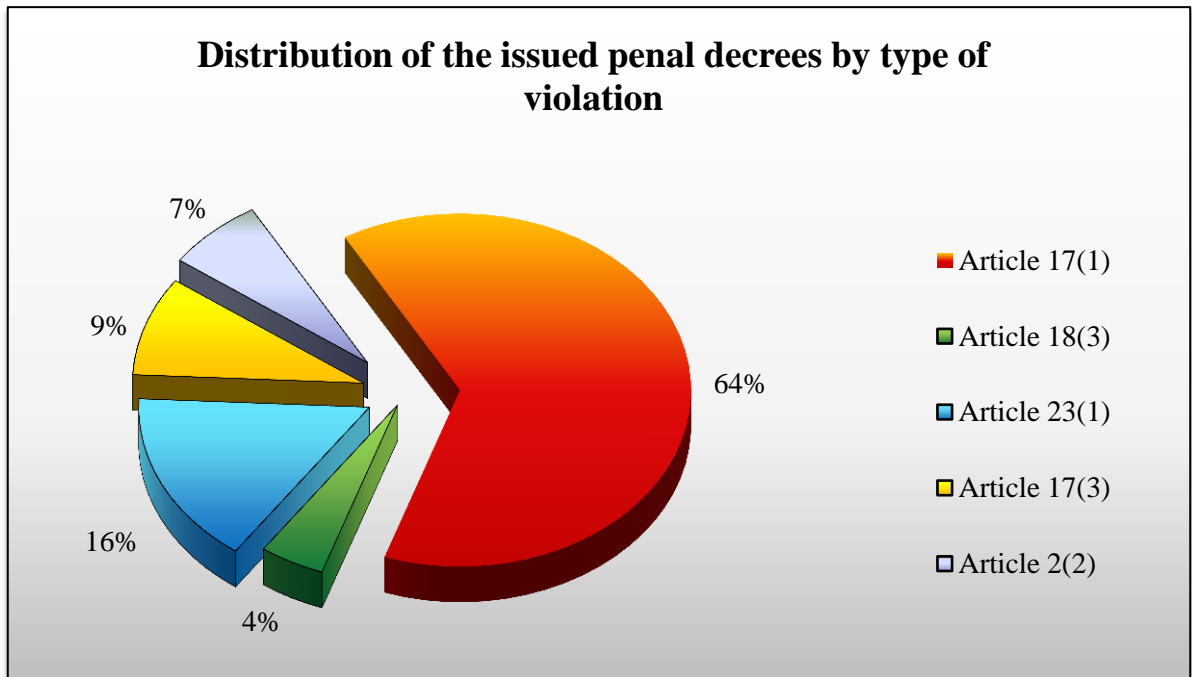


Figure 10

A natural continuation of the findings regarding the most frequent violations found in completed inspections is the failure of data controllers to submit applications for registration at the CPDP before they begin any processing of personal data, as required by Article 17(1) of the PDP Act. For such violations, 28 penal decrees were issued. For failure of personal data controllers 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, 2 penal decrees 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, 4 penal decrees were issued.

The next most numerous group of PDs are the 7 penal decrees for non-compliance with the provision of Article 23(1) of the PDP Act regarding the obligation of personal data controllers 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.

Three penal decrees were issued for violations in the processing of personal data comprising failure to comply with one of the legal requirements of Article 2(2) of the PDP Act, and one penal decree was issued for a violation of Article 4(1)—(7) of the PDP Act. The small number of administrative-penal proceedings for this type of violations also results from the fact that they are frequently the subject of other types of proceedings initiated on

complaints from individuals and are considered by the Commission acting as a collective body.

In 2016, the penalties imposed were amounted to BGN 101,500, and the total amount collected was BGN 24,500. Of these, BGN 7,000 were collected coercively by the National Revenue Agency (NRA).

Appeals against 14 of all penal decrees issued during the year are pending in courts. 10 PDs were paid without being contested and the offenders paid a total of BGN 13,500 in penalties, all of them near the minimum level 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 were of greater factual and legal complexity and of significant public interest. Examples include penal decrees against: ‘Customer Care’ Bulgaria EOOD with a total penalty imposed of BGN 17,000, Association ‘Sporten Club Puls — Sofia’ — BGN 11,000, BTC AD — BGN 10,000, United Bulgarian Bank AD — BGN 10,000, ‘Mobiltel’ — BGN 3,000, ‘Speedy’ AD — BGN 2,000, and others.

The Tax and Social Insurance Procedure Code is implemented for collecting the claims under penal decrees 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 National Revenue Agency (NRA). At present 36 penal decrees are being enforced by the NRA.

In 2016, the outcomes of the court cases initiated on appeals against penal decrees issued in previous years were as follows: 10 PDs were cancelled in their entirety, 4 PDs were confirmed in their entirety, and in 2 penal decrees the size of the penalty was reduced. Currently, 23 appealed penal decrees are in the trial phase.

In the court cases initiated on appeals against penal decrees during the year, the CPDP was represented in 52 court hearings by staff members that hold degrees in law and are officially admitted to practice the profession.

If valid legal grounds exist, the first-instance judgements, by which courts cancel the Commission’s penal decrees in their entirety or reduce them, are appealed before higher instance courts. When amending penal decrees, the court almost always reduces the imposed penalties to the minimum amount prescribed by law. The motives are the existence of attenuating circumstances, such as first offence and subsequent implementation of obligations under the PDP Act. Although they are noted in the penal decree, the court gives them greater credit than to aggravating circumstances. In other cases, the court wrongly accepts as a

mitigating circumstance the absence of a harmful result, as the corpus of the relevant provisions of the PDP Act has been formally performed and does not provide for such a result.

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

Below are the more significant and important grounds from the case law, on which the courts in the country have pronounced different rulings on the two most common violations of the PDP Act — failure to comply with the obligation for initial registration under Article 17(1) of the PDP Act and with the obligation to notify the CPDP of changes in data from the initial registration according to the requirements of Article 18(3) of the PDP Act.

Like in previous years, the most frequent reason in court rulings for cancelling a penal decree is related to determining the date of the offence in view of the assessment regarding the application of the limitation period for invoking administrative penal liability under Article 34(1) (2) of the AVP Act. The court has ruled that the date of the inspection by the CPDP team and the finding regarding the violation is not the date of the offence as stated in the statement establishing an administrative violation and the penal decree. In other words, this period has lapsed because the personal data controller has started the initial processing of personal data far before this time limit and the inspection itself.

This reason has substantiated cancelling of penal decrees by both regional and administrative courts, in particular:

- Regional Court (RC)/Administrative Court(AC) Sofia under PD No 34/2014 against Political Party ‘Christian Democratic Party of Bulgaria’;
- RC/AC Sofia under PD No 38/2014 against Political Party ‘People’s Voice’
- RC/AC Sofia under PD No 48/2014 against Political Party ‘Communist Party of Bulgaria’.

In the cases of political entities collecting subscription lists, it is virtually impossible to establish the exact date of the initial commencement of processing — i.e. the date when the first citizen signed a subscription list and the date when the political entity had to fulfil its obligation to register in the CPDP. This is because the standard forms endorsed by the CEC do not contain the requisite “date” for the signatures of voters supporting the registration.

In some judgements other courts confirm appealed penal decrees by accepting the date of the CPDP inspection as the date of the violation and, therefore, accepting that the three-month period under Article 34(1)(2) of the AVP Act is complied with. Such reasons have been brought and penal decrees have been confirmed, as follows:

- RC Sofia under PD No 31/2014 against Political Party ‘Bulgarian Left’;
- RC Sofia under PD No 35/2014 against Political Party ‘United Social Democracy’;
- RC Sofia under PD No 37/2014 against Political Party ‘Bulgarian Democratic Community.

Under the continuing in 2016 court proceedings, out of the 30 issued penal decrees against political entities, registered with the CEC for participation in the elections of members of the European Parliament from the Republic of Bulgaria, held on 25 May 2014, the penalties imposed under 12 penal decrees were paid, and 4 penal decrees are currently with the NRA for collecting the claims. Out of the court cases initiated on the appeals of political parties against the penal decrees issued, which were completed in 2015—2016, 7 penal decrees were cancelled with legally enforceable rulings and the proceedings relating to other 7 penal decrees are pending at different stages of the trial phase, being appealed before a second instance.

All court judgements and especially their reasons have been 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 establishment of violations of the PDP Act and to ensure that they are properly documented in accordance with the provisions of the PDP Act. The introduced good practice all court decisions to be sent in a timely manner by e-mail also to the Chairperson and the Members of the CPDP contributed to this. As a result, it has been observed that the staff members authorised to issue acts establishing administrative violations, draft penal decrees and for legal 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 penal decree for violation of the PDP Act. A striking example of such a large period of over 5 years is penal decree No 27/2011, issued against the Municipality of Pernik for 2 violations of the PDP Act. Following the appeal against this decree in 2011 before the Regional Court of Pernik, an administrative case was initiated in 2014, and after a cassation appeal the case was solved at the end of 2016 by the Sofia–District AC.

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

The analysis of the court judgements in 2016 shows that, like in previous years, the number of penal decrees for the two most frequent violations of Article 17(1) and Article 18(3) of the PDP Act, cancelled by courts, has increased. This leads to the conclusion of the need to initiate legislative changes in order to clarify these provisions of the law to eliminate the difficulties in their practical implementation.

VI. Personal Data Protection during the Elections for President and Vice President of the Republic of Bulgaria and the Referendum. Analysis of Proceedings

Pursuant to provisions of the Electoral Code, personal data in the submitted lists of individuals supporting the registration of political entities with the CEC shall be processed and provided in compliance with the requirements of the PDP Act. For this reason, pursuant to Article 3(4) of the PDP Act, each political entity as a personal data controller shall ensure compliance with the requirements of Article 2(2) of the PDP Act, in particular lawful processing of personal data of individuals participating in subscription lists supporting its registration.

In items 3 and 4 of its opinion No P-4553 of 1 August 2016 the Commission explicitly acknowledged this fact and stated the legal grounds based on which political parties, initiative committees and coalitions of parties are personal data controllers and shall declare the registers of personal data they process depending on the different categories of individuals and the purposes for which the data are processed.

On these grounds and in view of carrying out its control activities under Article 12 of the PDP Act, during the reporting period the Commission voted decisions and carried out inspections of 21 political entities – 6 parties, 3 coalitions of parties and 12 initiative committees, which submitted documents for registration with the CEC for participation in the elections for President and Vice President of the Republic of Bulgaria and in the information campaign of the national referendum on 6 November 2016, but did not file with CPDP applications for registration or update as personal data controllers.

The 2 groups of violations found in connection with the tasks stipulated in the CPDP decision on the inspections are related to failure to comply with the provisions of Chapter Three of the PDP Act regarding the obligations of political entities laid down in Article 17 and in Article 18(3) for registration in the register referred to in Article 10(1)(2) of the PDP Act before they start any processing of personal data and/or updating the entries in the register upon any change of the circumstances stated in the initial application for registration. 20 SEAVs were drawn up, as follows: for failure to file an application, which constitutes a violation of Article 17(1) of the PDP Act, 19 SEAVs were drawn up, and 1 SEAV was drawn up for failure to update a submitted application, which comprises a violation of Article 18(3) of the PDP Act.

During the inspections and the initiated administrative-penal proceedings, 8 political entities fulfilled their obligations for registration/update, and this was taken into account when the amount of the penalties imposed on them was determined.

Based on the 20 statement establishing an administrative violation drawn up, 15 penal decrees were issued, with 9 appeals filed so far. Again, difficulties were encountered in delivering the acts and decrees, especially to the representatives of initiative committees. This directly affects the timely completion of the proceedings.

In addition to the above, the CPDP received 220 complaints with regard the processing of personal data of citizens in the lists supporting the participation in the Presidential/Vice Presidential elections and in the information campaign of the national referendum.

Out of this total number, 137 complaints were filed with regard the processing of personal data in lists of individuals supporting the registration of a party, coalition or initiative committee for participation in the elections for President and Vice President of the Republic of Bulgaria on 6 November 2016. The complaints are against 28 political entities: 10 initiative committees; 14 political parties, and 5 coalitions of parties.

In addition, 78 complaints were filed with regard the processing of personal data in lists of individuals supporting parties, coalitions and initiative committees for participation in the information campaign of the national referendum on 6 November 2016. In 11 complaints within this category, the complainants assert that their personal data has been processed simultaneously in two lists submitted by two different initiative committees. The complaints are against 20 political entities: 16 initiative committees; 3 political parties, and one coalition of parties. The proportion of complaints received is presented below (Figure 11):

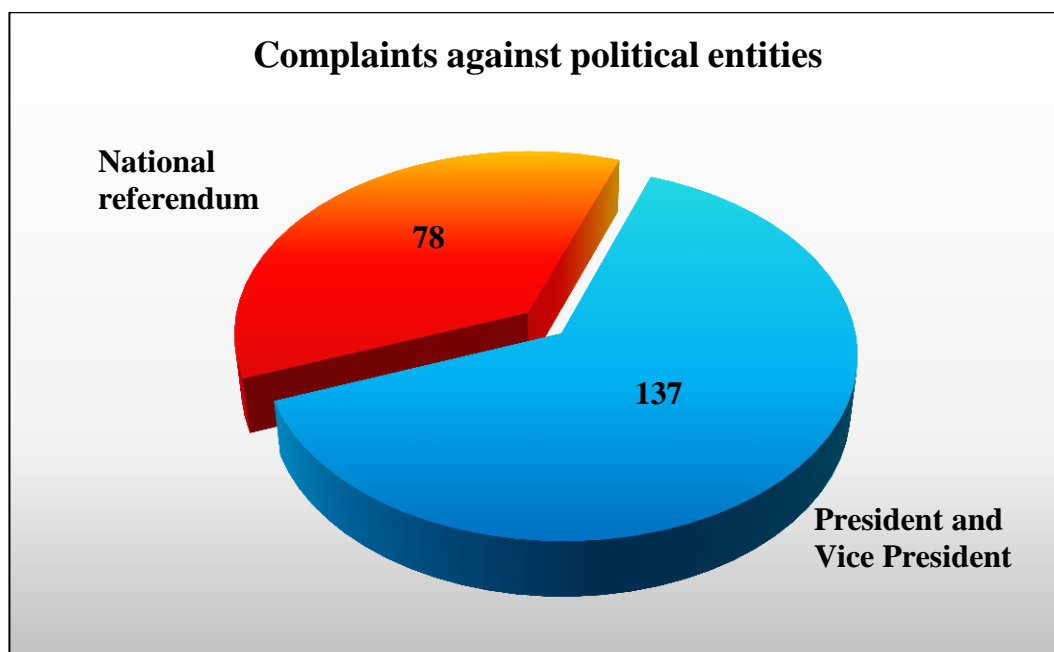


Figure 11

With the lodging of the first complaints to the CPDP, actions were taken to inform the complainants, whose complaints were irregular, about the need to remove the irregularities.

At its session held on 6 October 2016, the CPDP adopted a decision for joining proceedings under complaints received by the CPDP in connection with the processing of personal data in the lists of persons supporting the registration of a party, coalition or initiative committee for participation in the information campaign of the national referendum on 6 November 2016. Also, proceedings were joined with regard to the complaints received by CPDP in connection with the processing of personal data in the list of persons supporting the registration of a party, coalition or initiative committee for participation in the elections for President and Vice President of the Republic of Bulgaria on 6 November 2016, by initiating and conducting corresponding proceedings against the defendant — political party, coalition of parties or initiative committee.

At the same session a decision was adopted to carry out handwriting analysis assessment with the task to ascertain whether the signatures of the persons who have provided comparative material were affixed on the lists by the persons concerned, and to give the complainants a 10-day period to provide comparative material for the purpose of drawing up the analysis assessment.

During the reporting period the possibility for the complainants to provide comparative material in the closest Regional Police Directorate to their settlement was agreed, in in the spirit of cooperation with the MoI authorities,

At present, comparative material has been provided in connection with 84 complaints (51 for the elections for President, and 33 for the national referendum).

The Central Electoral Commission has provided the evidence required for the analysis assessment: the corresponding lists in support of participation in the elections for President and in the information campaign of the national referendum, and lists of persons supporting the registration of a party, coalition or initiative committee for participation in the elections for President and Vice President of the Republic of Bulgaria on 6 November 2016.

The preparation of the documents for the carrying out of the commissioned analysis assessments by the RICF is forthcoming. The results from the analysis assessments will shed light on the main issue of the proceedings: if the complainants have affixed their signatures on the corresponding lists.

Based on the inspections of political entities and the handling of complaints alleging misuse of personal data of voters in relation to all the elections held during the period 2014—2016, the CPDP identified a number of problems in the activity of these entities as personal

data controllers. Regardless of the Commission's recommendations, clarifications and mandatory instructions, political entities continue to commit the same violations of the PDP Act. The CPDP considers that it is appropriate additional measures to be taken, including those of legislative nature, to ensure compliance with the requirements in the field of personal data protection and to guarantee the rights of individuals. In order to establish a practice complying with the requirements of the PDP Act regarding the processing of personal data by political entities, at the end of the reporting period CPDP presented to the CEC reasoned proposals for legislative and/or organisational measures, as follows:

1. A certificate of registration in the register pursuant Article 10(1)(2) of the PDP Act for a data controller to be included in the list of documents that political entities are obliged to submit to the CEC with their applications for the respective registration.

2. The 'date of signature' field to be included as a mandatory field in the standard forms of the lists of voters supporting the registration of the relevant political entity with the CEC together with the name, PIN and signature of the persons.

3. To provide a legal opportunity in the Electoral Code for the person to identify himself/herself with an identity document before signing in support of the registration of the relevant political entity. If the individual refuses to provide a document confirming his/her identity, the person collecting the subscription shall have the right to refuse the voter to exercise his/her right to support by participating in the subscription.

The CPDP proposals for discussion by the CEC will remove the conditions for unscrupulous practices in the processing of personal data of individuals in connection with collecting subscriptions.

VII. Proceedings for Issuing Opinions and Participation in Legislative Coordination Procedures on Matters Relating to Personal Data Protection

In 2016 CPDP responded to 125 requests by issuing official opinions pursuant Article 10(1)(4) of the PDP Act. For comparison, requests for opinions on which the Commission ruled during the previous two years were as follows: 92 in 2015, 80 in 2014, and 79 in 2013 (Figure 12).

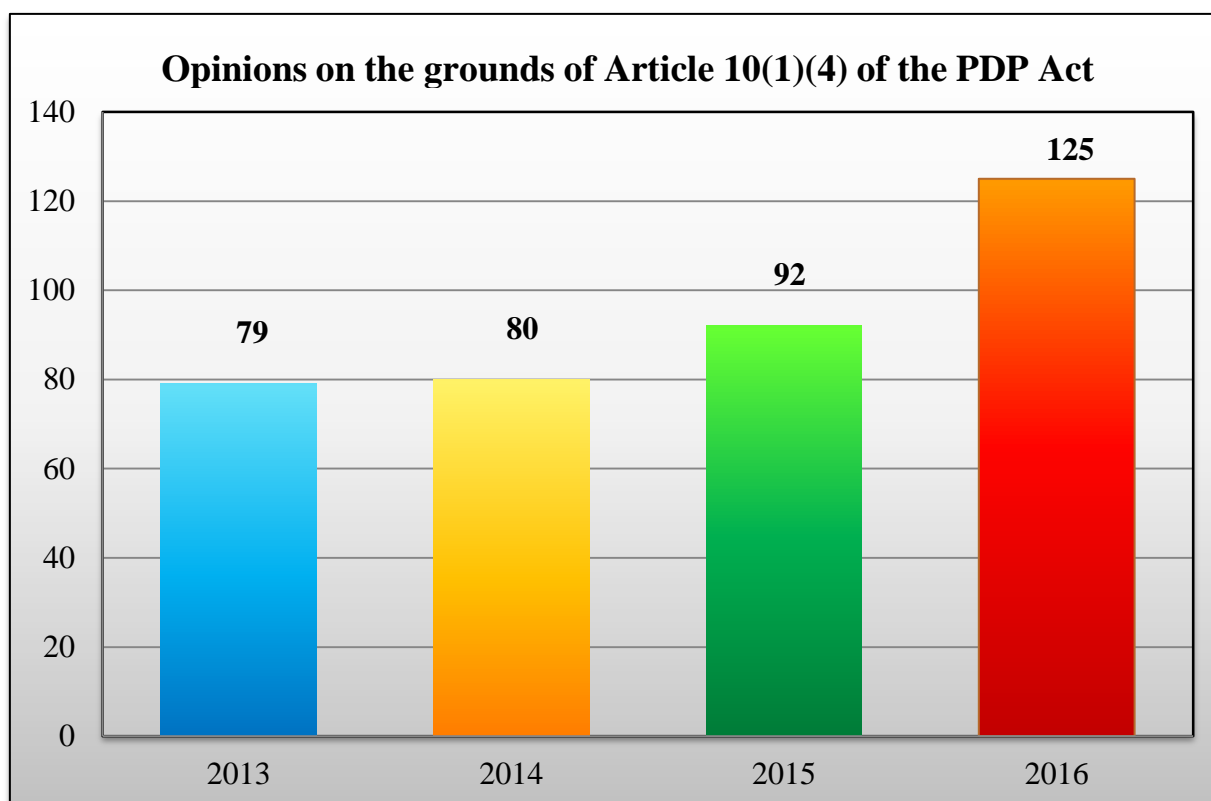


Figure 12

Some of the more specific cases on which the CPDP issued an opinion in 2016 in the context of personal data protection are as follows:

1. Chief Directorate of Civil Registration and Administrative Services at the Ministry of Regional Development and Public Works (GD GRAO) requested an opinion regarding the implementation of Article 106(1)(3) of the Civil Registration Act — granting of permission by CPDP to provide access to the Population Register — National Database ‘Population’ (NDB ‘Population’) to banks and credit institutions in order to check the credit ability of borrowers.

In the legal analysis carried out, CPDP took into account the statutory responsibilities of credit institutions under Article 16(1) of the Consumer Credit Act. Pursuant to this provision, before signing a loan agreement, a creditor shall evaluate the consumer's credit ability on the basis of sufficient information, including information, received from the consumer, and if needed, shall make reference in the Central Credit Register or in another database, used in the Republic of Bulgaria for evaluation of the consumers' credit ability. Furthermore, pursuant to Article 4 of the Measures against Money Laundering Act, when entering into a business relationship with an individual, the bank is required to identify the individual by collecting a certain set of data about him/her, as well as to verify this data. Information already provided by individuals can be verified only by a check in an official register containing the relevant data, such as the NDB 'Population'.

In connection with the above, the CPDP defined in its opinion and in its subsequent decisions the conditions and parameters that guarantee the lawfulness and proportionality of the access to the NDB 'Population' by credit institutions for the purpose of verifying the credit ability of individuals — customers:

- explicitly defined scope of the personal data accessed: name — given name, father's name, surname, PIN, permanent and current address, marital status (married/not married/widow(er)/divorced), number of minor children, date of death;

- access to the data can only take place in the presence of freely expressed, concrete and informed consent of the individual — customer, to whom the personal data in the NDB 'Population' refers;

- the credit institution shall keep written evidence of the obtained consent;

- explicitly defined time limits for data retention: with regard to customers to whom a loan has been granted: for the period of repayment of the loan, unless otherwise provided for in a statutory instrument; with regard to customers who have been denied a loan: for a period of 6 years from the date of consent by the respective customer;

- the Ministry of Regional Development and Public Works, in its capacity as data controller, shall undertake adequate and effective practical steps to provide access to, respectively, track and prove the access made to the NDB "Population" to ensure full compliance with the mandatory data protection requirements stemming from the PDP Act, the Civil Registration Act, Ordinance No. 1 of 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection, and the CPDP decisions.

2. In 2016 the CPDP received a number of requests for opinions from mayors of municipalities in their capacity as civil status officials in connection with requests from banks for the issuance of certificates of inheritance upon the death of a borrower. In such cases, on the grounds of Article 10(1)(4) of the PDP Act in conjunction with Article 106(1)(3), CPDP expressed the opinion that mayors of municipalities in their capacity as civil status officials cannot provide the bank 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 a loan agreement, are debtors of the bank is a fact which must be proved and the burden of proof is on the person making this assertion. The CPDP's position is also supported by the case law of the Sofia City Administrative Court (Ruling No 4859 of 8 July 2015 under administrative case No 4858/2015 of SCAC; Ruling No 5206 of 21 July 2015 under administrative case No 4862/2015 of SCAC; Ruling No 5175 of 20 July 2015 under administrative case No 4234/2015 of SCAC, etc.).

3. Other requests for access to personal data from civil status records in the form of certificates of inheritance were received during the year on different grounds. For example, 'Electricity System Operator' EAD, the Road Infrastructure Agency and 'Chimkomplekt Engineering' AD are investors and/or contractors of infrastructure projects of national importance. They need up-to-date information about property owners or their heirs, who/which will be affected by the land acquisition procedures under the State Property Act (SPA). In these cases CPDP considered that the hypothesis of Article 4(1)(5) of the PDP Act exists — processing is necessary for the performance of a task carried out in the public interest, and allowed the provision of the requested information.

4. The opinion of the CPDP in response to a request from a company providing professional condominium management services for permission to obtain personal data concerning owners and occupants of buildings in condominiums merits particular attention. In particular, the company would like to receive from Sofia Municipality and the mobile service providers the names, the permanent and the current address, and the telephone numbers of the owners of the properties in the condominium, especially in cases when such owners have not lived in the premises owned by them for many years. In its opinion CPDP stated that in such cases the condition of Article 4(1)(7) of the PDP Act exists — processing is necessary for the execution of the legitimate interests of the party to whom the data is disclosed. The activities of personal data processing of owners are aimed at preserving in good condition and maintaining the common areas, the respective share of which is owned by the owner in the condominium, and are undoubtedly in the interest of all owners in the condominium. In this

connection, Sofia Municipality can provide condominiums, represented by their management boards through the respective attorney, personal data about owners of independent properties in the building from NDB 'Population', as follows: full name, subject of management, permanent address and current address. Such data shall be provided after sufficient evidence of a justified need for these data is enclosed in advance with the application. At the same time, in accordance with the principle of proportionality, CPDP considers that the provision of additional data about the owners, including telephone numbers from telecommunication service providers, can only take place if a relevant court certificate under Article 186 of the Civil Procedure Code exists.

5. The Chairperson of the Energy and Water Regulatory Commission approached the CPDP with a request to issue an opinion on the processing of personal data for the purposes of accounting and invoicing of water consumed in condominiums, including the distribution of 'total consumption' costs. Various cases from managers of condominiums are presented to the attention of the regulator, in which the water and sewerage operator does not provide information about properties, the liabilities of which are formed on the basis of the number of occupants. According to the complainants, the number of occupants in the properties in question is not up-to-date, and therefore they are willing to assist in establishing the exact number of occupants in order to correctly allocate the 'total consumption' costs, thus minimising the negative effect of the actions/omissions of defaulting consumers who cause loss to the other residents in the condominium. The CPDP examined the case with particular attention because the issues addressed concern a wide group of citizens, and took the view that when the way of supply of water to a building (with one water supply deviation for all entrances) makes it necessary in connection with a complaint from the owners of one of the entrances (comprising one condominium) the EWRC to take into account information, including personal data of owners and occupants of separate units in a different entrance (different condominium), there is no obstacle for the EWRC to provide the representative of the condominium, which referred the issue to the EWRC, all information sent to it by the operator in connection with the complaint, while complying with the PDP Act and the basic principles and rules of the administrative proceedings within the meaning of the APC. The CPDP accepts that, on the grounds of Article 4(1)(5) of the PDP Act and in conjunction with Article 3(2) of the Water Supply and Sewerage Services Regulation Act, the water and sewerage services operator can provide the complainant — manager of one entrance data regarding the water consumption by the consumers in another entrance, when the two entrances are supplied by a single water supply deviation and while observing the

requirements of the PDP Act. The information in question can only be accessed by persons whose interests are affected in connection with fair reading of the total consumption in the specific interconnected sites.

6. Another important opinion of the CPDP that had a specific positive result was related to the manner of generating the numbers of contracts for electronic communications services, concluded between ‘Bulgarian Telecommunication Company’ EAD (BTC) and subscribers — individuals. The CPDP was approached by the Chairperson of the Communications Regulation Commission, who stated that the contract number includes the entire personal identification number of the subscriber. The CPDP expressed an opinion that such a practice is contrary to the principles of processing of personal data, reflected in the provisions of Article 2(2)(3), in particular that the processing shall be proportionate to the purposes for which personal data is being processed and not exceeding its scope. Contract numbers shall be generated in a way that excludes the possibility of unauthorised access and unlawful distribution of the personal identification number of the individual subscriber. The CPDP also decided to initiate administrative proceedings on the grounds of Article 10(1)(5) of the PDP Act for issuing a mandatory instruction to BTC EAD. Subsequently, the CPDP was officially notified by the company that, as of 20 October 2016, the numbers of customer contracts do not contain personal identification numbers, and provided the relevant evidence. In view of the above, the CPDP decided to terminate the initiated administrative proceedings.

7. In 2016, the CPDP continued its practice from previous years to provide guidance on compliance with data protection principles and rules in the electoral process. In response to requests from the CEC, the Commission expressed two opinions: on the ways and means of informing and motivating young people to participate in the presidential elections and the national referendum without affecting their personal data and privacy, and on the need to register observers in the electoral process as personal data controllers.

8. During the reporting year the CPDP adopted several opinions relating to the processing of personal data in the Education sector.

The CPDP made a self-referral in connection with the plans of the MoES announced in the media that outpatient sheets issued by general practitioners shall serve as an excuse of absence from school. The reason for this idea was the increasingly frequent falsifying of medical notes that serve to excuse absences from school. The CPDP expressed the opinion that taking appropriate measures to strengthen the control of pupils’ participation in the learning process is a socially significant issue the solving of which, however, shall not be contrary to the personal data protection rules. In the specific case there is no legal basis for the

disclosure of pupils' health information in the volume specified in the outpatient sheet for the stated purposes — excusing of absences. At the same time using outpatient sheets would be unlawful and inappropriate measure contrary to the main principles of personal data processing. The opinion was sent to the Ministry of Education and Science and the Ministry of Health. Subsequently, the MoES refused the idea to use the inappropriate measure for excusing absences and included in a statutory instrument a new balanced solution of the problem, which guarantees both a good way to excuse absences and protection of personal data, including information regarding health, fully in line with the reasoning in the CPDP opinion.

9. The CPDP received an inquiry whether it is acceptable for schools to publish on their websites lists containing the three names and the results from the external evaluations of the pupils. The MoES was requested to give an opinion on this. In the meanwhile, the CPDP received an opinion from the headmaster of the school that announced the results, in which the CPDP was informed that there are no texts prohibiting such publishing — it is made on the school's website in order to inform parents more effectively about the results. In order to avoid such cases in the future, questions were asked as to when it is not a violation to place in public places (entrance or website of schools) lists of pupils' names, number of points or grades received (newly enrolled pupils, results from academic and sports competitions, results from equalising and other exams).

The CPDP expressed the opinion that because of the absence of legislation in the field of education regarding the way the results from different types of examinations are published and the volume of information to be published, the general rules of the PDP Act shall apply. 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.

10. In 2016 the CPDP received several requests for opinions from medical institutions as well as from the National Centre for Addictions to the Ministry of Health in connection with letters received from the court or pre-trial authorities concerning the provision of information regarding specifically mentioned persons included in treatment programmes. Such letters are on the grounds of Article 159 of the Criminal Procedure Code (CrPC),

pursuant to which, at the request of the court or pre-trial authorities, all institutions, legal persons, officials and citizens are obliged to keep and hand over the objects, papers, computer data and other data in their possession, which may be relevant to the case. In such cases the CPDP has expressed the opinion that the provision of information containing personal data of specific patients to the court or pre-trial authorities on the grounds of Article 159 of the CrPC for the purposes of specific criminal proceedings for serious crimes is permitted, since it is within the meaning of Article 4(1)(1) of the PDP Act.

11. During the reporting period CPDP was approached by the General Directorate 'National Police' at the MoI in connection with the development of an automated information system for counteracting child crime and child protection under a project funded under the Bulgarian–Swiss Cooperation Programme. In this respect, the MoI asked for an opinion on the compliance with the Bulgarian legislation to ensure the protection of personal data in the prepared technical terms of reference for the development of an automated information system for counteracting child crime and child protection. In its opinion, the CPDP supported in general the initiative to develop an automated information system for counteracting child crime and child protection with the following comments and remarks, which shall be taken into account and reflected in the terms of reference for the development of the information system:

- statutory instruments shall clearly specify the time periods for retaining personal data in the system, in particular that personal data shall be deleted no later than two years after the person concerned has reached legal age;

- clear mechanisms shall be set out for access, correcting and deletion of personal data of persons concerned;

- in view of the different purposes for which personal data is processed within the system, the personal data of different categories of the persons concerned (children – offenders and children – victims of crime) shall be separated;

- in order to achieve a better balance between the objectives of the system and the principles of personal data protection, the CPDP encourages the wider use of anonymisation and/or pseudonymisation of the personal data of minors.

In response, the MoI informed the Commission that all notes and comments expressed in the opinion will be reflected in the Organisational and Technological Rules for work with the information system.

12. In 2016 the CPDP considered a request from the Veliko Tarnovo Administrative Court regarding the implementation of the PDP Act in the drafting and provision of

announcements regarding criminal cases to mass media. After examining in detail the statutory framework related to the issues raised, the CPDP expressed the opinion that the provision of press releases containing information on criminal cases of general nature, sent by the Veliko Tarnovo Court of Appeal to the mass media, shall be carried out in compliance with the PDP Act, without any possibility for direct or indirect identification of natural persons. The provisions of Article 4(2) and Article 5(2)(7) of the PDP Act are not applicable to the activity performed by the court, which does not fall within the scope of the concept ‘exclusively for the purposes of journalism, literary or artistic expression’. Information contained in press releases for media shall respect the restrictions imposed by the principle of transparency of the process set out in Articles 263—265 of the Criminal Procedure Code. Pursuant to Article 4(2) and Article 5(2)(7) of the PDP Act, personal data may be processed in the cases where the processing is performed exclusively for the purposes of journalism, literary or artistic expression provided that it does not violate the right of privacy of the person to whom such data refers. In the cases of dissemination of information containing personal data for the purposes of journalism, a fair, reasonable and proportionate balance between the freedom of expression and the right to information, on one hand, and protection of personal data and privacy, on the other hand, shall be sought in each specific case.

13. In several opinions the CPDP took a stand on the balance between the protection of personal data and the right of access to public information in 2016.

The Director of the Center “Fund for Treatment of Children” (CFTC) requested from the CPDP an opinion in connection with a request from ‘bTV Media Group’ EAD for information under the Access to Public Information Act (API Act) concerning: 1. Information regarding the number of children sent abroad and children treated in Bulgaria using resources from the CFTC; 2. Information about the children treated by the Fund in hospitals in Bulgaria – the names of the doctors, in which hospitals, clinics, at what cost and what implants were made for the children; 3. Information regarding the amounts paid by the Fund for implants and medical devices as a percentage of the total budget of the Fund.

The CPDP held that the provision of the requested information is admissible under Article 4(1)(1), (5) and (6) and Article 5(2)(7) of the PDP Act. In order to ensure the fair processing of the data in the cited legal hypotheses and in order to achieve the objective of the PDP Act (to ensure privacy), the personal data controller shall provide the requested information under the following conditions:

With regard to items 1 and 3 of the request there are no personal data, i.e. the API Act is fully applicable and the CFTC shall provide the requested information in full, as follows:

- summary information regarding the number of children treated in Bulgaria and abroad using resources from the CFTC;

- financial information regarding the amounts paid by the Fund for implants and medical devices as a percentage of the total budget of the Fund.

With regard to item 2 of the request, full information can be provided with anonymised or deleted personal data, meaning that it will be provided in the following form: child (without personal data leading to its individualisation), hospital, clinic, value of the intervention, implant. In this way, the public interest will be fully satisfied, without in any way violating the right of privacy of the persons concerned.

14. During the year a request from the Rector of the University of Library Studies and Information Technologies (UniBIT) was received in connection with an application from Nova TV for access to information regarding the remuneration of the Rector, the Vice Rectors and the Deans for years 2015 and 2016, and regarding the rules for formation of such remuneration. CPDP expressed the opinion that, in order to ensure the fair processing of the data in the cited legal hypotheses and in order to achieve the objective of the PDP Act (to ensure privacy), the university shall provide the requested information under the following conditions:

With regard to the information concerning the current rules for forming the salaries of people occupying management positions in the educational establishment, there is no personal data, i.e. the API Act is fully applicable and the UniBIT shall provide the requested information in full.

With regard to the remuneration received, information shall be provided which includes only the position according to the classifier of the higher school and the corresponding gross/net remuneration received in 2015 and 2016. From the point of view of the grounds for lawful processing of personal data, the following provisions apply: Article 4(1)(1) of the PDP Act — the processing is necessary for the execution of an obligation of the personal data controller, stipulated by law; Article 4(1)(5) of the PDP Act — the processing is necessary for the performance of a task carried out in the public interest; Article 4(2) of the PDP Act — the processing is performed exclusively for the purposes of journalism, literary or artistic expression provided that such processing does not violate the right of privacy of the person to whom the data refer.

15. In 2016 CPDP was approached by ‘Protection of Children’s Rights’ Foundation with a request for an opinion on issues concerning the processing of personal data by foster families. Several questions were asked in the request: 1. Is it lawful for a foster parent or

family to handle personal data of children without being entered in the Register of Personal Data Controllers and is their registration in the register mandatory? 2. Is it lawful, in view of the nature of the ‘foster care’ in Bulgaria, for persons exercising the profession of foster parents to have access to personal data such as: PIN, personal medical records and documents, court instruments, administrative instruments, etc.? 3. Has the Commission received any applications for registration in the Register of Personal Data Controllers from persons exercising the profession of foster parent?

After a careful analysis of the case, taking into account the specifics of foster care, CPDP expressed the opinion that the persons who are foster families within the meaning of Article 31(1) of the Child Protection Act, are personal data controllers according to Article 3(2) of the PDP Act. At the same time, the Commission exempts them from the obligation to register with CPDP, but not from the other obligations they have under the PDP Act and its implementing regulations. The processing of personal data concerning children and their biological parents in accordance with the provisions of the Ordinance on the Criteria and Standards for Social Services for Children and the Ordinance on the Terms and Procedure for Application, Selection and Approval of Foster Families and Placement of Children in Them is admissible on the grounds Article 4(1)(1), (3), (4) and (7) of the PDP Act.

16. In response to a request from the Acting Chairperson of the Commission for Prevention and Ascertainment of Conflicts of Interest and the Executive Director of the ‘Access to Information Programme’ Foundation, the CPDP expressed an opinion related to the implementation of Article 17(2) of the Prevention and Ascertainment of Conflicts of Interest Act (PACI Act), namely the disclosure of the declarations of obligated persons on the websites of the institutions. The established practice of the Commission on this issue is the balanced approach, according to which personal data in the declarations under Article 12 of the PACI Act, with the exception of the names of the declarant, which must appear, shall be disclosed after an express written consent of the person, made in a separate declaration. In these declarations, the personal identification number, the signature of the person and the bank accounts, as well as the personal data of third parties who are not obligated under the PACI Act and have no relation to the declaring under Article 12 of the said law, shall be deleted.

The opinions adopted by CPDP on the grounds of Article 10(1)(4) of the PDP Act are an important tool for clarifying the legal provisions in the field of personal data protection by developing and enhancing both the practice of the supervisor and the overall policy in this area. At the same time, they are fully in line with the competence of the CPDP and are not

intended to interpret or give guidance on the implementation of special statutory instruments, except where specific provisions explicitly regulate the protection of personal data in the respective area or impose powers and/or obligations on the CPDP. It is also important to point out that CPDP opinions do not have the characteristics of an individual administrative act within the meaning of the Administrative Procedure Code.

During the reporting year, an upward trend was observed of approaching the CPDP with requests for opinions regarding various topics from public life and by different data controllers. The analysis that can be made with regard to the subjects of such opinions and the controllers that requested them is that the subject of personal data protection becomes more relevant in all areas of modern society.

In 2016, the largest number of requests for opinions were received in connection with the provision of data from and/or access to the NDB 'Population' maintained by DG GRAO at the Ministry of Regional Development and Public Works — a total of 44 requests. The main portion of data controllers requesting such access are banks and non-banking financial institutions.

The requests relating to public order, security and judicial system come second – a total of 15 requests.

Requests for opinions relating to the Telecommunications sector and the implementation of the Electronic Communications Act (EC Act) come next — a total of 7 requests. On the majority of occasions the CPDP was approached by the Communications Regulation Commission, which is indicative of the good interaction between the two institutions.

Six requests for opinions were made on issues relating to education and access to public information. In particular, the increased interest in the first of these two groups of opinions can be explained by the serious reform of pre-school and school education made in 2016.

The remaining requests for opinions concern specific issues relating to the scope of activity of specific data controllers and cannot be included in a common heading — a total of 51 requests (Figure 13).

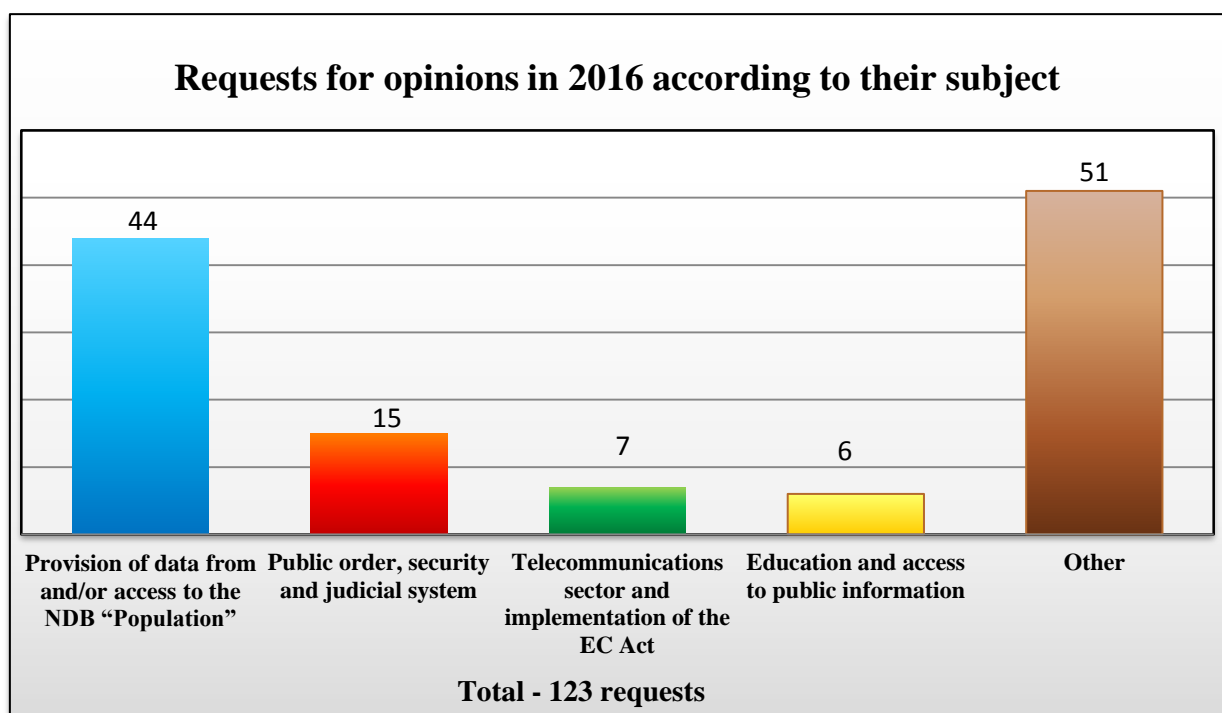


Figure 13

Within the Commission's mandate under Article 10(1)(8) of the PDP Act and in accordance with the coordination procedure under Article 32(1) of the Structural Regulations of the Council of Ministers and Its Administration, in 2016 the CPDP expressed opinions on a total of 32 draft statutory instruments and international agreements in terms of the protection of personal data and privacy of citizens. These include opinions on:

Draft national statutory instruments:

- Draft Decree of the Council of Ministers amending and supplementing the Implementing Regulations of the State Agency for National Security Act aimed at bringing the national legislation in accordance with 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 (PNR Directive);

- Draft Instruction amending and supplementing Instruction No 81213-1122 of 12 September 2015 on the procedure for processing of personal data at the MoI;

- Draft Instruction on the Preventive Activities at the MoI;

- Draft Implementing Regulations of the Electronic Identification Act;

- Draft tripartite agreement for data access between the Municipality of Troyan, the Ministry of Education and Science and the Ministry of Transport, Information Technology and Communications;

- Draft tripartite agreement data access between the National Social Security Institute, the Ministry of Education and Science and the Ministry of Transport, Information Technology and Communications.

Draft statutory instruments of the EU:

- Draft Regulation on the establishment of the European Public Prosecutor's Office;
- Legislative package in the field of migration and asylum;
- Draft Regulation for the establishment of an Entry/Exit System;
- Proposal for amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement and Directive 2013/34/EU as regards certain elements of the corporate governance statement;
- Proposal for amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Draft international agreements:

- Draft Memorandum of Cooperation between the Doctors of the World Association — France (an international non-governmental organisation) and SAR;

- Draft agreements for international operational police cooperation to which the MoI is party (with the USA, Mexico, China, Malaysia) — the main focus of this type of coordination is to ensure lawful exchange of personal data by identifying and clearly defining the objectives of the exchanges, the compliance with the basic principles of data processing, the introduction of appropriate technical and organisational measures, as well as the traceability and accountability of processing, thus safeguarding the rights of data subjects.

In its capacity as a coordinating authority in relation to specific legal instruments, the Commission for Personal Data Protection contributes to the introduction of clear rules for the protection of personal data, both with regard to the national provisions relating to the work of a single institution and with regard to international agreements to which the institutions are party.

VIII. Provision of Personal Data to Third Countries

In 2016 the CPDP expressed opinions on a total of 29 requests and notifications for the provision of personal data to third countries, as follows: 22 notifications based on standard contractual clauses, 6 requests for authorisations based on binding corporate rules, and one request based on an agreement between countries.

1. Standard contractual clauses

Based on contractual clauses, companies typically transfer personal data of their employees, clients and suppliers. It shall be noted that some of the notifications mention the transfer of personal data of third parties – close relatives of the aforementioned categories of individuals. The justification is that such data will be processed as contact information in emergencies. In such cases the CPDP requires that personal data controllers to comply with their obligations stemming from Article 19 and Article 20 of the PDP Act, and to provide evidence to this effect. Typically such evidence is in the form of a statement certifying the informed consent of the data subject.

When examining the notifications, the CPDP looks into the following:

- if the provided text of the transfer agreement reproduces in full the text of the standard contractual clauses — this condition was complied with in all notifications received during the reporting period;

- if the requirements envisaged in Article 19 and Article 20 of the PDP Act have been complied with. Following instructions provided by the CPDP, personal data controllers provide evidence of the fulfilment of this obligation, usually in the form of a statement confirming the informed consent of the data subjects. In this way the legitimate interests of the latter are protected;

- the applicable legal basis for the transfer of data under Article 4(1) of the PDP Act - on most occasions, the data controller states as ground for the data transfer the consent of the individual to whom the data refer (item 2) and the execution of an obligation stipulated by law (item 1).

Data is mainly transferred to EU countries and countries in the European Economic Area, and to third countries – mostly to the USA.

In connection with the latter and following the judgement of the Court of Justice of the European Union of 6 October 2015 delivered under case C-362/14 (Schrems), CPDP expressed the following view:

As an independent authority, the Commission carries into effect the protection of individuals in the processing of their personal data and the access to such data, i.e. exercises general supervision of the protection of personal data. In view of the fact that the transfer of personal data is a type of processing of personal data, it shall meet all requirements of the PDP Act. The assessment of its legality is within the competence of the CPDP, i.e. the existence of a decision of the European Commission finding that a third country guarantees a sufficient level of protection of the personal data transferred cannot revoke or reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and Directive 95/46/EC to exercise control over compliance with data protection rules.

2. Binding Corporate Rules

During the reporting period CPDP adopted five decisions for transfer on the basis of binding corporate rules. Data of employees, applicants for employment and clients is mainly transferred. Human resources management, employment and financial and accounting activities are stated as main objectives of transfers. On one occasion data of third parties – legal representatives and proxies, related to clients of the corporation, were subject to data transfer. Personal data controllers provide evidence of compliance with their obligations under Article 19 and Article 20 of the PDP Act. All of them have provided sufficient safeguards with respect to the protection of the privacy and the fundamental rights and freedoms of individuals. Transfers of personal data are made to all companies within the corporate group established and existing in a third country and bound by the Financial Intermediaries Act.

3. 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) with respect to oversees transactions of US taxpayers

In 2016 the CPDP received a request for transfer from the Executive Director of the NRA. The request was made on the grounds of Article 36b of the PDP Act in connection with the obligations of the Republic of Bulgaria to carry out automatic exchange of financial information with the United States under the concluded 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 (FATCA). In the specific case, the automatic

exchange of information with the US will take place in compliance with the Treaty on Avoidance of Double Taxation. Guarantees were provided that the information will be considered confidential and will be provided only to persons or authorities (including courts and administrative authorities) dealing with the identification, collection or administration, enforcement or prosecution, as well as the resolution of complaints relating to the taxes mentioned above, as well as with the oversight of the above. Such persons or authorities will use the information only for the purposes above, and can disclose it in legal proceedings or in holding judgements. The FATCA Agreement is of the utmost importance both for Bulgarian financial institutions and for expanding and increasing the effectiveness of the administrative cooperation with the USA in the fight against tax fraud and tax evasion. The processing of personal data by the financial institutions as well as by the NRA for the purposes of the automatic exchange of financial information by automatic means shall take place in compliance with the PDP Act and the international treaties to which the Republic of Bulgaria is a party. The use of automated means for processing personal data can have a significant impact on the data subjects. Therefore, this essential element must be taken into account when carrying out the impact assessment and undertaking the corresponding technical and organisational measures required in order to protect the data within the meaning of Article 23(1) of the PDP Act and when setting the deadlines for periodical reviews of the accuracy, adequacy and relevance of the data in relation to the purposes for which they were collected.

Having verified that the data controller providing the financial information (NRA) and the data controller receiving it (the US Tax Administration) have provided sufficient safeguards for the protection of personal data, the CPDP adopted a decision authorising the transfer of tax information, containing personal data, for the purposes of the regular exchange of such data between the governments of the US and Bulgaria.

4. EU—U.S. Privacy Shield Adequacy Decision

On 29 February 2016 the European Commission proposed a draft adequacy decision, establishing a new framework for transatlantic exchange of personal data for commercial purposes: EU—U.S. Privacy Shield (referred to as Privacy Shield), aimed at replacing the former Safe Harbour framework repealed by the Court of Justice of the European Union (CJEU) on 6 October 2015 in the *Schrems* case. On 12 July 2016 The Commission adopted the adequacy decision that protects the rights of EU citizens whose personal data are transferred to the United States and establishes legal clarity for undertakings relying on

transatlantic data transfers. The CPDP was actively involved in the discussion and decision-making process within the Article 29 Working Party. The Commission is also involved in efforts to inform EU citizens in a timely manner of the legal opportunities for protecting their interests under the new mechanism by publishing on its website a specially developed manual.

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

On 4 May 2016 the new EU legal framework in the field of personal data protection was published in the Official Journal of the European Union: 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.

The Regulation will be directly applicable in all Member States from 25 May 2018.

The Member States shall transpose the Directive in their national legislation by 6 May 2018.

The new General Regulation aims to modernise the existing rules on the protection of personal data in view of the rapid development of technology and globalisation. It will replace the Directive on the protection of individuals with regard to the processing of personal data, adopted in 1995. The Regulation introduces a number of new elements that provide citizens with greater control over their personal data in the digital world, while providing greater clarity and legal certainty and reducing the bureaucratic burden on businesses. The General Regulation also encourages the use of innovative technical solutions built on the principles of ‘data protection by design and by default’. The very serious financial penalties provided for in the General Regulation, amounting to up to EUR 20 million or 4 % of the total annual turnover of the company — data controller concerned, serve as convincing evidence of the importance of the horizontal privacy policy in the EU.

Immediately after the adoption of the two legal acts, the CPDP started preparing for the practical application of the new European data protection rules, including by starting the preparation of the legislative amendments necessary, clarifying the new rules and training data controllers, building administrative capacity, etc. A detailed action plan was adopted with clearly defined tasks, deadlines and responsibilities, and an interdepartmental working group was set up, which is planned to subsequently involve experts from other departments. Experts from the specialised administration of the Commission prepared a first draft of a structure of amendments and supplements to the PDP Act as a basis for the work of the working group.

The draft structure will be considered at a meeting of the CPDP. The CPDP representatives are actively involved in the discussions of the ad hoc expert group at the European Commission set up specifically to monitor and support the process of preparing Member States to implement the new rules. The CPDP experts were nominated and participated in the work of an interdepartmental working group at the MoI, set up with the task to analyse and make legislative proposals for the implementation in the national legislation 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.

The first information and explanatory materials on key new legal issues stemming from the General Data Protection Regulation were prepared and published.

X. International Activity

In 2016 the CPDP continued expanding and broadening its international activity. The key priorities during the year in this area were as follows:

- active involvement and contribution to discussions and initiatives within the EU aimed at preparing the practical implementation of the new European personal data protection legal framework after 25 May 2018;

- a joint application of the CPDP and the European Data Protection Supervisor to host the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2018;

- preparation of the CPDP for the implementation of the commitments stemming from the Bulgarian presidency of the Council of the EU in 2018 as part of the overall preparation of the government administration;

- further development of bilateral and multilateral cooperation with data protection authorities from other countries with a special focus on the countries in the region.

Joint application to host the 40th International Conference of Data Protection and Privacy Commissioners

In September 2016 the Commission for Personal Data Protection and the European Data Protection Supervisor (EDPS) officially submitted a joint application to host the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2018. The plenary part of the forum is planned to be held in Brussels, and two regional meetings are planned to be held in Sofia for the supervisory authorities of the Western Balkan countries and the Commonwealth of Independent States. The two capitals and the events held in them within the international conference will be connected in a video conference. 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 countries hosting of the conference is entrusted to have proven experience and capacity in the area of personal data protection and history of observing and respecting human rights and freedoms. At the end of the reporting period the Executive Committee of the International Conference had not decided yet on the choice of the host for the annual meeting of the Data Protection and Privacy Commissioners in 2018.

Participation in international data protection forums

Traditionally, most of the international participation of the CPDP members and staff is related to the EU working formats and the joint supervisory bodies, primarily the Working Party under Article 29 of Directive 95/46 EC and its expert subgroups, in particular ‘Future of Privacy’, ‘Borders, Travel and Law Enforcement’, and ‘Technology’. A leading topic on the agenda of the Article 29 Working Party in 2016 was the establishing of the future European Data Protection Board (EDPB) — a new EU structure with its own legal personality and the power to adopt binding decisions, which will become operational in May 2018.

The Chairperson of CPDP Mr Ventsislav Karadjov, who is also a Vice-Chairman of the Article 29 Working Party since the autumn of 2014, is a member of the management team monitoring the implementation of the action plan for the establishing of the EDPB. The re-election of Mr Karadjov as a Vice-Chairman of the Article 29 Working Party on 13 December 2016 under the conditions of strong competition is a convincing proof of the increased authority of the Bulgarian data protection authority within the EU. This election is even more important in view of the fact that during his new mandate the Working Party will be transformed into the future EDPB.

Extremely intensive discussions in 2016 were also held in connection with the new transatlantic framework for the transfer of personal data from the EU to the US — the so called EU — US Privacy Shield.

Legal experts from the CPDP, members of the team preparing the draft amendments to the PDP Act, participated in all meetings of the Expert Group at the European Commission on the implementation of the newly adopted General Data Protection Regulation and the Directive on Data Protection in Police and Criminal Justice Activities, set up in the autumn of 2016.

The CPDP representatives participated in the most important global and regional forums of the data protection authorities during the year: the 38th International Conference of Data Protection and Privacy Commissioners in Marrakesh, Morocco; the IAPP Global Privacy Summit in Washington, USA; the European Data Protection Conference in Budapest, Hungary; the Conference of Central and Eastern European Personal Data Protection Authorities in Sarajevo, Bosnia and Herzegovina; the Annual International Enforcement Cooperation in Manchester, United Kingdom; the 28th European Workshop on Case Studies in Podgorica, Montenegro; the 7th International Conference ‘Personal Data Protection’ in Moscow, Russian Federation. In addition to contribution of the discussions, in part of the forums Commission representatives presented presentations on specific topics such as video

surveillance, personal data protection in employment relationships, online risk assessment tools, etc.

In 2016 the participation of the CPDP in the work of the specially established joint supervisory bodies and supervision coordination groups of the large-scale information systems of the EU continued. These collective bodies are managed by the European Data Protection Supervisor 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 Supervision 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. A specific result of the work of these groups was the adoption of common models for the inspection and supervision of individual AISs.

It shall also be noted that the mandate of Mr Tsvetelin Sofroniev, CPDP member, as a Vice-Chairman of the Customs Joint Supervisory Authority was continued at the end of 2016. He took the position in December 2014.

Regional cooperation

In 2016 the tradition of the CPDP engaging actively in regional cooperation to assist other Western Balkan data protection authorities in building their capacity and harmonising their practice with European rules and standards continued. In this connection, during the reporting period the Commission hosted a working visit by a delegation from the Office to the Serbian Commissioner for Protection of Access to Public Information and Personal Data. The guests from Serbia had the opportunity to learn about the functioning and practice of the CPDP and to share experience relating to the European integration in the field of personal data protection. In 2016 the activity of expert support for administrative capacity building by the data protection authorities from Kosovo and the Republic of Macedonia also continued.

CPDP experts, together with MoI representatives, regularly participate in the meetings of the Personal Data Protection Working Party at the Police Cooperation Convention for Southeast Europe.

Preparation of the CPDP for the Bulgarian presidency of the Council of the EU in 2018

The CPDP participated actively in the process of preparation for the Bulgarian presidency of the Council of the EU during the first semester of 2018. The Commission will be the leading institution in Working Party on 'Information Exchange and Data Protection',

‘Data Protection’ format, and will nominate a chairperson, a deputy chairperson and a team of experts. Mr V. Karadjov, Chairperson of the CPDP, was appointed ‘Chairperson/Minister (chair of the format), and Mrs M. Mateva, CPDP Member, was appointed “Deputy Chairperson (Alternate Chairperson) / Responsible Deputy Minister (deputy chair of the format)’. With the relevant administrative orders, a team of experts from the Commission, nominated as part of the team of the Bulgarian presidency of the Council of the EU in 2018, was established. It includes a ‘lead expert’, a ‘support expert’ and four ‘other experts’. The Secretary General of the Commission holds the positions of a ‘national delegate’ and a member of the group of Secretaries General.

The experts designated as team members were assessed according to the Methodology for assessing the professional qualities and skills of the persons proposed to be included in the team for the Bulgarian presidency and the Methodology for verifying the English proficiency of the members of the Presidency team.

The necessary administrative actions were taken to keep the team’s data up-to-date on the portal of the Presidency. A team of CPDP coordinators in the different directions for preparation of the Presidency was also appointed, and the information was provided to the National Centre for the Preparation and Conducting the Bulgarian Presidency.

During the reporting period, the necessary organisational, technical and motivational actions for the establishing, strengthening and appropriate preparation of the team members proposed by the CPDP were undertaken.

Enhanced expert capacity of the CPDP team members is ensured by including them in the national training programme in relation to the Presidency – training events organised by the Institute for Public Administration, the Diplomatic Institute at the Ministry of Foreign Affairs and others, as well as by developing a CPDP programme for working visits and internships at the European Data Protection Supervisor and other institutions.

In connection with the preparation of the team of experts for the Presidency, in November 2016 three CPDP experts from the team took internships in three different EU institutions and bodies — the General Secretariat of the Council, the European Commission and the European Data Protection Supervisor. In addition to getting acquainted with the working processes in these institutions, the representatives of CPDP received valuable information about the expected legislative programme of WP ‘Exchange of Information and Data Protection’ for the first semester of 2018. For working visits and internships in EU institutions, additional expenditure in the amount of BGN 10 750 was approved for the year in the Commission’s budget with Council of Ministers Decree No 143/2016 amending and

supplementing Council of Ministers Decree No 125/2016 approving the forecast allocation of expenditure for the preparation and the conducting of the Bulgarian Presidency of the Council of the European Union in 2018 and additional costs for 2016 were approved. The funds spent for the working visits and internships amounted to BGN 6 339.

The preparation of the CPDP for the fulfilment of the commitments related to the Presidency will continue in 2017.

Readiness to fully implement the Schengen acquis — implementation of the plan of measures in the field of personal data protection, participation in Schengen evaluation missions

In 2016 the CPDP implemented its commitments stemming from the interdepartmental plan with measures on Bulgaria's readiness to fully implement the Schengen acquis. The 'Schengen Area' section of the Commission's website was fully updated, training events in the field of personal data protection were held for employees of institutions with access rights to the National Schengen Information System, and at the end of the reporting period information materials were adopted in the field of personal data protection for the employees of the representations of the Republic of Bulgaria abroad.

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 Italy and Malta. Mr Ts. Tsolov — CPDP member, is a member of the evaluation team for the implementation of the Schengen acquis in Italy, and Mrs M. Mateva — CPDP member, is the head of the evaluation mission in the field of personal data protection in Malta.

Preparation and implementation of international projects

At the end of 2015 a project proposal by the CPDP under the 'Erasmus+' Programme entitled 'Innovative Postgraduate Programme: Meeting Market Needs and Introducing New Models' was approved. The project was developed and submitted in partnership with the data protection authorities of Poland and FYROM and the universities of Lodz, Poland, and Ohrid, FYROM. 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 2016 the Commission participated actively in the implementation of the project activities. CPDP representatives prepared and conducted a large-scale study of the attitudes of the academic community and employers in Bulgaria towards the need for developing a postgraduate programme and its content. The study covered the leading universities in Bulgaria and some of the largest employers in the country. The Commission also hosted the first meeting of the project consortium partners held in Sofia in April 2016.

The project continues in 2017 with the development and appraisal of the academic curriculum. The deadline for its implementation is March 2018.

In November 2016 CPDP, in cooperation with NGOs, research centres and universities from 8 EU Member States — Germany, Italy, Austria, Belgium, Ireland, the Czech Republic, Greece and Cyprus, prepared and submitted a project proposal to the Directorate-General for Justice and Consumers at the European Commission. The draft proposal aims to stimulate judicial cooperation in civil matters in relation to the exchange of sensitive personal data of children and other vulnerable groups between the courts and other competent authorities in cases of international adoptions, parental responsibility and other family matters. The outcome of its assessment, as well as the possible commencement of activities, is expected in 2017.

The initiative for becoming part of the project consortium is a continuation of the CPDP policy for emphasis on protection of the rights and personal data of children and adolescents in all areas of public life.

XI. Training in the Field of Personal Data Protection

General information and statistics of training events held during the year

The Commission for Personal Data Protection 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 individuals and entities and public authorities that have the status of data controllers. One of the main tools for prevention and establishing uniform standards among personal data controllers from the private and the public sector is the conduct of training events. This obligation has been entrusted to the Commission with the PDP Act (Article 10(13)).

Based on the training needs analysis carried out by CPDP, two key priorities were identified for 2016: training events for organisations accredited for mediation in international adoption, and for the authorities entitled to access, update and delete alerts in the National Schengen Information System. Training seminars for magistrates and representatives of the judiciary together with representatives of the non-governmental sector were also organised.

In 2016, a total of 12 training events were held. Of these, 4 were for individuals processing personal data and having access to the National Schengen Information System, 3 — for representatives of the judiciary organized with the assistance of the International Cyber Investigation Training Academy, 3 training seminars — for representatives of organisations accredited for mediation in international adoption, one training event — for training of students at the University of Library Studies and Information Technologies, and one internal training — for staff in the CPDP administration. The total number of participants in training events in 2016 was 420 people.

Types of training events, comparative analysis of the training events held in prior years and during the current year, assessment and recommendations

In 2016, the CPDP decided to focus on conducting training events for narrowly specialised target groups instead of mass participation. For this reason the target groups of the training events were identified based on the CPDP priorities for the current and the past year: protecting the personal data of vulnerable groups such as children and continuing efforts in the area of personal data protection for accession to the Schengen area. In this connection, the training events during the reporting periods covered employees with access to the National Schengen Information System and representatives of organisations accredited for mediation in international adoption. Training materials were tailored to the needs of the target groups.

The analysis of the feedback from the training events held shows that they have achieved their objectives set in advance. Almost 87 % of the trainees find the training to be excellent or very good and only 3 % think it is just satisfactory. Three-quarters of all respondents who completed feedback questionnaires believe that one-day training sessions are sufficient. One in three participants has chosen to point out specific positive aspects of the training, including well-prepared lecturers, accessible and concise presentation of the material, presentation of case studies and possibility for dialogue with trainers. 13 % of the respondents specified at least one recommendation for improving the training process, the most common among them being conduct of upgrading training events, development of individual training programmes for each individual group of learners according to their functional obligations, as well as conduct of remote training for data controllers and persons processing personal data.

In 2016 the Commission continued the tradition to research the training needs of personal data controllers in order to increase its efficiency. More than half of the respondents to the CPDP survey in 2016 believe that they have a vague idea of the PDP Act and its application, as well as basic knowledge of the personal data protection issues. Two-thirds have never encountered problems with personal data protection. Approximately the same percentage of data controllers state that they are aware of their legal obligations and of the rights of individuals. There is consensus in the responses to the survey that the staff of data controller shall go through training — 97 % responded ‘yes’ and ‘mostly yes’, and half of the respondents felt that the training shall cover all employees. Most of the respondents (71 %) are of the opinion that training shall be held in the form of training seminars with presentations, and the main topics of interest are the legal framework and the measures for personal data protection and privacy. According to the survey, over 90 % of the respondents who participated in the survey would like to receive information materials relating to personal data protection, preferably in electronic form (Figure 14).

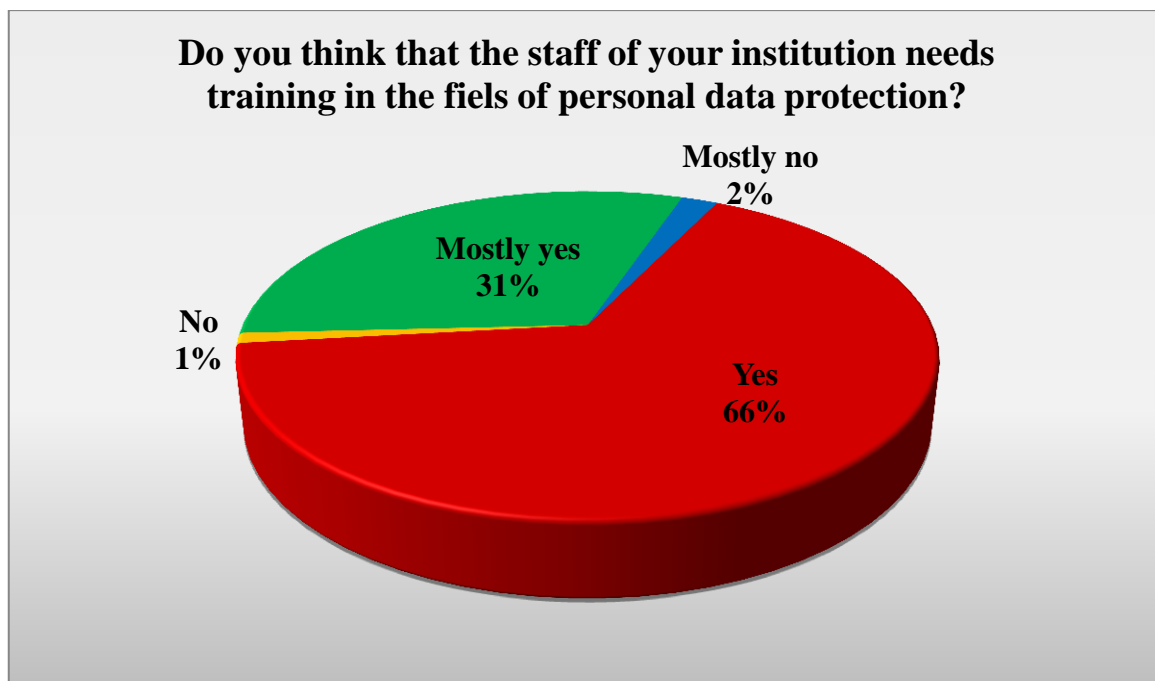


Figure 14

Part of the survey covers the attitudes and knowledge of citizens on the topic of personal data protection. In 2016, a total of 260 citizens responded to the questions of CPDP intended for individuals, as data subjects whose personal information is processed by a multitude of data controllers. 80 % have stated that they are aware of the content of ‘personal data’, and over 60 % assess their knowledge of the sector as basic. Over $\frac{3}{4}$ of the people surveyed claim that they know what their rights relating to personal data protection are, but over 70 % share that they have never exercised these rights. Over half of the respondents would like to receive information materials, most of them by electronic means. One of three participants thinks that his/her rights have been violated, and citizens perceive the following main actions as violations: copying of identity cards by mobile operators, use of telephone numbers for unsolicited advertising messages, and inadequate safeguards by personal data controllers (such as postal services, Internet sites, etc.).

Project for the construction of a training centre of CPDP

A legislation package of entirely new European data protection rules was adopted in the spring of 2016, including the General Data Protection Regulation and the Directive on Data Protection in Police and Criminal Justice Activities. They aim to modernise the existing rules on the protection of personal data in view of the rapid development of technology and globalisation.

The General Regulation which shall apply from 2018 introduces a number of new elements that provide citizens with greater control over their personal data in the digital world, while providing greater clarity and legal certainty and reducing the bureaucratic burden on businesses. The Regulation also provides for a completely new approach to training in the field of personal data protection. It introduces the figure of the so-called data protection officer, whose role will be to supervise the compliance with the rules for the protection of personal data within the organisation of a specific personal data controller. This person will also act as a point of contact with data protection authorities whose powers of control over data controllers have been strengthened (including by aligning and raising the level of sanctions on a European scale).

All this requires specialised and targeted training of data controllers 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. In this respect, one of the most pressing tasks of the future European Data Protection Board (a supranational European institution established by the new regulation) is the unification of curricula in the EU Member States and the introduction of uniform training standards.

Given the overarching nature of the European data protection reform, Member States have a two-year period to take all the necessary measures at national level to ensure the uniform application of the new legal framework. In this connection, during the period 2016—2018 CPDP as a national data protection authority shall organise and conduct information and education activities, as follows:

- a large-scale targeted information and training activity for personal data controllers to explain the new obligations deriving from the legal framework, including the obligations of multinational companies with multiple branches and offices in different Member States. This training activity shall also be adapted to their sectoral specifics and cover both the business and the government and the non-governmental sector. As of December 2016 the number of data controllers subject to clarifying activities in the field of personal data protection was approximately 359 000.

- conducting training events for personal data protection officers, which shall be appointed by a large number of personal data controllers (as of December 2016, the estimated number of data controllers obliged to designate or appoint a personal data protection officer was approximately 45 000, of which about 600 are from the public sector).

Currently, in view of the fact that the CPDP is the only body that conducts training in the field of personal data protection, in order to facilitate the public sector data controllers the

Commission has developed a training programme and participates with its lecturers in training events conducted by the Institute for Public Administration. This, however, is highly insufficient.

The fact that for a period of 6 years CPDP has managed to hold just over 100 seminars and train only 2 000 people from the public and private sectors, but is expected to raise the awareness of at least 45 000 data protection officers and 352 000 data controllers during the upcoming three-year period, speaks loudly about the need for a thorough rethinking of the currently existing approach to training. Therefore, in order to ensure the implementation of its information and educational initiatives, which result from the new regulation, during the reporting period CPDP launched an initiative for establishing a national training centre.

In view of the above, the construction of a training centre and providing the necessary human resources and facilities are among the main objectives of CPDP for the future. This would help increase the effectiveness and scope of training events conducted by the Commission, which in turn would automatically lead to easier and more adequate implementation of the new legal framework on personal data protection and reduce the administrative burden for citizens and the business.

XII. CPDP in the capacity of Data Security Supervisor under the Electronic Communications Act

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

The Commission for Personal Data Protection is a supervisor under the Electronic Communications Act (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.

During the reporting period 77 undertakings submitted information to the CPDP.

According to information from the Public Register of undertakings which have notified the Commission of their intention to provide public electronic communication services (Article 33(1)(1) of the EC Act), the number of such undertakings as of 25 May 2016 (the date as of which CPDP prepares its annual analysis) was 1 143. Like in previous years, the number of undertakings which submitted to the CPDP annual statistics did not correspond to the total number of obligated entities. This steady trend could be explained by the understanding of obligated undertakings that their legal obligation arises only if they have received specific requests for access to traffic data during the reporting year.

Based on the information provided by undertakings, the following statistics can be summarised in accordance with the requirements of Article 261a(4)(1—3) of the EC Act:

- the cases where data were provided to competent authorities under Article 250b(1) and Article 250c(4) totalled **70 543**, or **96 %** of all requests;
- the time elapsed from the initial date of storage until the date on which the competent authorities requested the transmission of data was mainly up to **3 (three) months** — in **74 %** of the cases;
- the cases where the request for provision of traffic data could not be responded to were **2 783**, which is a **four times increase** compared to the previous year.

- the total number of requests for access to traffic data was **73 326**, which is a **32 % decrease** on the previous year.

The main conclusions that can be made based on the summarised statistics under Article 261a(5) of the EC Act are as follows:

- The significant changes in the national regulatory framework introduced with the Act Amending and Supplementing the EC Act (AASEC Act), effective as of 31 March 2015, already have their practical effect.

- The decrease in requests for access to traffic data — by 32 % compared to the previous year, and the 4 times increase in the cases of failure to provide information are a logical and expected result of the higher requirements to competent authorities and the increased judicial control after 31 March 2015.

- The significant shortening of the periods for data storage introduced by the AASEC Act — from 12 to 6 months, actually corresponds to the practical needs of the competent authorities responsible for protecting national security and prevention, detection and investigation of serious crimes, as in the vast majority of cases the traffic data requested by these authorities have a storage period of 3 months.

At the end of 2016 CPDP updated its mandatory instructions to all entities under the EC Act in connection with the retention and processing of traffic data — undertakings, competent authorities under Article 251c of the EC Act, court and supervising prosecutor. Due to the legislative changes in the EC Act, amendments and supplements were prepared at the end of the reporting period in the mandatory 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.

2. Instruction No 1 of 21 December 2016 on the circumstances under which undertakings providing public electronic communications services shall notify consumers of personal data breaches, the form and manner of notification

In pursuance of its powers under Article 261d of the EC Act, at the end of the reporting period the Commission adopted Instruction on the circumstances under which undertakings providing public electronic communications services shall notify consumers of personal data breaches, the form and manner of notification. The Instruction is in compliance with the current legal framework in the field of personal data protection in Bulgaria and with the requirements of Commission Regulation 611/2013/EC on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic

communications. The statutory instrument was promulgated in the State Gazette, No 1 of 2017, and is effective as of 7 January 2017.

3. Statistics regarding received protocols regarding deleted traffic data

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 deleted data.

Based on the good interaction with representatives of undertakings providing public communications networks and/or services and on the experience already gained, at the end of 2016 the Commission, by its decision, streamlined the structure of the register under Article 251g(1) of the EC Act, respectively the standard form of the protocol regarding deleted data. This decision aims at helping all participants in the process by ensuring that their legal obligations are met in a high quality.

Statistics regarding the protocols received in 2016 is presented in Figure 15.

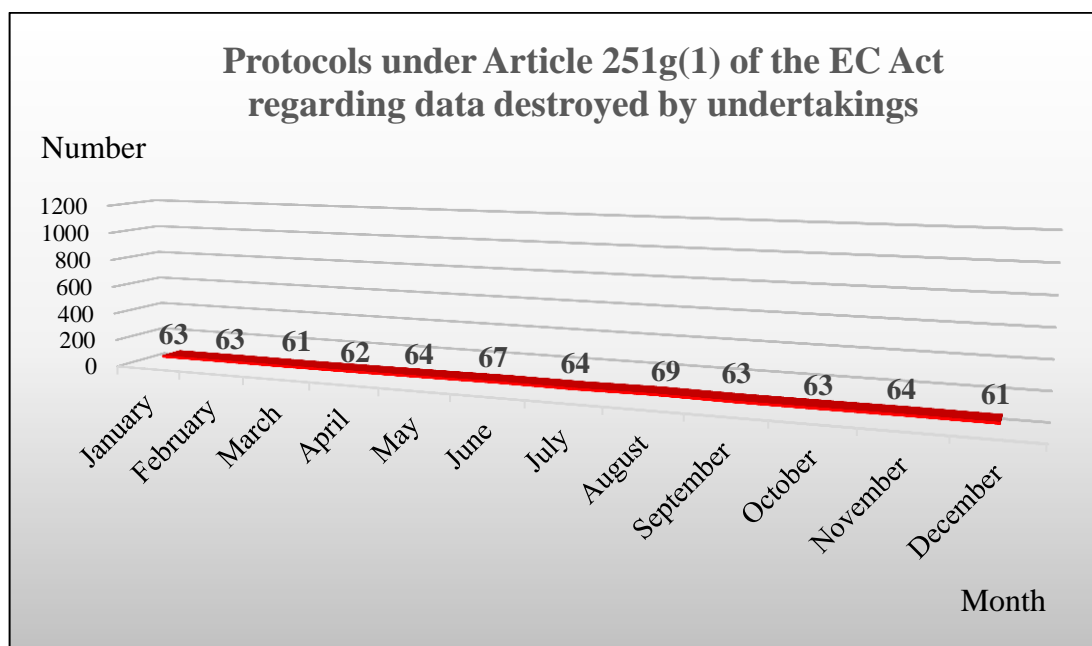


Figure 15

The number of undertakings that fulfil their obligation to provide monthly protocols regarding destroyed data under Article 251g(1) of the EC Act does not correspond to the total number of obligated entities. This trend could result from a possible interpretation of obligated entities that their legal obligation arises only if they have received a specific request for access to information during the reporting year, as specified above.

4. Implementation of the requirements of Commission Regulation 611/2013/EU on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications

In accordance with Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches, a software system for monitoring, reporting and processing of events of personal data breaches was developed during the reporting period. The introduction of the system aims at:

- providing quick and convenient access for providers of publicly available electronic communication services to registration of notifications of personal data breaches using the specially designed web application;

- providing quick and convenient access for providers of publicly available electronic communication services to submission to the CPDP of protocols regarding the data destroyed during the previous month;

- increasing the interoperability of management, and accelerating the flow of information processes within the CPDP;

- reducing the time and resources required for processing the received notifications of breaches;

- reducing the time and resources required for processing the received protocols regarding the data destroyed during the previous month;

- reducing the time and resources required for preparing information sheets.

Pursuant to Article 261c of the EC Act, in the event of a personal data breach the undertaking providing public electronic communication services shall notify the CPDP within three days of establishing such breach. Where the breach may adversely affect the personal data or privacy of a subscriber or another person, the undertaking shall notify the subscriber/the other person promptly.

Until now the CPDP has not been notified by undertakings providing public electronic communication services or citizens of events of personal data breaches.

XIII. Institutional Collaboration. Partnership with Media Representatives and Information Activity

1. Cooperation with government bodies and non-governmental organisations

In pursuance of its power to keep a register of personal data controllers and the registers kept thereby, CPDP interacts with DG GRAO at the MoRDPW with respect to granting access to personal data from NDB 'Population' about a specific individual in its capacity of personal data controller. This information is required for maintaining the register under Article 10(1)(2) of the PDP Act.

CPDP maintains an institutional interaction with GD GRAO also through any administrative proceedings relating to requests for access to data from ESGRAON (the civil register), which requires the CPDP to give permission under Article 106(1)(3) of the Civil Registration Act. Detailed information regarding the administrative proceedings considered by CPDP during the reporting period is presented in Section VII.

Since 2014, when CPDP for the first time started receiving complaints from individuals alleging unlawful processing of personal data in connection with elections, there is a need for cooperation between CPDP and the MoI, including the Research Institute of Criminology and Forensics at the MoI (RICF).

With the help of the MoI authorities, the possibility was provided for citizens who have filed complaints with the Commission, but have no opportunity to visit the CPDP, or for their convenience, to provide comparative materials in the place of residence before MoI officials. This possibility still exists in respect of complainants who have filed complaints in connection with the processing of personal data of citizens in the lists in support of participation in the elections for President and in the information campaign of the national referendum held on 6 November 2016.

In 2015 the CPDP finalised the procedures initiated on complaints filed in connection with the elections held in 2014 with the assistance of the RICEF, which carried out the expert assessments of signatures assigned by the Commission. The RICEF prepared over 200 expert opinions which clarifies the facts and circumstances around the filed complaints and determined whether such complaints were justified.

With regard to the complaints filed in connection with the processing of personal data of citizens in the lists in support of participation in the elections for President and in the information campaign of the national referendum held on 6 November 2016, the preparation

of expert opinions is forthcoming and the conclusions in them are of utmost importance in the formation and justification of the CPDP decisions.

In addition to the complaints above, the RICF prepares expert assessments of the authenticity of signatures in individual proceedings before the Commission on claims of absence of consent for personal data processing, respectively challenging circumstances related to signing of contracts or other documents.

In connection with streamlining the process of collecting the receivables under legally enforceable penal decrees and in order to improve the cooperation between the CPDP and the NRA, the bilateral instruction for interaction initiated by the Agency through the new e-service of NRA 'Acceptance of instruments from which the public claim of external creditors arises' is currently being finalised.

In connection with the elections for President and Vice President of the Republic of Bulgaria and the national referendum in 2016, the Commission developed together with the Institute for Public Environment Development an electronic manual 'My Personal Data' giving useful advice and information regarding the process for conducting elections and referenda. The manual was posted on the CPDP website in the 'I vote' Section and gives answers regarding the participation of citizens in elections and referenda and the collecting of personal data in this connection. It allows citizens to receive information about possible threats to their personal data and how to prevent them. The rights of citizens relating to the processing of their personal data are explained in detail and the basic safeguards against misappropriation of the signatures are presented. The electronic document raising the awareness of citizens also provides detailed information regarding the types of subscription lists and the protection of personal data in connection with each of them.

The already established institutional collaboration with the Central Electoral Committee in connection with holding elections continued during the reporting period. On the occasion of a request by the CEC, during the reporting period CPDP expressed an opinion regarding the capacity of electoral commissions to be appointed, parties, coalitions, initiative committees and organisations to be registered for participation in the election with observers or in the information campaign for the national referendum, as data controllers, respectively processors of personal data, and gave relevant instructions to them in the field of personal data protection. At the same time, in connection with citizens' allegations of misuse of their personal data in connection with the elections for President and Vice President of the Republic of Bulgaria and the national referendum, during the reporting period CEC constantly provided up-to-date information about the received complaints and alerts during the election

process and forwarded such complaints and alerts to CPDP. At the request of CPDP, information and evidence were also provided on the collected signatures of citizens supporting the registration of political entities and on the exact date on which political entities submitted to CEC the collected personal data.

In 2016 the CPDP issued a mandatory instruction to the Ministry of Regional Development and Public Works, Chief Directorate of Civil Registration and Administrative Services, to terminate the concluded agreements for access to the National Database 'Population', where the legal grounds and conditions required by law do not exist. In order to avoid legal vacuum and not to jeopardise effective credit ability reviews as an important element of the credit system, at the initiative of the Association of Banks in Bulgaria CPDP started an active dialogue with all stakeholders, resulting in a balanced and workable solution, fully compliant with the principles of legality and proportionality in the processing of personal data. At present, on the grounds of Article 106(1)(3) of the Civil Registration Act and on the basis of the consensus reached in the meetings, CPDP has issued 29 authorisations to banks for access to NDB 'Population'.

The development of interinstitutional links with different departments in the field of law enforcement was enhanced in 2016. The traditional cooperation with the Ministry of Interior and the State Agency for National Security in connection with the transposition of the new personal data protection legislation continues with participation in joint working groups and coordinating the international relations of Bulgaria in the field.

The joint activities of the CPDP with the Ministry of Justice continued during the reporting period, both in terms of coordination of the national position on individual dossiers of legal instruments discussed at European Union level, and on national issues. The foundations were laid for convergence with regards to differences identified in previous periods in the interpretation and implementation of the extant legislation regarding the cross-border processing of personal data of children. Experts from the Ministry and representatives of stakeholder NGOs participate in the basic data protection training. CPDP hopes that this would lay a good foundation for bringing closer the understanding of the main concepts and procedures relating to this specific activity.

In 2016, the cooperation with the NRA continued and new relations were established with the newly created Financial Intelligence Unit within SANS in connection with the discussion of the latest amendments to the European legislation on anti-money laundering measures. The participation in the working group on these issues at national level developed the interinstitutional relationship with the Ministry of Finance, whose representatives

participate in the working groups of the Council of the EU. The position of CPDP is taken into account within these groups as part of the national framework position on personal data protection in the development of the register of beneficial owners and the access to it.

In 2016, on the initiative of Mr Anton Gerunov, Head of the Political Cabinet of the Deputy Prime Minister for Coalition Policy and Public Administration, a working group was set up with the task to draft amendments to secondary legislation (preparation of draft Ordinance on the common requirements for information systems, registers and electronic administrative services), which needs to be brought in line with the provisions of the Act Amending and Supplementing the E-government Act effective as of 1 July 2016. In view of the fact that this Ordinance also discusses issues relating to the protection of personal information of citizens, the CPDP participated actively in the work of the group. The involvement of the Commission aims at ensuring the spelling out of rules for safeguarding the privacy of individuals and the technical and organisational measures necessary for security of personal information. The draft Ordinance was prepared and published on the website of the Council of Ministers for public discussion.

In the process of preparing two projects with EU funding in 2016 — under the ‘Erasmus+’ Programme and the Justice Programme of the EC, the CPDP established a partnership with the Sofia University ‘St. Kliment Ohridski’ and the International Cyber Investigation Training Academy (non-governmental organisation).

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

The consistent policy of the CPDP to provide to the public information about its activities and about the personal data protection in Europe and the world is reflected on the institutional website. News about events and initiatives in the field of personal data protection are published there. In the ‘Legal Framework’ section the main international and Bulgarian statutory instruments in the area of human rights and protection or privacy are published — laws, regulations, directives, rules. The ‘International Cooperation’ section provides information about the activities of supervisors and groups and the work of European and global forums and initiatives. Extremely detailed and updated information is provided regarding the Schengen area — legal framework, a manual for exercising the right of access to the Schengen Information System, catalogues of best practices. The right of individuals in the field of personal data protection in the Schengen area are described in detail. The practice of CPDP is presented — anonymised decisions on complaints, opinions, mandatory instructions, decisions of the SAC and the SCAC on appeals against the CPDP decisions are

published. Decisions and opinions regarding requests for transfer of personal data to third countries are publicised. Special forums for filing complaints through the website of the Commission and for asking questions are developed. There is an area for personal data controllers; they can find in the website detailed information about the registration process and have access to the information system eRALD through the CPDP website. Information is provided about the work on CPDP projects under different programmes. To study the public awareness and attitudes, questionnaires are provided for filling and expressing opinions.

Another information tool for the benefit of public awareness is the issued newsletter. The bulletin reflects events and initiatives in the field of protection of personal data both of the CPDP and in Europe and worldwide. Summaries of opinions of the European Data Protection Supervisor, the Article 29 Working Party, important judgements of the Court of Justice of the EU are published. International events and forums with the participation of CPDP representatives are reported here. Decisions and opinions of CPDP, statistics and analyses of control activities and the activities relating to the registration of personal data controllers are published. The newsletter has its own ISSN 2367-7759.

Every year, the CPDP celebrates the Day of Personal Data Protection, 28 January, with a number of initiatives. In 2016, in addition to the traditional events ‘Open day’ and ‘Open reception for citizens and personal data controllers’, the Commission emphasised on information and clarification activities. In January, information and educational materials on topical issues in the field of personal data protection were prepared and published in media with national coverage, as follows:

- Processing of personal data in NDB ‘Population’;
- Personal data in the Commercial Register;
- Provision of data of employees and clients to third countries by multinational companies;
- New European legal framework.

An annual award for journalism has been announced, to be given annually on the criteria of activity, objectivity and constructiveness. The first prize will be awarded on 28 January 2017. On the Day of Personal Data Protection, another initiative of public interest was announced — a competition with awards for children’s and pupils’ creative works (drawing, essay, poem) under the motto: ‘What others know about me?’ The distinguished children and pupils will receive their awards in 2017 on the occasion of the 15th anniversary of CPDP. Detailed information about the children’s competition is provided below.

In the years of its work, the Commission for Personal Data Protection has aimed at providing the highest possible level of awareness about its daily activities on long-term projects.

During the reporting period, due to the already established and facilitated personalised contacts between the Commission and media representatives, over 120 interviews and materials were realised with the participation of the Chairperson, members and experts from the 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. During the year, the 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 +, the Bulgarian National Radio ('Horizon' and 'Hristo Botev' Programmes), '24 Hours' newspaper, 'Trud' newspaper, 'Politics' newspaper, 'Monitor' newspaper, etc. The issue of misappropriation of personal data by various parties, coalitions and initiative committees in the collection of signatures in support of their participation in the elections for President of the Republic of Bulgaria and the referendum initiated by Slavi Trifonov attracted the greatest public interest in 2016. In this connection, the Chairperson of the Commission took part in a series of broadcasts on all national televisions and the general opinion of the participants is that the CPDP is performing its obligations well, because all complaints received are being dealt with as swiftly as possible and the relevant sanctions are imposed where violations are found. In these interviews, it was explained that citizens should not be concerned about the collecting of personal data to support certain political parties, but they should check whether the political parties comply with the law. The 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.

The Chairperson of the Commission Mr Ventsislav Karadjov participated in a press conference with the subject 'Elections and referenda: using personal data of citizens — risks and prevention', held in BTA (Bulgarian News Agency) on 19 September 2016 and organised by the Institute for Public Environment Development. He presented the role of the Commission for Personal Data Protection during elections and referenda, clarified the obligations of personal data controllers — who is a data controller and must register at the Commission, the obligations of parties/coalitions and initiative committees in the process of collection and storage of personal data, and presented findings from inspections carried out and made recommendations to the obligated persons.

3. Competition for children's creative works under the motto 'What others know about me?'

The broad possibilities offered by the rapid development of information technology allow for serious and often aggressive intrusion into the personal space of children. The adolescent group is the most vulnerable group in modern society in terms of privacy abuses, especially when communicating on the Internet. The practice of the CPDP shows that malicious actions often bordering on crime are frequently committed in the contract with well-intentioned naive and inexperienced children. Guided by its belief in the need to promote among children in school age the basic rules for safe communication in the social environment, especially through information technology and the internet, in 2016 the CPDP disseminated an educational and information video clip and announced a competition for children's and pupils' creative works. The motto of the competition is 'What others know about me?' Each child aged between 7 and 18 years is invited to participate in the competition with his/her creative work (drawing, essay, poem, short story, song). The aim of the competition is to introduce children at the earliest age to the importance of protecting their personal data by paying attention to the main risks and threats to the privacy of children on the Internet. The deadline for sending children's works is 30 April 2017. The assistance of the Ministry of Education and Science was requested so that the competition can cover the entire territory of Bulgaria. The initiative is a continuation of the information and educational campaign among children and adolescents held by the CPDP on the occasion of the 10th anniversary of the institution in 2012, where 6,600 information brochures were distributed and a competition under the motto 'Me and the Internet' was organised. Special attention is paid to the safety of children on the Internet and to raising awareness among children and parents about the importance of protecting personal data when working with the Internet and communicating online.

XIV. Administrative Capacity and Financial Resources

1. Administrative capacity

The ability of the CPDP as an administrative structure to fulfil its statutory tasks and respond to the public expectations is inextricably linked to the professionalism and motivation of its employees.

The Commission employs 57 members of staff under civil service relationships and 18 under employment relationships, and 7 of these (5 under civil service relationships and 2 under employment relationships) were appointed during the reporting period. The employment relationships with 8 members of staff were terminated. During the period January—December 2016, 7 members of staff were promoted in rank, and 1 member of staff was promoted in position.

During the reporting period 8 competitive procedures for filling vacancies in the CPDP administration were held, and 4 of them were completed with appointments.

For the CPDP, staff training is an important element of the human resources management function. During the reporting period 55 employees increased their professional qualifications by participating in training courses on the Annual Training Plan for 2016, conducted mainly by the Institute for Public Administration. Four newly appointed civil servants 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. Administrative services – procedures, access to public information under the API Act

In 2016 CPDP synchronised its activity of publishing information with the amendments to the Access to Public Information Act of December 2015 and February and July 2016. The purpose of these changes was to ensure transparency in the administration's activities and to facilitate the access to public information as much as possible. Over the years the CPDP has regularly published on its institutional website updated and detailed information on its activities, thus fulfilling in practice most of the requirements of the API Act defined by the amendments in 2015 and 2016, which introduced specific requirements for publication of information by public sector entities.

In accordance with the requirements of the API Act, in 2016 a section ‘Get Informed’ was included in the CPDP website. It includes:

- Procedure for reviewing requests for access to public information and provision of information for re-use, updated in 2016 to synchronise it with new requirements of the API Act;
- 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 databases 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.

3. Report on the requests for access to public information and requests for re-use of information received at CPDP in 2016.

Total number of received requests for access to information:	10
- from citizens of the Republic of Bulgaria	8
- from foreign citizens	0
- from media	1
- from NGOs	0
- from private individuals	1
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	3
Information provided under the procedure of providing administrative services or in accordance with the procedure of the APC	4
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	0

In 2016 the Editor in Chief of “Legal World” filed a request for access to public information concerning the provision of a complaint by a citizen and the corresponding decision of the CPDP on this complaint. The complaint is against the chairman of the Supreme Administrative Court and concerns the introduction of the practice of publishing on the SAC website of information containing personal data of an unlimited number of people – names, addresses, PIN, telephones, signatures. The access to this information is unrestricted and is achieved through the option for making inquiries on cases. With its decision on the complaint CPDP imposed a penalty on SAC.

During the reporting period an individual filed a request for access to public information concerning the rules for the organisation of the documentary turnover and the filing activity of CPDP.

On both occasions CPDP granted the applicants full access to the information in the form of copies of the relevant documents.

Through the Open Data Portal maintained by the Council of Ministers administration, CPDP provides and regularly updates in an open, machine-readable format for reuse the following public information that it collects, creates and processes:

- List of personal data controllers registered in the register under Article 10(1)(2) of the PDP Act;
- List of data controllers exempted from the obligation for registration;
- List of data controllers with denied registration.

In 2016, in order to improve the quality of administrative services in CPDP, a new Records Management Nomenclature was prepared and adopted. The Client Charter regarding the administrative services provided through the Electronic Portal for Access to Electronic Administrative Services was updated, and Internal Rules for Administrative Services in CPDP

regulating the organisation, coordination and general provision of the administrative services of CPDP were adopted.

Compared to the volume of correspondence processed in previous years, in 2016 a trend towards increasing the number of files processed in the record-keeping office of the CPDP was established. For the reporting period the Commission did not receive any complaints, alerts or objections relating to irregularities and deficiencies in the administrative services provided by the CPDP staff.

In its daily work, CPDP seeks to work in the public interest by providing high quality and timely administrative services to citizens and businesses. Efforts are constantly being made to improve the efficiency and quality of the work of the administrative staff in order to achieve better service, adequacy and empathy towards the problems of citizens, institutions and businesses.

Evidence of the high level of administrative services is the fact that at the end of 2016 the Citizens against Bureaucracy Foundation awarded the CPDP with a certificate for 'Best service to citizens'. The award was given for the first time to a government institution in Bulgaria. Given that the mission of the Citizens against Bureaucracy Foundation is to contribute to building and developing a well-organized civil society and create conditions for free access to accurate and true public information, and reduce the bureaucratic burden on citizens and businesses, the awarded prize is a strong attestation of the CPDP's work so far and an important incentive to continue in the future its efforts for protecting individuals and helping personal data controllers.

4. Public procurement

In order to provide resources for the activities of CPDP in 2016, public procurement procedures were awarded through the collection of tenders with announcement, as follows:

- '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 fuel and accessories for vehicles owned by the CPDP through cards for cashless payment';

- 'Complementing the functionality of the existing System for management of documents and workflows in CPDP and control of decisions, and streamlining certain processes in it'.

5. Acquisition of a new building

By Decision No 536 of the Council of Ministers of 30 June 2016, the Commission for Personal Data Protection was given a two-storey building with a built-up area of 540 sq. m. The CPDP plans to develop a training centre in the building and launch a large-scale training campaign targeting personal data controllers and specifically the individuals taking the new position of 'Data Protection Officer'. As the building has not been used and maintained for over 20 years, CPDP needs to carry out reconstruction and repair activities, as well as to purchase the necessary facilities, equipment and furnishings, in order to make it suitable for trainings. The following activities were carried out in this regard:

1. On the grounds of Article 2(1) of Ordinance No 5 on technical passports, a technical passport of the building was prepared.

2. Pursuant to the requirements of Ordinance No E-RD-04-1 of 22 January 2016 on the terms and procedures for performing an energy efficiency audit and certification of buildings, and for preparing an energy savings evaluation, an energy efficiency audit of the building was carried out, where energy saving measures are prescribed so that the building can be classified as energy class 'B'.

3. Based on the energy efficiency audit, an investment design for refurbishment and internal reconstruction of the building was prepared in order to convert it into a modern training centre of CPDP.

6. State of play of the implemented information and communication systems in CPDP in 2016

During the reporting period, the information and communication infrastructure of CPDP was further improved.

The increased volume of document turnover and the need to improve the interaction between the different administrative units and the administrative services in the Commission put on the agenda in 2016 the need to develop a new information system that would fully cover the activities of CPDP. In this connection, during the reporting period an audit of information systems was carried out and a business analysis for the implementation of an information system was prepared.

The business analysis made an overall assessment of the functionalities of the existing systems in CPDP and on this basis reached the conclusion that the existing System for management of documents and workflows in CPDP and control of decisions needs to be upgraded by introducing specific functionalities specially tailored to and related with the needs of the Commission. 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.

Employees participate actively in the planning and execution of contracts relating to the modernisation of information systems at CPDP.

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.

7. Financial resources – general information on budget spending of CPDP for 2016

In accordance with the 2016 State Budget of the Republic of Bulgaria Act and Council of Ministers Decree No 380 of 29 December 2015 on the implementation of the 2016 state budget of the Republic of Bulgaria, the approved operating budget of CPDP was BGN 2 283 000.

During the year the Commission’s budget was increased by BGN 16 006, of which BGN 10 750 in pursuance of Council of Ministers Decree No 143/2016 amending and supplementing Council of Ministers Decree No 125/2016 approving the forecast allocation of expenditure for the preparation and the conducting of the Bulgarian Presidency of the Council of the European Union in 2018, and for additional costs for 2016, and BGN 5 256 transfers received from the Ministry of Labour and Social Policy under a contract under the ‘Career Start’ Employment Programme.

After these changes, the budget of CPDP amounted to BGN 2 299 006.

The operational expenditure of Commission for Personal Data Protection and its administration amounted to BGN 2 274 449, or 98.93 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	1 093 837
02-00	Other remunerations and staff payments	57 681
05-00	Mandatory social insurance contributions paid by employers	276 217
10-00	Running costs	691 665
19-00	Taxes, fees and administrative sanctions paid	14 431
46-00	Expenditure on membership fees and participation in non-commercial organisations and activities	250
52-00	Acquisition of long-term tangible assets	44 436
53-00	Acquisition of long-term intangible assets	95 932
	Total budget expenditure	2 274 449

XV. CPDP Goals and Priorities in 2017

Given the entry into force of the new European legal framework for data protection in 2016 and the ensuing commitments of the Commission for Personal Data Protection at national and international level, the Commission has set the following goals for the upcoming reporting period:

1. Focusing the effort of CPDP in key areas of national and supranational importance

To achieve this goal, the Commission defined the following priorities in personal data protection activities:

- *Presidency of the Council of the EU*

The main priority area of the CPDP activities in 2017 will be the preparation for the successful implementation of the tasks resulting from the Bulgarian Presidency of the Council of the EU in the first half of 2018. The efforts will be focused both on building on the professional qualifications of the CPDP team involved with the Presidency and on defining specific topics in the legislative dossiers to be included in the agenda of the Working Party on Information Exchange and Data Protection during the period of the Bulgarian Presidency.

- *Hosting the 40th International Conference of Data Protection and Privacy Commissioners*

During the next reporting period, following a positive decision of the Executive Committee of the International Conference of Data Protection and Privacy Commissioners regarding the hosting of the 40th Anniversary Forum in 2018, the Commission for Personal Data Protection will launch jointly with the European Data Protection Supervisor the preparatory actions necessary for organising the event. The specific implementation of the individual activities will follow the plan-programme of this most important international forum in the field of privacy and personal data protection, already announced by the applicants.

- *Full accession to the Schengen area*

The activity in the field of personal data protection for Schengen accession and the preservation of the Schengen acquis as well as the continued participation of CPDP in Schengen evaluation missions remains a continuing priority in 2017.

2. Ensuring the readiness of Bulgaria to implement its commitments stemming from the new European legal framework in the field of personal data protection

To achieve this goal, the Commission defined the following priorities in personal data protection activities:

- *Institutional and legislative preparation for the implementation of the new legal framework*

The main part of the activities for preparing the amendments and supplements to the PDP Act based on the new EU rules in this field shall be performed in 2017. In this regard, one of the main directions in the work of CPDP next year, besides drafting the proposals for the necessary legislative changes in the field of personal data protection at national level, will be the deployment of an information and awareness campaign on the most important issues in the Regulation and the Directive, including the obligations of personal data controllers and data processors.

- *Development of a national training centre*

A major step towards the deployment of an information and education campaign remains the development of a national training centre in the field of personal data protection, intended primarily for distance online training for the persons appointed as personal data protection officers, and the appointing of the necessary staff. In addition, the efforts of CPDP over the next reporting period will be focused on the development of new curricula in line with the new European legal framework and the resulting changes in the national legislation, practical exercises and tests for assessing the knowledge acquired. This will make it necessary to change the traditional approach of CPDP of conducting on-site training according to a plan for the current year approved in advance.

- *Developing and commissioning of an information system in pursuance of the requirements of the new legal framework*

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

- register of personal data protection officers;
- register of certifying and accredited bodies;
- register of the organisations having codes of conduct;
- register of the internal violations of the Regulation;
- register of the measures taken in the course of exercising corrective powers.

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

To achieve this goal, the Commission defined the following priority in personal data protection activities:

- *Inspection in the Healthcare sector*

In the forthcoming reporting period, CPDP will build on the activity already carried out by conducting an inspection in the Healthcare sector, taking into account the experience accumulated in the field of control activities in previous periods, including the inspection in the Education sector in 2016. The leading criterion in selecting the sectors of social and economic life, which will be subject to inspections, remains unchanged, i.e. the processing of personal data of extremely large numbers of individuals and/or personal data expressly referred to in Article 5(1)(3) of the PDP Act, mainly related to the health of individuals.

The successful implementation of the goals and priorities set by the CPDP in the next reporting period will ensure stability of the protection of personal data in the national context and a better recognition of the institution in the Bulgarian society and among the foreign partners. The choice of objectives and priorities is aimed at a long-term perspective and sustainability of the results achieved.

The Annual Report of the Commission for Personal Data Protection for its activities in 2016 was adopted by a Decision of the Commission at a meeting held on 18 January 2017 (Protocol No 3).

CHAIRPERSON:

Ventsislav Karadjov (signed)

MEMBERS:

Tsanko Tsolov (signed)

Tsvetelin Sofroniev (signed)

Mariya Mateva (signed)

Veselin Tselkov (signed)