REPUBLIC OF BULGARIA

COMMISSION FOR PERSONAL DATA PROTECTION

ANNUAL ACTIVITY REPORT

of the Commission for Personal Data Protection

for 2015

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

TABLE OF CONTENTS

List of the acronyms used in this document

PDC	–	Personal data controller
APP	–	Administrative-penal proceedings
APC	–	Administrative Procedure Code
SAA		Social Assistance Agency
SCAC	–	Sofia City Administrative Court
SEAV	–	Statement establishing an administrative violation
SAC	–	Supreme Administrative Code
VIS	–	Visa Information System
GD GRAO	–	Chief Directorate of Civil Registration and Administrative Services
CG	–	Consulate General
CPC	–	Civil Procedure Code
EU	–	European Union
SACP	–	State Agency for Child Protection
SANS	–	State Agency for National Security
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
CR Act	–	Commercial Register Act
eRALD	–	CPDP's electronic system for registration of personal data controllers
AVP Act	–	Administrative Violations and Penalties Act
BID Act	–	Bulgarian Identity Documents Act
CReg Act	–	Civil Registration Act
SBRB Act	–	State Budget of the Republic of Bulgaria Act
EC Act	–	Electronic Communications Act
EG Act	–	Electronic Governance Act
PDP Act	–	Personal Data Protection Act
HI Act	–	Health Insurance Act
MoI Act	–	Ministry of Interior Act
MAML Act	–	Measures Against Money Laundering Act
PP Act	–	Public Procurement Act

CI	–	Compulsory instruction
Acc Act	–	Accountancy Act
PS Act	–	Private Security Act
ElC	–	Election Code
IPA	–	Institute of Public Administration
SF	–	Statement of findings
ACCIPEC	–	Anti-Corruption, Conflict of Interests and Parliamentary Ethics Committee at the National Assembly
QES	–	Qualified electronic signature
CPDP	–	Commission for Personal Data Protection
CEIBG	–	Confederation of Employers and Industrialists in Bulgaria
MoI	–	Ministry of Interior
MFA	–	Ministry of Foreign Affairs
CIS	–	Customs Information System
MoRDPW	–	Ministry of Regional Development and Public Works
NRA	–	National Revenue Agency
NDB "Population"	–	National Database "Population"
ENU	–	Europol National Unit
NHIF	–	National Health Insurance Fund
RICF	–	Research Institute of Criminology and Forensics
OGROAS	–	Ordinance on the general rules for the organisation of administrative services
PD	–	Penal decree
CrPC	–	Criminal Procedure Code
NSIS	–	National Schengen Information System
OPAC	–	Operational Programme "Administrative Capacity"
RACPDPA	–	Rules on the activity of the CPDP and its administration
PP	–	Political Party
WG 29	–	Working Group under Article 29 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
CEC	–	Central Electoral Commission

I. Introduction

This Annual Report of the Commission for Personal Data Protection (CPDP) is drawn up in accordance with Article 7(6) of the Personal Data Protection Act (PDP Act) and covers the period 01 January 2015 — 31 December 2015.

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 registration of personal data controllers (PDCs), the control and administrative-penal activities and the projects implemented with national and European funding during the year. Statistics and aggregated information on inquiries from citizens and the consultations related thereto are presented. Due attention is paid to activities relating to international cooperation and training events held in the field of data protection.

The Report also discusses the information activities and the activities relating to the media policy and promotion of the CPDP. The actions undertaken by the CPDP in connection with the improvement and expansion of electronic services to businesses and citizens and the introduction of complex administrative services are identified.

The degree of achievement of the objectives and priorities set for year 2015 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 Commission for Personal Data Protection set in the 2014 Annual Report

In 2015 the CPDP managed to achieve most of the objectives and priorities set in the 2014 Annual Report.

During the reporting period the CPDP was among the government institutions which formed part of the e-government of the Republic of Bulgaria. The implementation of the project entitled "Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services" contributed to the expanding and improving the electronic administrative services provided to the business and individuals by the Commission and to the enhanced quality of the services provided. In line with the e-government strategy adopted by the government, all electronic services offered shall be accessible via the single point of access to administrative e-services. With the completion of the project in 2015, the strategy became a reality in the field of personal data protection. The project objectives and outcomes are in full compliance with and helped achieve two specific objectives of Operational Programme "Administrative Capacity" (OPAC), namely: *Effective functioning of the administration* and *Contemporary services provided by the administration*.

In connection with the introduction and implementation of complex administrative services, in 2015 the CPDP approved standards for administrative service, provided more opportunities for open communication with citizens so that they can share opinions and recommendations, respectively give feedback when they are not satisfied. This ensured compliance of Commission officials with the ethical standards of conduct stipulated in the Code of Conduct for Civil Servants, which in turn increased public confidence in the professionalism and morale of the Commission and ensured higher level administrative services.

A main priority in relation to the control activities of the Commission was the conducting of sectoral inspections and the need to change the approach to the selection of personal data controllers to be included in the scope of sectoral inspections. The objectives of these inspections were to create conditions for uniform implementation of data protection rules by PDAs with similar scope of business. In connection with this priority, in 2015 the CPDP assigned a working group of experts from its administration to prepare a draft methodology for sectoral inspections. Several key criteria were taken into account in the development of the methodology: the existence of a large number of PDAs in individual

sectors of public life; the processing of specific categories of personal data by PDAs; the different legislation regulating the operations of PDAs with similar scope of business;, and the experience of other European Union (EU) Member States conducting sectoral inspections. The working group is close to completing its work and the adoption of the methodology by the CPDP is forthcoming, so that it can be implemented in practice in the control activity in 2016.

With regard to achieving the priority of the Republic of Bulgaria – full accession to the Schengen area in 2015, the CPDP nominated before the European Commission its representatives to participate in Schengen evaluations in the field of personal data protection in Belgium, Germany, the Netherlands and Liechtenstein, and the Member of the Commission Maria Mateva was selected as a leading expert (head of the group of experts) for the evaluation in the Netherlands.

In addition, the CPDP participated in the working group established by an order of the Minister of Interior with the task of carrying out a self-assessment under Schengen to ensure full implementation of the Schengen acquis. Taking into account the international experience gained in the course of conducting Schengen evaluations, the Commission proposed that 10 measures relating to issues of its competence be included in an interdepartmental action plan.

For the purpose of creating the necessary conditions for the introducing of the so called Data Protection Officer in Bulgaria after the draft general data protection regulation, special attention was paid to this topic during the international conference entitled "Trust, Privacy and Security of Personal Data in the Digital Age". When the new figure of data protection officer was presented, the presentation on the topic discussed the advantages and disadvantages of the mandatory and/or optional introducing in European legislation of a data protection officer, respectively the obligations that arise for data controllers in this respect.

As a result of the completed inspections of political entities acting as data controllers and the complaints by individuals against unlawful processing of their personal data for registration of political entities in the election, examined by the Commission, the CPDP identified certain problem areas in electoral legislation with respect to the obligations of political entities in the electoral process. In 2015 the CPDP developed and disseminated guidelines to all political entities acting as personal data controllers and also made recommendations to citizens regarding the protection of their personal data in the election process for the purpose of registration of political entities. The successful cooperation with the Central Electoral Commission continued during the reporting period. As a result, the complaints against political entities declined significantly.

The CPDP's priority to strengthen its international activity at all levels aiming at maximum contribution to the work of European data protection authorities, formulation of European policies and strengthening the role of the Republic of Bulgaria as an active member of the EU, was achieved to a large extent. This was achieved firstly by formulating and defending at EU working formats of consistent and well-grounded positions on key aspects of the two legislative proposals to reform the EU legal framework in the field of data protection – the draft General Regulation and the Directive for processing of personal data in policing and prosecution activity. The CPDP contributed to the clear positioning of Bulgaria in the group of Member States which insist on upgrading and improving existing standards for the protection of citizens' personal data – a position fully shared by the European Parliament. Another specific result in this area during the previous year was the developing of a very good working cooperation with the European Data Protection Supervisor, evidence to which was the personal presence and welcome of the head of the institution Giovanni Buttarelli to the participants in the international conference "Trust, Privacy and Security of Personal Data in the Digital Age" held in Sofia.

In 2015, the CPDP continued as a priority to build on its activities for protection of personal data of children and adolescents by directing its efforts towards synergies with partner institutions and stakeholders. The CPDP is among the initiators and active participants in an interdepartmental working group comprising representatives of the State Agency for Child Protection, the Social Assistance Agency, the Ministry of Justice, Ministry of Foreign Affairs and other institutions on the problems of international transfers of personal data, including sensitive personal data of children and their parents. Based on the information collected and the needs identified in this area, the CPDP is currently preparing a proposal for an international multidisciplinary project with EU funding under the EU Justice Programme aimed at facilitating judicial cooperation in civil matters of parental responsibility, international adoptions, etc., requiring the exchange, processing and storage of large amounts of personal data, including sensitive personal data, of children and other vulnerable groups.

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

Pursuant to Article 10(1)(2) of the Personal Data Protection 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 consistent with the e-Government concept and aims to provide citizens with a highly efficient and user-friendly service based on the "single window" technology. This activity is performed based on the information system for electronic registration of personal data controllers (eRALD). The system is a web-based application accessible from the CPDP'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 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.

During the reporting year the Commission implemented a project entitled "Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services", OPAC, financing contract Reg. No 13-32-13 of 11 February 2014, Priority Axis III "Quality administrative services and e-government development", Sub-priority 3.2: Standard information and communication environment and interoperability, budget line BG051PO002/13/3.2-04. The main objective and purpose of the project is to introduce new and improve the existing electronic administrative services of the CPDP for citizens and businesses, thus providing an opportunity to reduce the administrative and bureaucratic burden on their activities. In the course of the project implementation, two new functionalities of e-RALD were introduced allowing to perform electronically the following processes and operations:

- Impact assessment and determining the level of protection of personal data registers;
- Carrying out ex-ante, ongoing and ex-post inspections for compliance of PDCs with the requirements of the PDP Act;
- Automated receiving and processing of data regarding traffic data retained by undertakings providing public electronic communication networks and/or services;

- Support for people with disabilities in the use of electronic services offered by the CPDP;

- Deregistration of personal data controllers and the registers kept thereby from the public register of PDCs;

- Processing of the processes relating to re-registration, merger, separation and deregistration of legal entities regarded as PDCs;

- Introduction of a tracking system that helps citizens in filling out electronic documents.

In addition to the above, some existing functionalities of the eRALD information system were further developed and updated, as follows:

- Integrating the access to electronic services offered by eRALD with the Single point of access to administrative e-services;

- Developing a standardised interface for electronic access from other information systems of the administration and businesses;

- Registration and processing of PDCs that do not have a unified identification code (UIC);

- Updating the registration and processing of individuals and legal entities by an authorised representative;

- Expanding and upgrading the module generating reports;

- Optimising the system for electronic communication with PDCs registered in e-RALD.

In 2015, PDCs continued to use widely the web-based registration service, including by means of Qualified Electronic Signature (QES).

Between the inception of eRALD in 2009 and 31 December 2015 the number of system users reached 350,385, of which 319,654 applied for PDC registration and 30,731 requested an exemption from the registration requirement (Figure 1).

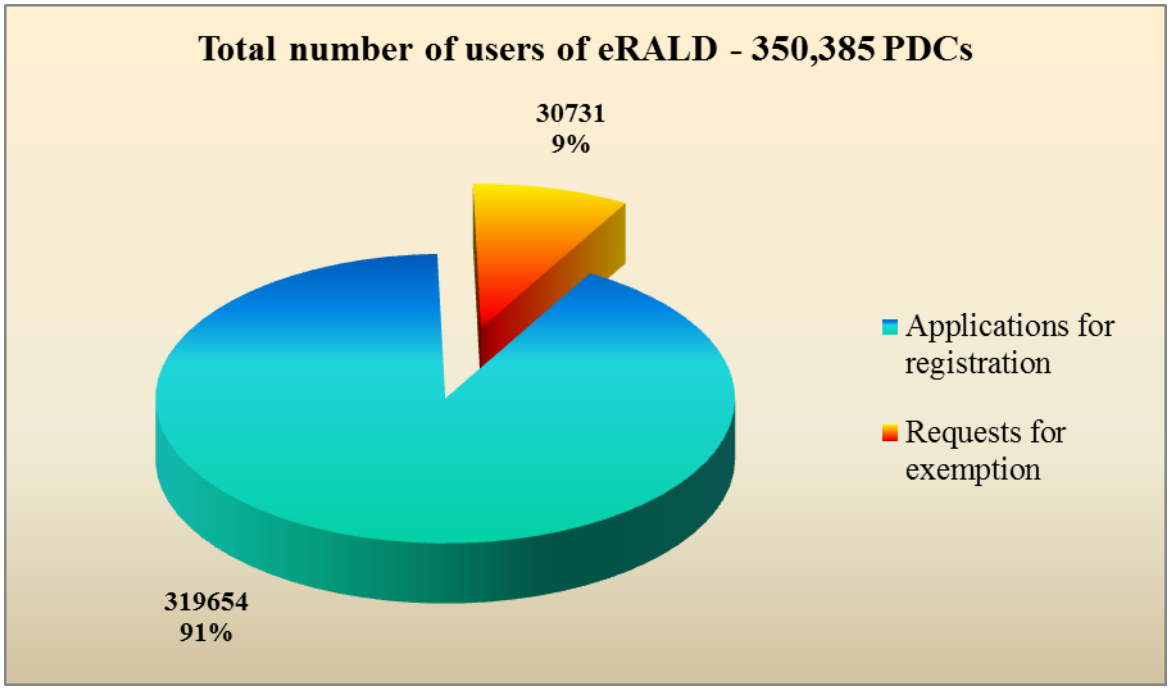

Figure 1

In 2015, the CPDP registered further 5,347 PDCs in the PDC Register. Thus, the overall number of registered PDCs became 278,416 (Figure 2).

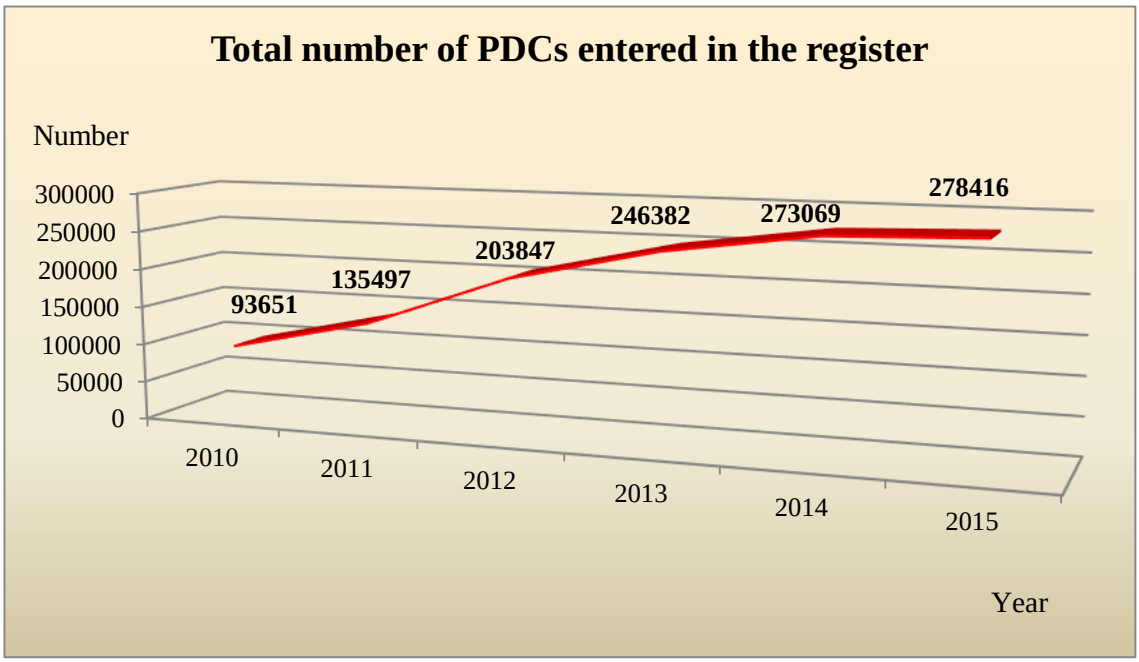

Figure 2

Of the 30,731 PDCs which applied for exemption from the registration requirement by 31 December 2015, the CPDP by its decisions exempted 27,671, including 174 during the reporting period (Figure 3).

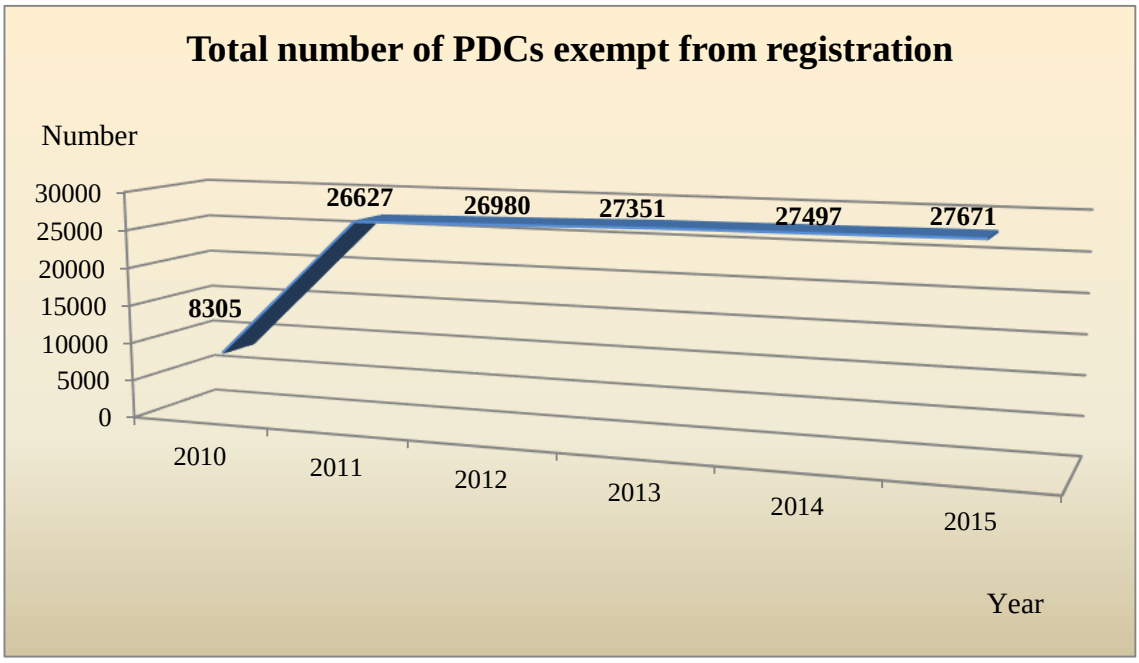

Figure 3

During the reporting period, the CPDP received 89 applications for deregistration of PDCs and adopted decisions for delisting these applicants from the PDC Register.

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, 424 controllers were subjected to ex ante inspections before entry in the PDC Register as per Article 10(1)(2) of the PDP Act. In 2015 the CPDP did not adopt any decisions for refusal to register PDCs in the register on the grounds of Article 17b(3)(3) of the PDP Act.

When comparing the data relating to the registration of personal data controllers and the personal data registers kept thereby with data from previous years, we can draw the following conclusions:

- The diagrams in Figure 2 and Figure 3 show that the rate of increase in the number of registered PDCs decreases over the years and the number of controllers exempt from registration remains unchanged, suggesting that the processes related to registration enter a steady state.

- For a third consecutive year the ratio of the number of applications for registration to the number of applications for exemption remains unchanged, respectively 91 % to 9 %, which can be defined as a trend.

IV. Protection of the Rights of Individuals in Relation to the Processing of Their Personal Data

1. Proceedings related to the examination of complaints and requests. Statistics and analysis of the complaints and requests received by the Commission

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 Personal Data Protection Act.

A complaint can be submitted only by an individual in connection of a violation of his/her rights. In the event that an individual reports of 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.

We shall draw attention to the fact that an individual can refer the case to the relevant competent court, but this right cannot be exercised if there is a pending proceeding before 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 ability to protect the rights, provided for in the PDP Act, is available to all individuals.

In recent years we observed a constant upward trend in the number of complaints filed with the Commission. This circumstance is due both to the increased activity of citizens in the field of protecting their rights and to the judgments of the Court of Justice of the European Union which ensures the proper interpretation and application of primary and secondary Union legislation in the EU. The judgments of the Court in the field of video surveillance and processing of personal data in social networks (the Facebook case) and by operators of software that allows Internet searches (the Google case) require an analysis on the introduction of measures to regulate these public relations relating to the processing of personal data. The technological development and the developments in the information society services can also be a reason for the increase in complaints.

The total number of complaints considered in 2015 was 817. Of these, 545 were filed against political entities in 2014 and 250 were filed in 2015. The total number of complaints filed with the CPDP during the reporting period was 567.

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 50 complaints, submitted (including during the previous year) without the mandatory requisites to be regular. It should be pointed out that when an irregular complaint is received, a letter to the sender with instructions for removing the irregularities is prepared. Instructions are sent to the sender of the complaint 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. In addition, individuals tend not to understand the procedure for filing complaints regardless of the instructions given to this end. 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.

In 2015 the Commission left without consideration 46 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.

On any admissible complaint, actions are carried out to clarify 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 person 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 Commission for Personal Data Protection delivers a decision in the form of an administrative instrument, which is subject to judicial control.

In its decision the Commission can give compulsory instructions, set a deadline for eliminating the violation or impose an administrative penalty.

In 2015 the complaints considered unjustified were 101, and those justified were 75. This statistics does not include complaints against political entities received in 2014.

During the reporting period the Commission imposed 74 administrative penalties for violations established in the course of administrative proceedings and issued 27 CIs 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): 8 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 138,000;

- Processing of personal data in the absence of a lawful reason for the data processing operation (Article 4 of the PDP Act): 28 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 445,700;

- 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): 15 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 18,800;

- 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: 12 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 43,500;

- Non-compliance with Article 19 of the PDP Act – failure of the PDP to provide information to an individual where personal data have been collected from the individual to whom they refer: 1 violation was established, in respect of which the CPDP imposed a sanction in the amount of BGN 3,500;

- Non-compliance with Article 24(6) of the PDP Act – the personal data controller or any person acting under the guidance of the data controller or of the data processor who has access to personal data, processes such data without instructions from the data controller: 1 violation was established, in respect of which the CPDP imposed a sanction in the amount of BGN 3,000;

- Non-compliance with Article 34a(2) of the PDP Act – the data controller failed to inform the individual of his/her rights to object against the processing of his/her personal data for the purposes of direct marketing: 3 violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 4,000;

- Non-compliance with Article 32(1) of the PDP Act – the 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 1,000;

- Failure of the PDCs to assist the CPDP exercise its supervisory powers (Article 22(5) of the PDP Act): two violations were established, in respect of which the CPDP imposed sanctions in the total amount of BGN 4,000.

In its practice, the Commission for Personal Data Protection also rules on resumptions of administrative proceedings and stays of the 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 2015 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 APC (where other administrative or judicial proceedings were initiated and the instrument cannot be issued

before their completion), the Commission for Personal Data Protection stays the administrative proceedings instituted before it.

During the reporting period the Commission stayed 16 administrative proceedings.

It shall be pointed out that outside the statistics above, in 2015 the Commission for Personal Data Protection concluded the proceedings initiated on complaints from individuals concerning the processing of their personal data for registration in the Central Electoral Commission of political parties and coalitions of parties for their participation in the 2014 elections for members of the Republic of Bulgaria to the European Parliament and members of the National Assembly.

Complaints filed in connection with the elections for members of the Republic of Bulgaria to the European Parliament were 496, and complaints filed in connection with the elections for members of the National Assembly were 47. Subsequently, requests for withdrawal were received in connection with 2 complaints. The number of complaints received at the CPDP in connection with local elections was even lower – 14 complaints filed by 9 complainants.

The figure (Figure 4) shows the number of complaints received at the CPDP in connection with the elections held:

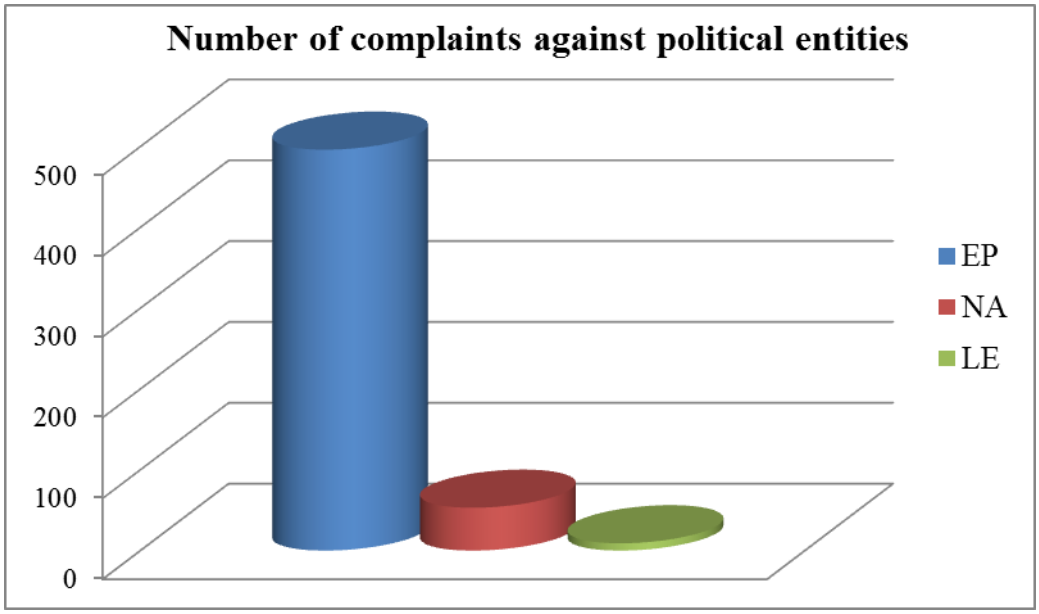

Figure 4

After the Research Institute of Criminology and Forensics (RICF) prepared expert opinions on the authenticity of signatures of voters, in June 2015 and in September 2015 the CPDP conducted open hearings on the complaints.

As a result of the concluded administrative proceedings, the CPDP imposed with administrative instruments sanctions with a total amount of BGN 36,100 to 23 political entities for non-compliance with Article 23 of the PDP Act.

The reduced number of complaints filed in connection with the election for representatives to the National Assembly is reflected in the sanctions imposed on political entities – defendants in administrative proceedings on complaints regarding the election of representatives to the National Assembly. The total amount of sanctions was BGN 8,000, and they were imposed on 12 political entities.

The ratio of the sanctions imposed is presented in the figure below (Figure 5):

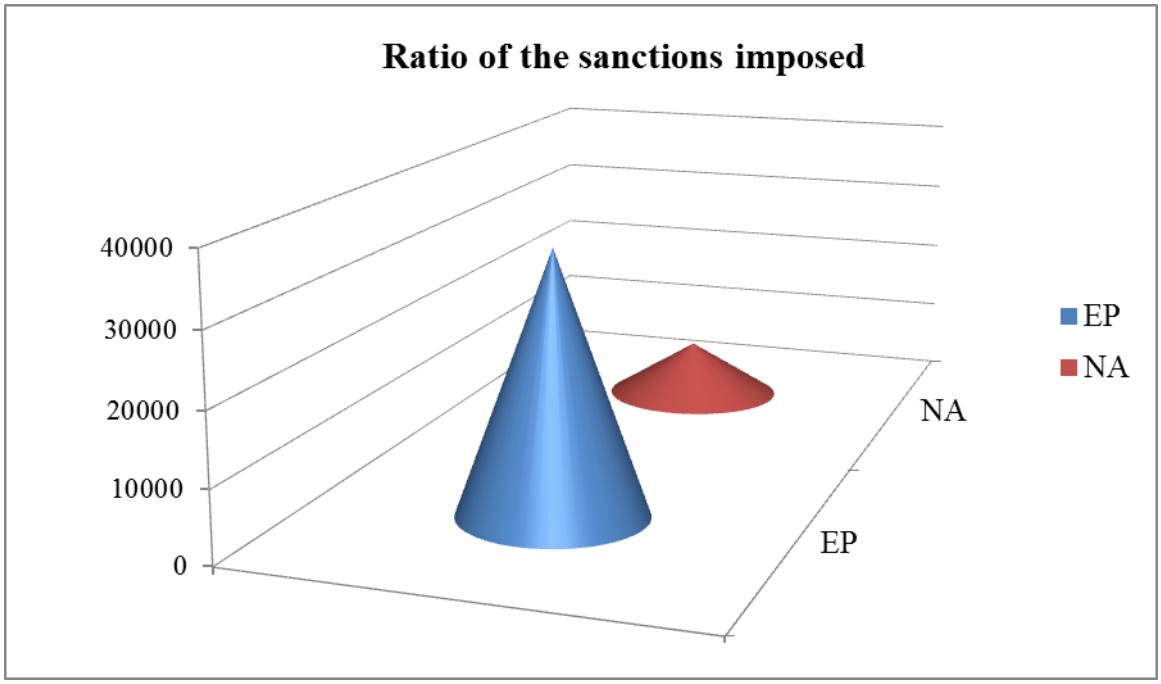

Figure 5

Comparative analysis of the complaints received at the CPDP during the current year and previous years based on the type of personal data controllers

During the reporting year an increase was observed in complaints filed in connection with the processing of personal data by CCTV. During the calendar year, 35 complaints alleging processing of personal data through video surveillance were filed. The complaints were against individuals – building managers or neighbours of the complainants, and against employers and/or judicial institutions.

In connection with the correct constituting of the defendant for the consideration of such appeal, the CPDP took into consideration 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 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 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.

The judgment above analyses a situation where an individual "has installed and used a camera system located under the eaves of his family home ... the only reason for operating the camera was to protect the property, health and life of his family and himself" – items 12 and 13 of Judgment of the Court dated 11 December 2014.

The considering of the judgment of the court was necessary in view of the similarity between the subject of Case C-212/2013 and the subject of the complaints referred to the Commission.

Pursuant to the provision of Article 1(9) of the PDP Act, this Act shall not apply to personal data processing by individuals for their personal or household activity, and in the recent case-law of the Commission the absence of the capacity "building manager" as one of the hypotheses of an individual, having the capacity of personal data controller, is a prerequisite for leaving the complaint without consideration as inadmissible due to the absence of a defendant and for terminating the administrative proceedings due to a legal obstacle to exercise the powers of the administrative authority.

The judgement of the Court of Justice of the European Union in reference for a preliminary ruling is of general application and binds the national court that referred the specific case to it, the EU institutions and Member States, and 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. In this sense, in their practice data protection supervisors shall take into account the following opinion of the Court of Justice of the EU: "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".

As a consequence of the said judgment, and as a result of the binding nature of the judgments of the Court of Justice of the European Union, the exception in Article 1(9) of the PDP Act, according to which the provisions of the special PDP Act shall not be applicable to personal data processing for personal and household activities, shall be narrowly construed.

The Commission justified its consideration of complaints received using the contents of Items 29 and 30 of Judgement of the Court in case C-212/13 of 11 December 2014, pursuant to which "since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter, the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed", and "this narrow construing has its basis also in the very wording of that provision, under which the directive does not cover the processing of data where the activity in the course of which that processing is carried out is a 'purely' personal or household activity, that is to say, not simply a personal or household activity".

In this sense, each case related to video surveillance by individuals shall follow the consideration of the legal grounds set out in Article 4(1) of the PDP Act.

Next, during the reporting year the Commission ruled in two cases related to the processing of personal data by Internet sites that provide searching and finding on the internet of information, including personal data. The case-law of the Commission is related to the Judgment of the Court of Justice of the European Union in case C-131/12 regarding a request of s citizen of Spain to have the information relating to his names and disclosed by a Spanish daily newspaper and the internet search engine Google withdrawn due to lapsed grounds.

The judgment states that "as the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question."

The judgment also states that "whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life", where no specific reasons exist and the role played by the individual in the public life justifies the overriding interest of the public, the internet engine may refuse to

erase such information. It is specified in the judgment of the court that each individual can address a request directly to the operator of the search engine (in the capacity as data controller), and such operator is obliged to duly consider such request and assess its justification; to proceed to erasure, the results shown shall be "inaccurate, inappropriate, no longer up-to-date or excessive having regard to the purposes for which they were processed".

In 2015 the Commission also expanded its case-law with respect to complaints received from individuals concerning unlawful use of their personal data for the purposes of their registration as champions of political parties for the elections held in 2014.

The complainants alleged that they have been refused registration as champions of political parties because another registration already existed in favour of a different party. This is how they understood that their personal data has been used without their consent. In the course of examining the cases it was found that there is no explicit legal procedure for requesting, respectively proving the existence of consent of the data subject for the purpose of the corresponding registration. In their activities political parties observe mostly the Electoral Code, which does not provide for such an obligation or requirement for registration of champions. At the same time and in view of the burden of proof in the administrative process, data controllers must commit evidence of a condition for admissibility of the processed personal data, therefore the requirement for consent of the individual.

During the past year the Commission also considered new cases relating to unlawful processing of personal data in the course of or in connection with carriage of passengers by air.

Cases related to the liability of air carriers regarding the safe transportation of luggage in the context of information that can qualify as "personal data". The Commission accepts that in Chapter VI of the Civil Aviation Act the legislator has bound the contract of carriage with the carriage of both the passengers and their luggage as part of the obligations under the contract. In addition to information about the passenger and his/her luggage, contracts of carriage contain information about the destination of the journey, the travel time and other characteristics of the journey, which in turn constitute personal data within the meaning of Article 2(1) of the Personal Data Protection Act. The provision of Article 2 of the PDP Act defines as personal data any information relating to an individual who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific features. The carrier is responsible for the individualisation of luggage associated with the relevant passenger. The carrier is also responsible for the integrity of the transported luggage. The absence of individualization leads to the creation of prerequisites for violation of privacy and personal life, including a prerequisite for unlawful processing of personal data. In

order to avoid the occurrence of these preconditions, the legislator has envisaged an obligation of each PDC to undertake all technical and organisational measures required 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(1) of the PDP Act).

Next, the Commission holds that the provision of a copy of the identity document shall not be set as a condition to the passenger for receiving compensation for damaged luggage. Such actions can be regarded as violation of the principles of personal data processing.

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 2015, are as follows:

Telecommunications – 130 complaints

Employment and social security services – 15 complaints

Banks and credit institutions – 55 complaints

Video surveillance – 35 complaints

Education – 14 complaints

Condominium management – 10 complaints

Judicial and executive authorities – 29 complaints

Political entities – 17 complaints

Local authorities – 9 complaints

Media – 8 complaints

Carriage of passengers and tourism services – 7 complaints

Specific cases and case-law of the Commission

Judiciary: The Commission received a complaint containing an alleged violation of the complainant's rights under the PDP Act committed by the District Court, city of O., through failure to erase the information contained in the bulletin of previous convictions.

In the administrative file it was found that the penalties imposed on the complainant under both sentences whereby he was declared guilty of indictable crimes committed by him, and the penalty imposed ("Fine") is not an administrative penalty under Article 78a of the Penal Code but a penalty imposed by criminal conviction under Article 148(1)(3) of the Penal Code. Pursuant to Article 5 of Ordinance No 8 of 26 February 2008, conviction offices maintain and store files of bulletins of previous convictions and bulletins of administrative

sanctions imposed under Article 78a of the Penal Code, alphabetical indexes and entry register on paper and in electronic form.

The time period for storing bulletins is different from the time period for storing of information on convicted persons contained in the bulletins, entered in alphabetical indexes and the entry registers on paper and in electronic form. Data on convicted individuals and the information recorded in connection with them is stored indefinitely, unlike the bulletins. With regard to the latter, Ordinance No 8 of 26 February 2008 provides a period of storage equal to that stipulated in Article 24(1) (bulletin of previous convictions, under which a hundred years have passed from the date of birth of individuals, are separated in a special file and destroyed after being microfilmed), respectively Article 31(1) (bulletins of administrative sanctions under Article 78a of the Penal Code are stored for and destroyed after a period of fifteen years of the entry into force of the judicial instrument).

In the specific case the Commission considered that the relevant hypothesis for processing the personal data of the complainant by the District Court, city of O., is that of Article 4(1)(1) of the PDP Act, according to which processing is necessary for the execution of an obligation of the personal data controller, stipulated by law. In this connection, the complaint was held to be unjustified.

Video surveillance: The complainants approached the Commission with a complaint that "for some time the entrance and staircase are under the influence of two CCTV cameras". Following an inspection, it was stated in a statement of findings that "at the address specified by the complainants a video recording system has been installed comprising 3 cameras and a video recorder (DVR), located as follows: first – recording the ground floor inside the entrance, and second and third – recording the space in front of the entrance outside the building with about 20 metres outside perimeter around the building, which includes the space in front of the block, which is used as a parking lot for the cars of the residents".

It was found that the general meeting of the condominium owners was held with the required quorum with an announced agenda, item 1 of which was "the condominium owners present decided unanimously to place video surveillance cameras for security purposes in the following places: close to the entrance of the building and at the elevator landing on the ground floor".

The need to find a balance between the interests of the data controller and the interests of the complainants, in pursuance of the principle regulated in Article 30(1) of the Constitution of the Republic of Bulgaria for personal freedom and inviolability of every Bulgarian citizen, justifies the Commission assessment that the complaint is grounded, inasmuch as the video surveillance also covers public areas. In this connection the

Commission issued a compulsory instruction to the condominium manager to take actions aimed at discontinuing the video recording in public areas and to apply for a "Video surveillance" register at the CPDP.

Police registration: The subject of the complaint received at the Commission is the disagreement of the complainant "with the decision of the Minister of Interior refusing to erase the personal data" of Mrs. M, processed by the ministry.

The complaint states the motives for the refusal, as follows: "delivered enforced convictions, because of which there are no grounds to erase the personal data from the databases of the institution, with regard to which the absence of a circumstance referred to in Article 3 of Instruction No 8121z-748/2014 of the MoI is invoked". In view of the above, Mrs. M is of the opinion that from the serving of the convictions imposed "over 27 years have passed for the first conviction and 25 years have passed for the second conviction", and in the meantime she has had the appropriate behaviour, and as she is currently working in a site with special regime, the interest in erasing her personal data from the databases of the Ministry of Interior (MoI) arises.

Pursuant to Paragraphs (1) and (2) of Article 33 of Ordinance No 8 of 26 February 2008 on the functions and organisation of the operations of conviction offices (the Ordinance), conviction offices issue certificates of previous convictions and records of previous convictions. Certificates of previous convictions are issued to individuals, specified in the Ordinance, at their request. Records of previous convictions are issued for official purposes of: courts, prosecution and investigation authorities; agencies and departments, which are entitled by law to receive such information; judicial authorities of another country, where so provided for in an international treaty to which the Republic of Bulgaria is a party or by an instrument of the European Union; Central Authority for transmission or reception of information on criminal records from a EU Member State; foreign diplomatic and consular missions in the Republic of Bulgaria with regard to their nationals.

Pursuant to Paragraphs (1), (2) and (3) of Article 36 of the Ordinance, records of previous convictions are issued on the grounds of a request from the corresponding body. The record states all convictions, regardless of any subsequent amnesty or rehabilitation, and contains the first, middle and last name of the official who prepared the record. Copies of the bulletins of previous convictions are sent to the body which made the request at the discretion of the Chairperson of the District Court or a deputy designated thereby depending on the purpose for which the record was requested. The record is sent ex-officio to the body that made the request.

It is exactly in view of the different purpose for which they are issued that the difference in the content of the Certificate of previous convictions and the record of previous convictions is specified.

In this sense, Article 39(2) of the Ordinance states explicitly that certificates of previous convictions do not contain criminal convictions for which an amnesty was given or for which the individual has been rehabilitated; and records of previous convictions on the Grounds of Article 40(1) contain all convictions and administrative sanctions imposed under Article 78a of the Penal Code.

In view of the provisions above, the conclusion was made that the information relating to initiated criminal proceedings, which were concluded with convictions, as in the case of Mrs. M, is not subject to erasing.

The clarification is made that this information is not reflected in the record of previous convictions but is stored on the relevant legal basis for purposes relating to: ensuring the fulfilment of the obligations of the Republic of Bulgaria under international bilateral and multilateral treaties and instruments of the European Union on receiving from and transmission to other countries of information on criminal records; some special laws as part of the extant Bulgarian legislation – Article 179(1)(2) of the Ministry of Interior Act, introducing requirements for entering the service in the MoI, one of which is that the person shall not have been convicted of a premeditated indictable crime regardless of rehabilitation or shall not have been released from criminal liability for premeditated indictable offence due to the imposition of an administrative penalty under Article 78a of the Penal Code; pursuant to Article 53(1)(4) of the State Agency for National Security Act, individuals who have not been convicted of a premeditated indictable crime regardless of rehabilitation or not have been released from criminal liability for premeditated indictable offence can be appointed as civil servants in the Agency; the provisions of the Judiciary Act regarding the appointment of judges, prosecutors and investigators contain similar legal requirements; pursuant to Article 420(1) in conjunction with Article 422(1)(3) of the CrPC, in the event of discovering circumstances that were not known to the court that issued the sentence, judgment, ruling or order and are essential to the case, the competent prosecutor has the possibility of reopening the criminal case exactly based on the indefinite storage of information in court bulletins.

In this regard, it was found that the processing of the personal data of the complainant by the Ministry of Interior, in the hypothesis of their storage, is permissible pursuant to Article 4(1)(1) of the PDP Act in conjunction with Article 29 of MoI Act given the need to fulfil a legal obligation of the data controller in relation with the time periods for storage of information defined by the Minister of Interior.

2. Case law relating to contested decisions the Commission for Personal Data Protection

In 2015, the Sofia City Administrative Court (SCAC) initiated 63 cases on appeals against administrative instruments issued by the CPDP. The Supreme Administrative Court (SAC), in the capacity of appellate court, dealt with 37 cases.

During the reporting year, sessions of panels of the SCAC were scheduled for 74 cases, of which 21 cases initiated in 2014 and 53 cases initiated in 2015. It shall be noted that 10 of the cases initiated before the SCAC in 2015 were scheduled for consideration in 2016.

Of all cases considered by the SCAC, 40 were concluded with judgments, and 26 are pending the judgement of the corresponding panels.

The information available shows that 28 judgments confirmed the appealed administrative instruments of the CPDP. In 7 of them the court decreased the penalty imposed by the Commission. In 12 judgments the instruments issued by the Commission were rescinded.

The figure (Figure 6) shows the number of confirmed and rescinded decisions of the Commission:

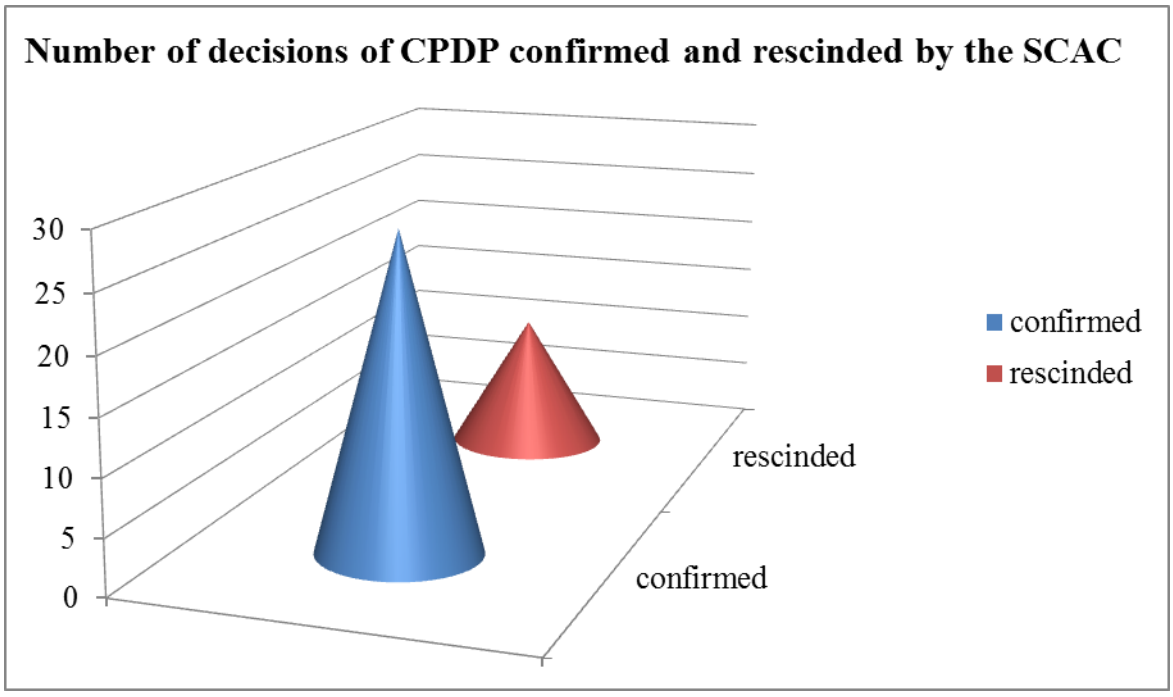

Figure 6

In 2015, the Supreme Administrative Court held sessions on 25 cases, of which 23 cases initiated in 2014 and only 2 cases initiated in 2015. All remaining cases initiated in 2015 were scheduled for consideration by the end of 2016.

The Supreme Administrative Court confirmed 8 judgments of the SCAC confirming the instruments issued by the CPDP and rescinded 2 judgments of the SCAC thus confirming the corresponding instrument issued by the CPDP. In 3 judgments the SAC rescinded the judgments of the SCAC and amended the CPDP decision, and 6 judgments confirmed the judicial instrument issued by the SCAC and rescinding the instruments of the CPDP. In one judgment the SAC rescinded both the judgment of the SCAC and the decision of the Commission.

In conclusion, it can be said that following a two-instance judicial control of 20 cases related to appeals against decisions of the Commission, 13 Commission decisions were enforced, and 7 were rescinded.

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

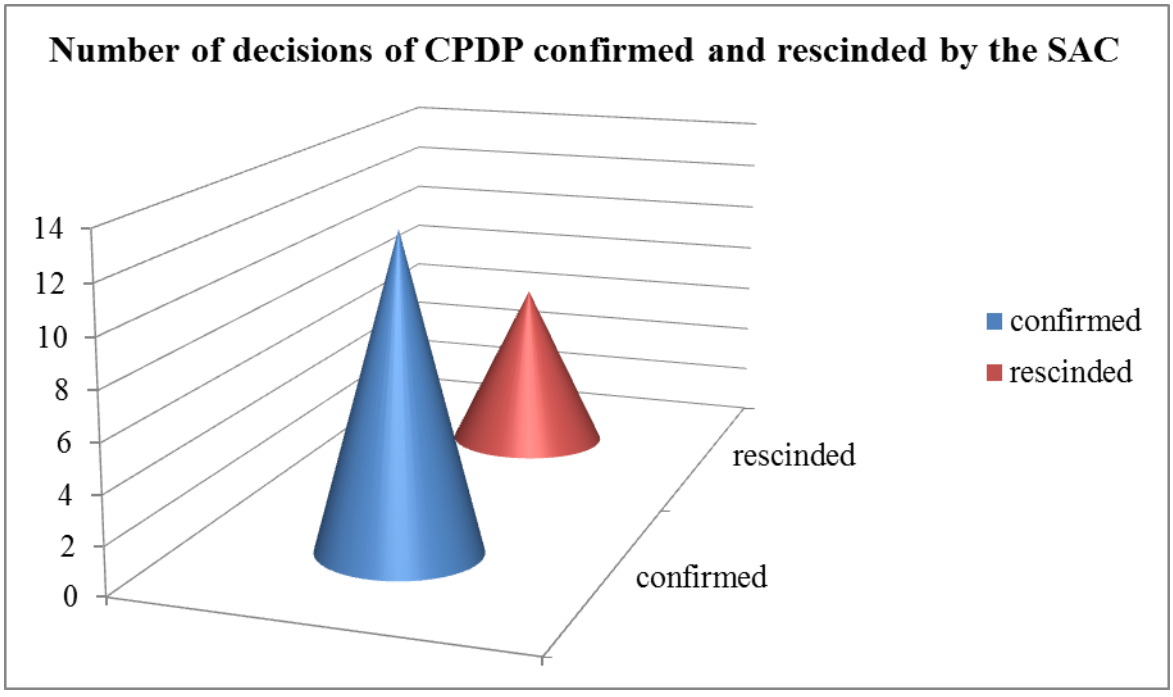

Figure 7

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

The total amount of the penalties imposed by CPDP administrative instruments in 2015 was BGN 737,600. This is almost twice the amount for the previous reporting period, when the amount of the penalties imposed by administrative instruments was BGN 476,400.

The amounts collected pursuant to CPDP decisions in 2015 came to BGN 166,269.61, of which BGN 27,240.11 were collected coercively by the NRA.

4. Advice provided to citizens

When carrying out a comparative analysis of the received inquiries from citizens according to the subject of inquiries, we concluded that the questions received by the CPDP in 2015 were many and varied. Citizens are becoming more active in seeking assistance and explanations in relation to the application of the PDP Act. This is equally confirmed by the statistical analysis of the 187 answers given by the Commission.

As in 2014, during the reporting period a large group of questions related to the fact that courier companies require information about PIN in relation to the sending or receiving of cash on delivery (CoD) consignments. The 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 Accountancy Act (AA) defines the information that must be included in 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.

A large group of questions relates to the functioning of websites known as online gaming sites, which require registration of pre-purchased tickets.

The questions most frequently asked concern the lawfulness of the mandatory fields in the sites, whereby upon registration 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 personal data controllers. 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.

In 2015 the number of questions relating to the transfer of personal data by various service providers (electricity suppliers, water and sewerage utilities, telecoms) to debt collection companies was great. Pursuant to Article 24(1) of the Personal Data Protection Act, personal data controllers (such as the service providers in this case) can process the data

themselves or have the data processed by an external data processing organisation (e.g. debt collection companies). If so required for organisational reasons, data processing services can be outsourced to two or more data processing organisations, including for the purpose of separating their specific obligations. In such cases the relations between the PDC and the data processing organisation are regulated by a statutory instrument, by a written contract or by another instrument of the PDC, which defines the scope of the obligations remitted by the PDC to the data processing organisation. Another reason for the transfer of data from one controller to another can be the consent of the person which the personal data relates to. According to the PDP Act, such consent must be provided in the form of a freely expressed, concrete and informed statement, whereby the subject of the personal data agrees to the processing of such data. Practice has shown that on most occasions individuals give their consent for the transfer of personal data from one controller to another at the time of concluding the service contracts.

The CPDP continues receiving inquiries about the provision of personal data (full names and PIN) when cash is deposited at or withdrawn from banks. The client identification procedure is mandatory for banking institutions in accordance with the Measures against Money Laundering Act (MAML Act). The CPDP's practice in this respect has been consistent and is expressed in the position that the explicit consent of the person whose data is being processed is only one of the preconditions set out in Article 4(1)(2) of the PDP Act, and the absence of this precondition does not prejudice the acts of the PDC (the bank). The existence of only one of the preconditions set out in items 1 through to 7 of Article 4(1) of the PDP Act is sufficient for the data processing operation to be lawful. In this case the data required by the banks is processed lawfully on the grounds of Article 4(1)(1) of the PDP Act, i.e. in fulfilment of obligations imposed on them by the law.

The citizens continue to question the right of shop cashiers to require customers to produce their ID card when they choose to pay by debit card. In reply to these questions, the CPDP informs the citizens that the so-called debit card is a payment card within the meaning of Article 25 of Ordinance No 3 of 16 July 2009 on the Terms and Procedure for the Execution of Payment Transactions and Use of Payment Instruments issued by the Bulgarian National Bank (BNB). The payment card can be used only personally by the authorised user of payment services. Pursuant to Article 32(1) of the said Ordinance, the merchant whose POS terminal is used to effect the payment may refuse a payment card to be used in case of a refusal by the holder to provide a document confirming his identity, or where the merchant finds that an unauthorised person uses the payment card.

Another group of FAQs relate to security activities carried out by private companies and to the personal data processed by security staff when they guard various sites. Pursuant to Article 24(2)(6) of the Private Security Act, for each guarded site the security service provider must draw up and maintain a site security plan, including a regime for accessing and leaving the site, approved by the customer to the security services contract or by a person authorised thereby. Pursuant to letters (a) and (b) of Article 30(1) of the PS Act, security staff is obliged to ensure compliance with the regime for accessing and leaving the guarded site and with the internal rules, as established by the customer, including by issuance of compulsory instructions and ensuring compliance with these instructions during:

1) checks of identity documents of visitors and of the passes of the personnel working at the site;

2) checks of luggage, cargoes and/or motor vehicles as well as the accompanying documents.

Accordingly, security staff has the right to write down the visitors' personal data shown on their identity documents, but cannot retain or make copies of the identity documents. This is in line with Article 11 of the Bulgarian Identity Documents Act, which clearly prohibits the giving or taking of an identity document as a pledge, the usage of another person's Bulgarian identity document or the surrender of a Bulgarian identity document in the possession of another person.

The CPDP received many inquiries from citizens containing questions about the possibility and procedure for making a complaint to the Commission. The answers provided detailed information on the methods for filing complaints with the CPDP and the required requisites of complaints, as well as on the ability of individuals to seek their rights regarding the protection of their personal data both under the administrative procedure before the CPDP and under the judiciary procedure before the Sofia City Administrative Court.

Another issue often referred to the attention of the CPDP both in connection with international cooperation and by citizens concerned the photocopying of ID cards by banks. As already stated above, the CPDP informs individuals that the photocopying of ID cards is a statutory obligation for banks in accordance with Article 6(1)(2) and Article 6(3) of the Measures against Money Laundering Act (MAML Act) and through it one of the measures to prevent the use of the financial system for the purpose of money laundering (client identification and verifying their identity) is implemented.

The CPDP uses its Centre for Information and Contacts (Call Centre) as an important communication channel for direct communication with citizens and to improve the quality of

services. It enables the Commission to satisfy inquiries by providing as full information as possible from the very first call.

The questions relating to the registration of personal data controllers were the most numerous. Frequently data controllers find it difficult to determine the scope of personal data registers processed by them, respectively the number and the statutory grounds for keeping such registers. Applicants are frequently not familiar with the statutory regulations and therefore need to get instructions from the call centre operators.

The main problem encountered in the practice of using eRALD is that data controllers do not fill out application – Part 2 "Description of Register", and in most cases the applicant prints out or signs with a universal electronic signature (UES) the so called confirmation sheet – a document which puts an end to the actions for performing electronic registration. Registrations made in this way are incorrect. In such cases the error needs to be rectified to continue the registration process.

A large number of issues giving rise to problems with the description of registers is that frequently requisites pertaining to different types of registers are combined. The difficulty is related to insufficient knowledge of data controllers and their desire matters relating to their registration to be resolved over the phone. In such cases corrections are made in real time in a dialogue mode following instructions from operators in the Centre for Information and Contacts. There is frequently lack of clarity in the applications for processing of personal data relating to health (data within the meaning of Article 5 of the PDP Act), with regard to which special legal requirements exist.

In addition, the Centre for Information and Contacts also receives calls relating to difficulties in the drafting of the Data Controller Instructions under Article 23(5) of the PDP Act. Applicants frequently look for an example of instructions – i.e. in the form of a standard form. Data controllers also encounter difficulties with regard to the criteria applicable to the defining of different levels of protection of personal data.

Another group of questions relates to whether companies selling online products over the Internet must register as PDCs and what would be the problem if no registration is made. Inquiries are received as to whether companies – representatives of companies registered abroad in EU Member States are required to register as PDCs in Bulgaria as well. Very frequently questions are asked regarding the registration of parent companies located overseas, with registered offices in Bulgaria.

A frequently asked question is whether the applicant can begin working as a PDC immediately after making a registration with the CPDP. Operators from the Centre for Information and Contacts inform citizens that each data controller can start processing data

after submitting the application for registration (Article 17 of the PDP Act). Although the capacity as a data controller arises ex lege, what the data controller should fulfil in accordance with the legal requirements is to submit an application with the CPDP, indicating the specifically kept registers, the type of personal data, the legal grounds, objectives and manner of processing such data, the technical and organisational measures taken for its protection, and also to comply with the procedure for processing and provision of data. It should be borne in mind that what determines whether it is necessary to apply for registration is not the formal capacity of the individual or entity (sole trader, foundation, a limited liability company, etc.) but whether it actually maintains a personal data register.

During the reporting period the call centre received on many occasions questions relating to the instructions of the Commission for Personal Data Protection to "Urban Mobility Centre" EAD regarding the notarised powers of attorney for persons accompanying persons with disabilities required by the company. In this connection, on 25 February 2015 the CPDP issued a compulsory instruction to "Urban Mobility Centre" EAD. The compulsory instruction is to discontinue the requirement to present identity documents of eligible persons with disabilities to recharge electronic transport documents, where this it is done by a duly authorised person. In addition, after issuing the compulsory instruction above, the CPDP published in its official website an announcement pointing out that the procedure to recharge the electronic transport documents is regulated by an order of the Executive Director of "Urban Mobility Centre" EAD. The requirements for the form of authorisation are not a subject of the compulsory instruction issued by the CPDP. With regard to new alerts received from citizens, in 2015 the CPDP carried out a follow-up inspection of "Urban Mobility Centre" EAD. Information about this inspection is presented in section "Control and Administrative-penal Activity" of this report.

In 2015, 4,269 inquiries were received in the Centre for Information and Contacts, allocated by months as follows:

I	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**	**X**	**XI**	**XII**
420	290	328	319	344	353	422	299	396	366	399	333

Summarised information regarding the frequency and number of inquiries during the reporting period

- In connection with the requirement for registration of PDCs – 1,308 inquiries with a frequency of approximately 109 inquiries a month;

- In connection with the registration as PDCs of companies selling online products over the Internet – 317 inquiries with a frequency of approximately 26 inquiries a month;

- The inquiries regarding the signing of the so called confirmation sheet with a UES were 343 with a frequency of approximately 28 inquiries a month;

- The questions relating to the Commission's instructions to "Urban Mobility Centre" EAD were 42 with a frequency of approximately 4 inquiries a month;

- Whether companies – representatives of companies registered abroad in EU Member States are required to register as PDCs in Bulgaria as well – 28 inquiries with a frequency of approximately 2 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 CPDP and its administration (RACPDPA), Ordinance No 1 of 30 January 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 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 who are assisted by the specialised administration – Control and Administrative-Penal Proceedings Department of the Legal Proceedings and Supervision Directorate. This activity includes inspections of PDCs to establish facts and circumstances and collect 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 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.

Inspections end by the issuance of a statement of findings or a compulsory instruction, and in the event that an administrative violation of the provisions of the PDP Act is established, administrative penal proceedings are initiated in accordance with the procedure established by the PDP Act.

In 2015, **654** inspections were initiated, of which:

- 456 ex-ante inspections;
- 19 ongoing inspections;
- 53 ex-post inspections;
- 126 inspections on requests and alerts.

The total number of inspections carried out (Figure 8), including finalised inspections initiated in 2014, and was **687**. Of these:

- 511 ex-ante inspections;
- 12 ongoing inspections;
- 48 ex-post inspections;
- 116 inspections on requests and alerts.

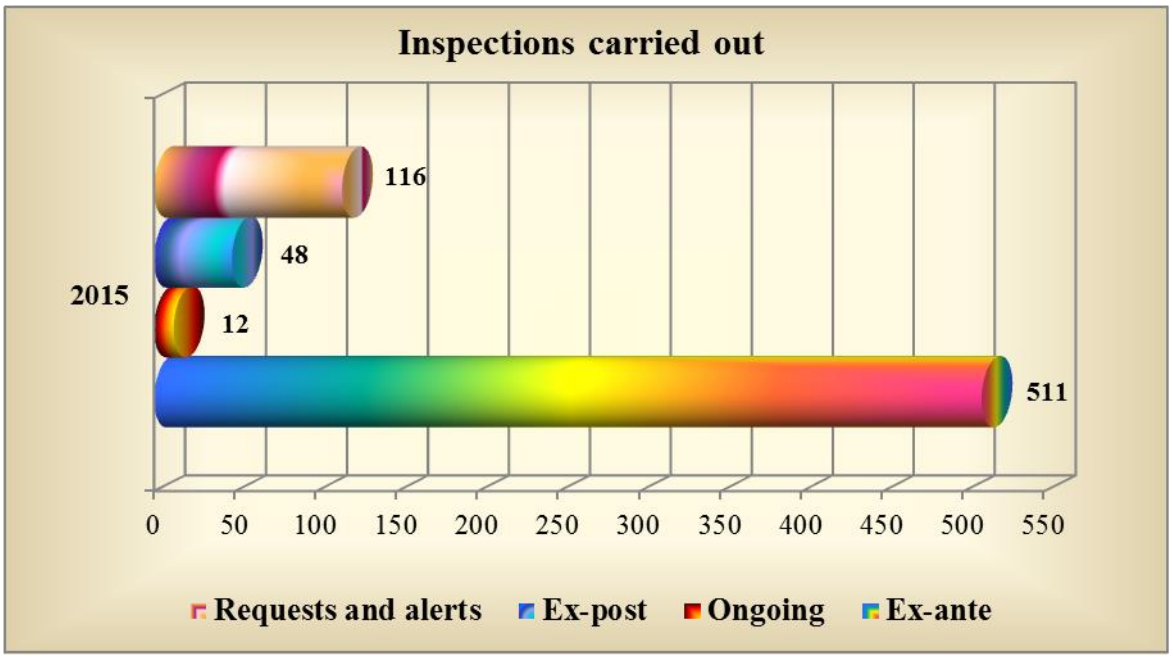

Figure 8

It is seen from the above data that the largest number of inspections were ex-ante inspections on the grounds of Article 12(2) of the PDP Act. The inspections carried out resulted in the issuance of 459 statements of findings and 12 compulsory instructions, and 20 inspections were completed with the issuance of statements establishing administrative violations.

Comparative statistics of completed inspections (ex-ante, ongoing, ex-post and consideration of requests and alerts) is presented in the following figures (Figure 9 and Figure 10):

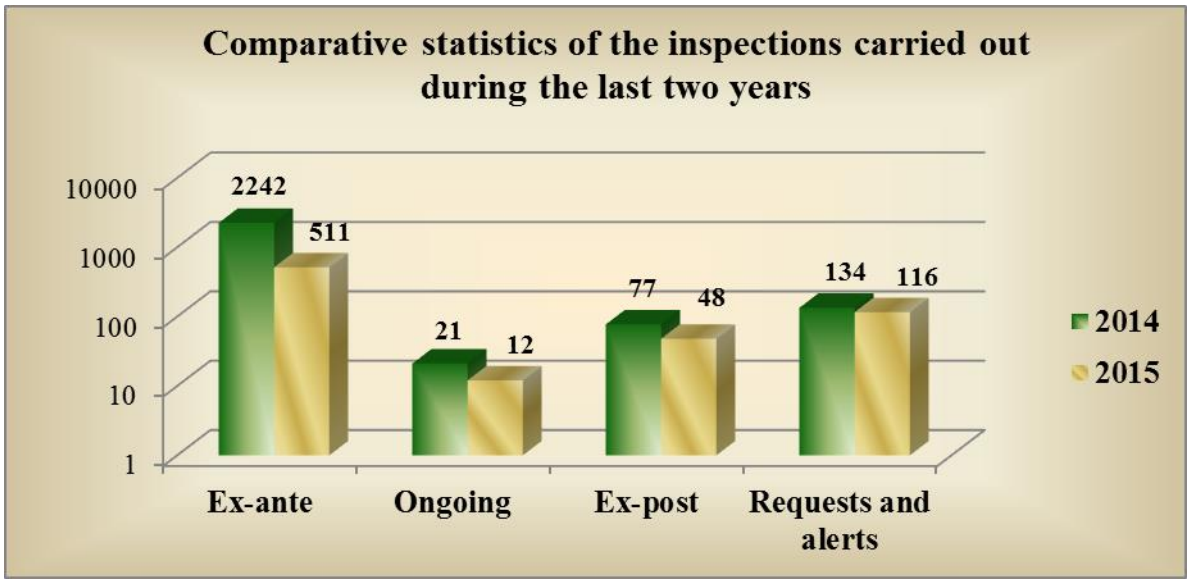

Figure 9

The analysis of the comparative statistics of the inspections carried out during the past two years leads to the conclusion that the lower number of inspections in 2015 compared to 2014 results from the lower number of submitted applications for registration as personal data controllers and the ex-ante inspections initiated in connection with such applications.

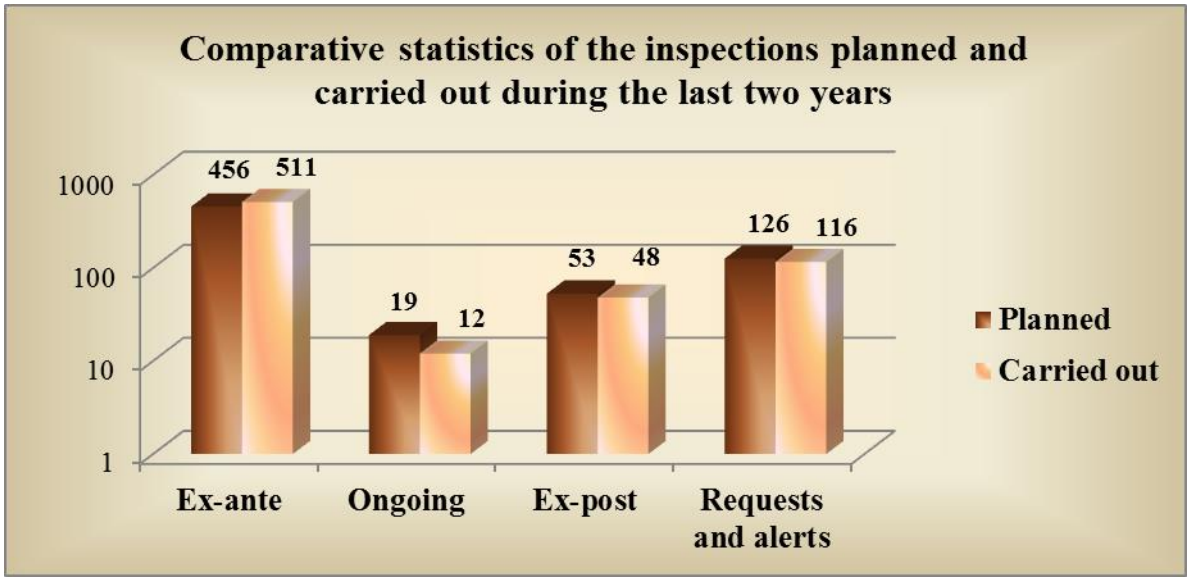

Figure 10

The specific environments in which personal data is processed mean that there is a need to differentiate the inspections by sectors. In pursuance of its activities in 2015, the CPDP carried out inspections in the following sectors:

No	SECTOR	NUMBER
1	Banking	1
2	Video surveillance	20
3	Other	12
4	Public administration	23
5	Energy	1
6	Insurance	9
7	Healthcare	275
8	Healthcare and internet	1
9	Election law	1
10	Internet	39
11	Internet, education	2
12	Internet, telecommunications	1
13	Information technology and services	6
14	Utilities	1
15	Consulting activities	6
16	Credit institution	1
17	Media	4
18	Local government	1
19	Research	2
20	Regional and local authorities	13
21	Processing and treatment of radioactive waste	1
22	Education and training	37
23	Public administration and internet	1
24	Defence	1

25	Security	5
26	Politics, political parties	13
27	Justice / law enforcement	8
28	Manufacturing	6
29	Industry and trade	5
30	Advertising and market surveys	2
31	Social activities	4
32	Sports activities	3
33	Construction	1
34	Collection of receivables	1
35	Telecommunications	3
36	Transport	8
37	Employment legislation	1
38	Tourism	2
39	Commerce and services	80
40	Real estate transactions	1
41	Financial sector	5
42	Financial and accounting services	10
43	Gambling and internet	3
44	Hotels and restaurants	2
45	Human resources	7
46	Non-profit legal entities	45
47	Legal services	14

1.1. Ex-ante inspections

Pursuant to Article 17b of the PDP Act, these inspections are required prior to the PDC registration in the register under Article 10(1)(2) of the PDP Act in the cases where the data controller has declared processing of data subject to special protection as per Article 5(1) of the PDP Act (related to health, sexual live or human genome, data revealing the person's

race or ethnicity, or the person's political, religious, philosophic beliefs or membership in related organisations) or data the processing of which, according to a CPDP decision, endangers the individuals' rights and lawful interests.

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

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

In 2015, a total of 511 ex-ante inspections were carried out, including 21 inspections of PDCs with regard to which a refusal of registration was ruled in CPDP decisions in previous years (Figure 10).

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

1.2. Ongoing inspections

Although the number of ongoing inspections under Article 12(3) of the PDP Act is much lower, these inspections present larger legal complexity. 12 ongoing inspections were carried out in 2015 (Figure 10).

According to the PDP Act, these inspections are carried out at the request of interested persons or at the initiative of the CPDP on the basis of monthly control plans adopted by the Commission.

During the reporting period, 12 ongoing inspections were carried out. Three of these were related to complaints filed by individuals for video surveillance of public areas and recording images in common areas of condominiums.

The ongoing inspections resulted in the issuance of 4 compulsory instructions.

The following inspections were more complex in factual and legal terms and provoked substantial public interest:

In order to obtain up-to-date information about the practical implementation of and compliance with the general and specific rules for personal data protection in the activities of the Europol National Unit (ENU) at the "International Operational Cooperation" Directorate

of the Ministry of Interior, the application of harmonized criteria for entering information into the Europol Information System, developed by the Europol Joint Supervisory Body, and the implementation of the recommendations from previous inspections of the CPDP, an inspection of the ENU was carried out during the reporting period. The inspection found that the ENU complies with the provisions of the PDP Act, including the requirements for work with the Europol Information System, and applies the harmonized criteria for entering information into the system.

In connection with joining the Visa Information System (VIS) of the European Union and the obligation of the CPDP to report before the VIS Coordination Group at the Council of Europe on the readiness of the Republic of Bulgaria, and in pursuit of one of the measures for self-assessment under SIS-II under the auspices of the Ministry of Interior, with a decision of the CPDP three inspections were initiated of consular missions of the Ministry of Foreign Affairs. Inspections were carried out of the Consulate General (CG) of the Republic of Bulgaria in Saint Petersburg, Russian Federation; the Consular Mission of the Republic of Bulgaria in Astana, Republic of Kazakhstan; and the CG of the Republic of Bulgaria in Istanbul, Turkey. The main tasks of the inspections were as follows:

- to check the visa policy and the functioning of the Visa Information System in the operations of the CG;

- to identify the technical and organisational measures taken to protect personal data within the meaning of Paragraphs (1) through to (4) of Article 23 of the PDP Act and whether they correspond to the levels of impact and protection as set out in the Ordinance;

- to check if personal data from the categories specified in Article 5(1) of the PDP Act are processed;

- to check if individuals whose personal data are processed are provided with the information required pursuant to Article 19(1) of the PDP Act;

- to check the actions taken by the CG after the purposes for which personal data are processed are achieved, in accordance with the requirements of Article 25 of the PDP Act.

The inspections carried out at the CG of the Republic of Bulgaria in Saint Petersburg, Russian Federation, the Consular Mission of the Republic of Bulgaria in Astana, Republic of Kazakhstan, and the CG of the Republic of Bulgaria in Istanbul, Turkey, resulted in the issuance of compulsory instructions.

During the reporting period an investigation of "International Social Service – Bulgaria" Foundation was carried out in connection with the foundation's activities in cases with an international component. Before and in the course of the inspection the CPDP initiated working meetings with the State Agency for Child Protection (SACP), the Social

Assistance Agency (SAA), the State Agency for National Security (SANS) and other government authorities relevant to the case. The inspection resulted in the issuance of a compulsory instruction to the "International Social Service – Bulgaria" Foundation with a Decision of the CPDP.

In order to establish whether the provisions of Chapter Three of the PDP Act are complied with, an inspection was carried out of the activities of a law firm relating to personal data processing through a job advertisement posted in the internet at http://www.jobs.bg. During the inspection no evidence of violations of the PDP Act were collected.

At a regular meeting the CPDP made the decision to carry out the inspections of State Enterprise "Bulgarian Sports Lottery" and First Investment Bank AD, planned for 2014 but delayed due to the involvement of most of the CPDP's administration in the pursuance of its decision to conduct inspections of political entities filing with the CEC registration documents for participation in the elections of European Parliament Members, held in the Republic of Bulgaria on 25 May 2014.

The inspection of First Investment Bank AD ended without findings of violations of the PDP Act. The inspection of State Enterprise "Bulgarian Sports Lottery" has not been completed yet.

1.3. Ex-post inspections

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

48 ex-post inspections were carried out in 2015 (Figure 10). The methodology employed in these inspections is similar to the one used for the ongoing inspections, as described above, the only difference being the legal basis on which they are carried out.

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

- the processing of personal data of staff and clients;
- the processing of personal data relating to DNA tests abroad;
- the requirement to send a scanned ID document to participate in gambling games;
- the processing of personal data in performing control of access to public buildings;
- the processing of personal data without existing registration with the CPDP;
- video surveillance in public areas;
- photocopying of ID documents of clients;

- unlawful removal of documents containing personal data from the building of the data controller;

- distribution of personal data;

- generally available on the internet information containing personal data of patients;

- "Urban Mobility Centre" EAD requiring the presenting of original identity documents of eligible persons with disabilities to recharge electronic transport documents, where this it is done through a duly authorised person;

- "Urban Mobility Centre" EAD requiring notarised powers of attorney issued by persons with disabilities whose transport documents are recharged;

- the possibility to send and process documents of ownership for creation of a cadastral map and cadastral register in the country by the Geodesy, Cartography and Cadastre Agency by public e-mail.

These inspections resulted in the issuance of 6 compulsory instructions and 16 statements establishing administrative violations.

The following ex-post inspections were more complex in factual terms and provoked substantial public interest:

In connection with a complaint received in 2014, with a Decision dated 23 March 2015 the CPDP issued a compulsory instruction to the SAC in its capacity as personal data controller, namely: to bring the documents published in the official website of the court and containing personal data in line with the requirements of the PDP Act and to anonymise the personal data contained therein. The CPDP received a complaint about the practice introduced in the SAC, where personal data are disclosed when making inquiries on cases, and the ability to view scanned documents containing unanonimised personal data when the number of a particular case is stated. In order to ascertain facts and circumstances relating to the implementation of the compulsory instruction and the complaint received, an inspection of the SAC was carried out. In the course of the inspection it was found that the implementation of the compulsory instruction is part of a project under OPAC, implemented by the SAC and entitled "Creating a Reliable Environment for Data Exchange and Communication between the Administrative Courts in the Republic of Bulgaria and Creating a Unified Information System Filing / EDIS / Deployment in the Administrative Courts in the Republic of Bulgaria", and the actual deployment will take place in January 2016.

An inspection was carried out in connection with an alert received by the CPDP regarding the use of the Second generation Schengen Information System (SIS II) at the SIRENE National Bureau at the "International Operational Cooperation" Directorate of the Ministry of Interior. The main tasks of the inspection were to establish facts and

circumstances relating to the alert and to establish actual interaction between the CPDP and the SIRENE Bureau in the examination of complaints and alerts filed by individuals. It was found that the provisions of the PDP Act and the statutory instruments regulating the operation of NSIS of the Republic of Bulgaria are complied with in the course of activities.

In connection with a large number of complaints, alerts and inquiries by interested persons and disabled persons in connection with the activities of "Urban Mobility Centre" EAD for recharging electronic travel documents through a duly authorised person, an ex-post inspection of the company was carried out. The inspection resulted in the issuance of a compulsory instruction along the following lines:

1. Documents confirming the identity of accompanying persons, copies of powers of attorney of authorised individuals and certificates for determining the guardian/custodian of the entitled individual shall be collected only once at the time of their initial provision for the purposed of issuing/charging an electronic card, and once in the event of change of the identity document of the accompanying or authorised person.

2. The data from the documents referred to in item 1 shall be entered in the single/centralised information system of "Urban Mobility Centre" EAD by stating the capacity of the representative (accompanying person, authorised person, parent, guardian, custodian).

3. The time period of storing the collected copies of documents referred to in item 1, including the data entered in the single/centralised information system of "Urban Mobility Centre" EAD, shall be in line with their period of validity, and after the expiry of this period they shall be destroyed in accordance with a procedure defined by "Urban Mobility Centre" EAD.

4. Internal rules/procedures shall be developed to regulate the activities relating to the recharging of electronic travel documents; the technical and organisational measures for personal data protection pursuant to Ordinance No 1 of 30 January 2013; the transmission of personal data to third parties; the 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.

In connection with an inquiry expressing doubts of the legality of personal data processing through the created possibility for sending scanned copies of title deeds of owners of properties in Sofia, required for the creating of a cadastral map, to an unprotected e-mail in abv.bg, with a decision of the CPDP an inspection was initiated for the compliance with and implementation of the PDP Act by the Geodesy, Cartography and Cadastre Agency. The inspection resulted in the issuance of a compulsory instruction.

An inspection of the National Health Insurance Fund on a complaint about unauthorised access to the medical record of the complainant was completed without findings of violations of the PDP Act on the occasion of the complaint.

In connection with an alert received by the CPDP, an inspection at UniCredit Bulbank AD was carried out to establish whether the provisions of the PDP Act were complied with and the volume of personal data of clients processed through scanning their identity documents. The inspection resulted in the issuance of a compulsory instruction to UniCredit Bulbank AD to inform its clients and contractors in a timely manner of the technological process for verification, using a specialised software application and a scanning device, of the authenticity and validity of identity documents, prior to the verification.

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 2015, the Commission considered 116 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.

In 2015 individuals and legal entities also filed alerts referring to the attention of the CPDP possible violations of the PDP Act in the form of unlawful actions relating to:

- processing of personal data of individuals without existing registration with the CPDP;
- publishing of personal data in websites;
- creating false profiles in websites;
- requiring personal data in online games;
- requiring personal data in the course of annual technical examinations of motor vehicles;
- requiring copies of identity documents;
- requiring larger volumes of personal data than those necessary in relation to completing registration forms for use of services in websites;
- possibility for unregulated access to personal data published in websites;
- possibility for unregulated access to personal data due to failure to take technical measures for protection of specific websites;

- sale of databases containing e-mail addresses;

- alerts against mobile operators;

- receiving unsolicited electronic communications;

- provision of personal data to unauthorised persons;

- processing of personal data for direct marketing purposes without having requested the consent of the individual;

- personal data processing by media;

- carrying out video surveillance in condominiums;

- processing of personal data for taking loans without the knowledge of individuals;

- alerts relating to the practice of "Urban Mobility Centre" EAD to require notarised powers of attorney issued by persons with disabilities whose transport documents are recharged.

The consideration of the requests resulted in the issuance of 2 compulsory instructions and 4 statements establishing administrative violations, and one request was referred by competence to the Geodesy, Cartography and Cadastre Agency. Appropriate replies were returned to the senders.

2. Administrative-penal Activity

2.1. Compulsory instruction

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, the CPDP issues compulsory instructions (CIs) to PDCs regarding the protection of the personal data processed.

The CIs aim to afford adequate protection of the personal data in the personal data registers kept by maintaining the minimum scope of appropriate technical and organisational devices and protection measures as per the PDP Act and Ordinance No 1 of 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection.

Seven of the 12 CIs issued in 2015 were complied with within the time-limits set by the CPDP, and the other 5 CIs are under implementation. Four CIs made in 2014 were also complied with.

CIs are issued in the event of findings concerning the processing of copies of identity documents of individuals when they enter into employment contracts or into civil service. Experience shows that employers require a copy of the identity document (ID card) when recruiting employees. When concluding employment contracts, each employer is obliged to comply with the requirements of Article 66(1) of the Labour Code and with Ordinance No 4

of 1993 on the documents required for the concluding of employment contracts. The Ordinance does not provide for the submission of an identity document copy at the time of applying for a job and at the time of subsequent conclusion of an employment contract, and as such there is no legal basis for requiring and retaining such copies. Furthermore, such a requirement is not included in the provisions of Article 2 of the Ordinance on the documents required for employment in civil service. For this reason the processing of personal data through keeping in employment and official records of individuals of copies of their identity documents is unlawful and is performed in violation of the provision of Article 2(2)(1) of the PDP Act, and all collected copies must be destroyed.

Instructions were also issued in connection with the processing of documents containing personal data, where the volume required is bigger than the volume necessary to identify the individual and the processing is not proportional to the objective of obtaining personal data.

In 2015, instructions were also issued in connection with 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.

Last but not least, CIs were also issued in connection with taking specific measures to ensure the required level of protection of personal data, including taking special measures when transferring personal data electronically.

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 Commission member or by officials authorised by the institution according to the requirements of Article 43(1) of the PDP Act, and PDs are issued by the Chairperson of the Commission in accordance with Article 43(2) of the PDP Act.

In exercising the controlling powers under Article 12(1) and Article 12(8) of the PDP Act by carrying out inspections for compliance with the personal data protection legislation, in 2015 the CPDP issued 20 SEAVs for violations of various provisions of the PDP Act, on the basis of which the CPDP Chairperson issued 19 PDs.

Similar to previous years, in 2015 the Commission continued to encounter major difficulties in delivering the issued SEAVs to addressees via municipal administrations in various parts of the country, in accordance with the provision of Article 43(4) of the PDP Act.

In some cases the SEAVs are delivered to persons not having representative powers, in other cases the recipients do not sign the receipts by which PDCs acknowledge that they have been informed of their right to raise objections to the instrument within three days, whereupon the documents must be returned for a new due delivery, and in other cases the written evidence accompanying the instrument are not delivered. Although not as a regular practice, the CPDP requests and receives assistance from the Ministry of Interior authorities for detailed search and delivery of SEAVs and PDs to addressees in various part of the country, and for delivery to the seat of the PDCs.

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

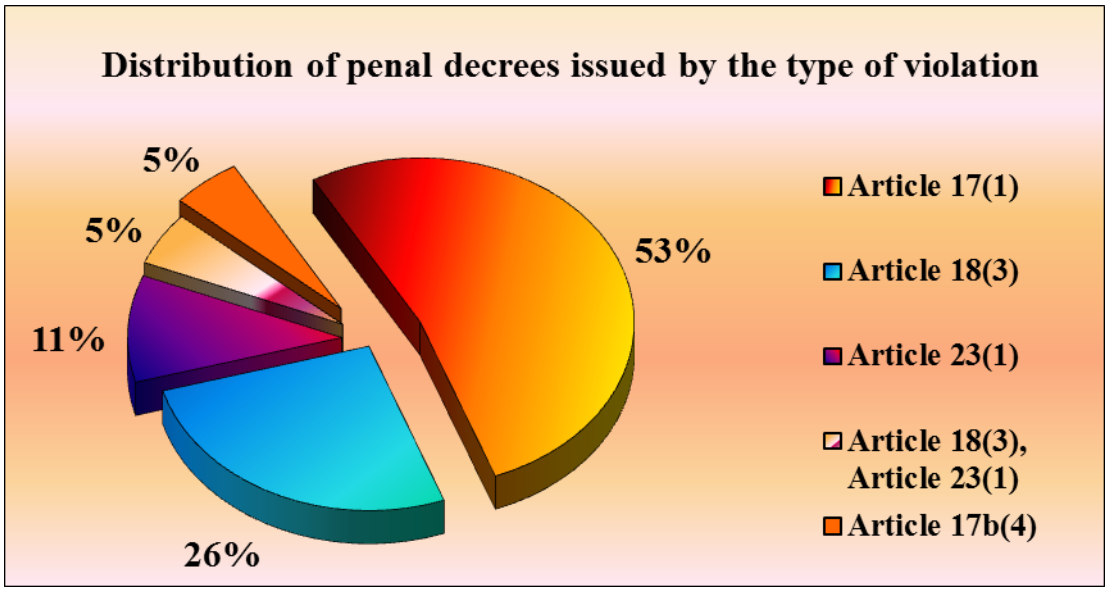

Figure 11

One of the most frequent violations of the PDP Act 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, 10 PDs were issued.

Five PDs were issued in connection with failure of PDCs to comply with their obligation to notify the CPDP in the event of changes in the data declared in the personal data register referred to in Article 10(1)(2) of the PDP Act pursuant to the provision of Article 18(3) of the PDP Act.

The next most numerous group of PDs are those for non-compliance with the provision of Article 23(1) of the PDP Act regarding the obligation 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. On these grounds, 2 PDs were issued.

One PD was issued for violation of the provisions of Article 18(3) and Article 23(1) of the PDP Act.

One PD was issued for violation in the course of processing personal data referred to in Article 5(1) of the PDP Act prior to the registration of PDCs in the public register of the CPDP pursuant to the provision of Article 17b(4).

19 PDs were issued in 2015, including 5 PDs on SEAVs issued at the end of 2014. The amount of penalties imposed by PDs is BGN 22,600. The amounts collected in 2015 totalled BGN 51,750, and BGN 27,750 of these were collected coercively by the National Revenue Agency (NRA).

Appeals against 4 PDs issued during the year are pending in courts. 7 PDs were paid without being contested and the offenders paid a total of BGN 6,500 in penalties, all of them near the minimum level envisaged in the PDP Act.

To collect the accounts receivable under PDs that have entered validly into force, invitations for voluntary payment are sent to the offenders on the grounds of and in accordance with the Tax and Social Insurance Procedure Code. If the offender does not pay within the time period specified, the case is transferred to the NRA. At present 21 PDs are being enforced by the NRA.

In 2015, the outcomes of the court cases initiated on appeals against PDs issued in previous years were as follows: 4 PDs were rescinded in their entirety, 6 PDs were confirmed in their entirety, and in 4 cases the size of the penalty was reduced. Currently, 30 appealed PDs are in the trial phase.

In the court cases initiated on appeals against PDs, the CPDP is represented by staff members that hold degrees in law and are officially admitted to practice the profession. In 2015 the Commission participated in 96 court sessions.

Some more significant and important examples of case-law, wherein the courts issued various types of rulings, are discussed in the following paragraphs. If valid legal grounds exist, the first-instance judgments, by which courts rescind the Commission's PDs in their entirety, are appealed before higher instance courts.

When rescinding a PD issued for violation of Article 17(1) of the PDP Act, in its judgment the Court invoked the expired limitation period under Article 34(1)(2) of the AVP Act and did not accept the date of the inspection and the finding of the CPDP team as the date of the offence ("Artikom" EOOD).

When revoking a PD issued for violation of Article 23(1) of the PDP Act, in its judgment the court invoked the right of journalism to perform a task in the public interest and the grounds for freedom of the press and other media proclaimed in Article 40 of the Constitution of the Republic of Bulgaria ("BTV Media Group" EAD).

In connection with the established violation of the provisions of Article 4(1), items 1–7 of the PDP Act, as grounds for rescinding the PD the court held that the personal data processing was necessary to perform a task in the public interest in accordance with Article 4(1)(5) of the PDP Act ("Olena-1" OOD).

When amending PDs, the court almost always reduced 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 PDs, the court gives them greater credited than to aggravating circumstances. On these grounds, the court amended PDs issued against Political Party National Democratic Party, Political Party Bulgarian Left, and ZAD "DZI – Life Insurance" EAD.

In 2015, the consideration of the administrative criminal proceedings (ACPs), initiated in connection with the inspections carried out in 2014 of all political entities that filed with the CEC registration documents for participation in the elections of European Parliament Members, held in the Republic of Bulgaria on 25 May 2014, continued. The main tasks of the inspections were the facts and circumstances relating to the alerts and complaints to each political entity and the manner of collection, further processing and destroying of personal data by parties and initiative committees in connection with the elections. The objective of the inspections was also to check for compliance with the PDP Act in the processing of data of other categories of individuals in connection with the operation of the parties as legal entities: participants in subscriptions, champions, representatives of political parties, parties to employment and service contracts, donors, contractors. The main objective of the CPDP was to prevent possible misuse of personal data of citizens participating in subscription lists and to verify whether the political entities comply with the PDP Act.

For violations established in the course of inspections of 54 political entities (44 political parties and 10 initiative committees), 15 compulsory instructions and 30 PDs were issued.

Currently, 13 PDs have entered validly into force: 10 PDs because they were not appealed and the penalties were paid, 1 PD that was rescinded in its entirety, 1 PD that was amended and the pecuniary penalty under which was reduced, and 1 PD that entered validly into force under the conditions of Article 58(2) of the AVP Act.

Seventeen appealed PDs are in the trial phase. In the first instance the court rescinded 6 PDs, of which 1 entered validly into force and the remaining 5 are appealed by the CPDP before the second instance, under 5 proceedings the judgments of the Regional Court are pending, and under 3 proceedings court sessions are scheduled.

The analysis of the court judgments, including those from prior years, demonstrates diverse case law on identical cases. These include cases involving violations of the obligation under Article 17(1) of the PDP Act, pursuant to which each PDC must apply for registration with the CPDP before starting personal data processing. The main problem here relates to determining the starting point of the obligation, i.e. the date of the offence, and the assessment regarding the application of the limitation period for invoking administrative penal liability.

In some judgments the court has confirmed appealed PDs by accepting the date of the CPDP inspection as the date of the offence and, therefore, accepting that the three-month period under Article 34(1)(2) of the AVP Act is complied with. There are court judgments rescinding PDs with the motive that the time period above has expired, since the PDP has started processing personal data of individuals outside it. For example, where one or over one year ago the PDC has concluded an employment contract containing personal data of an individual, the court holds that the PDC was obligated to file an application for registration as at the date of conclusion of such contract, i.e. the time period under Article 34(1)(2) of the AVP Act has expired.

All court judgments 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. As a result, it has been observed that the staff members authorised to issue SEAVs in the context of the Commission's control remit have increased their legal competences.

A priority of the administrative-penal activity is to maintain the percentage of PDs rescinded by courts at the existing relatively low levels.

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

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

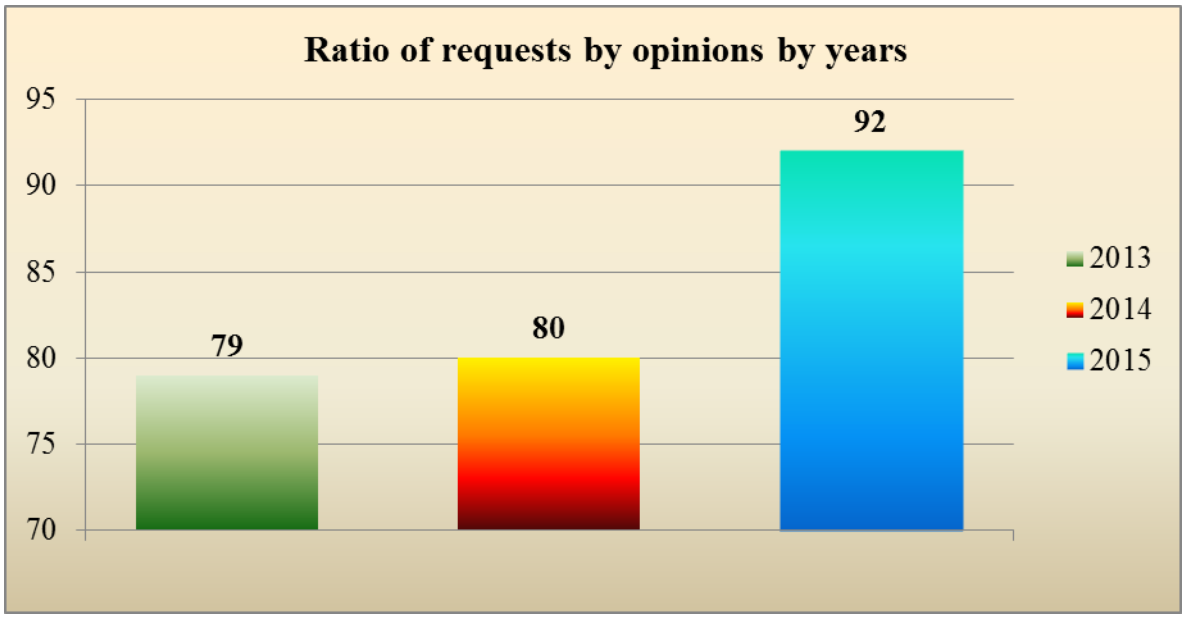

Figure 12

During the reporting year, a trend was observed of approaching the CPDP with requests for opinions regarding various topics from public life and by diverse data controllers. The analysis that can be made with regard to the subjects of such opinions and the controllers that requested them is that the subject of personal data protection becomes more relevant in all areas of modern society. An increasingly wide range of individuals having the capacity of data controllers ask the Commission to express competent opinions to outline the accurate direction in which controllers shall develop their activities in relation to the processing of personal data.

In 2015, the CPDP expressed several fundamentally important opinions in the context of personal data protection on issues relating to topical events of public life in Bulgaria.

At the beginning of 2015 the Commission considered the issues relating to the provision of the entire database of the Commercial Register and the updating of the

circumstances referred to in Article 2 of the Commercial Register Act (CR Act) and Ordinance No 1 of 14 February 2007 on the keeping, safeguarding of and access to the Commercial Register. The opinion analysed the concept "electronic database of the Commercial Register" and reached the conclusion that the broad interpretation and practical application of the understanding that it also contains the electronic images of documents, based on which entries and announcements were made, results in violation of the principles of processing and consequently the protection of personal data of individuals. The CPDP ruled categorically that the documents, based on which entries, announcements and deletions are made, are not part of the Public commercial register within the meaning of Article 2(1), Article 4, Article 5 and Article 11 of the CR Act, since in their nature these are not circumstances concerning the status of individual traders but evidence that the circumstances subject to entry in the register have occurred. In view of this, the personal data controller (the Registry Agency) shall take technological measures to redevelop the software applications allowing automated access to the database of the Commercial Register and access to information with unconcealed personal data, and access to electronic addresses of (links to) scanned images also containing signatures of individuals. Otherwise the provision of unconcealed information containing personal data is contrary to Article 2(2), Article 11(2) and Article 13(6) of the CR Act.

During the reporting period the CPDP also ruled on two requests sent by the receivers of "Corporate Commercial Bank" AD (in bankruptcy).

The first request concerned the legal actions that need to be taken in connection with the publishing in the website of CCB AD (in bankruptcy) of the lists of accepted claims under Article 64 of the Bank Insolvency Act. The Commission held that the list of accepted claims under Article 64(1) of the BI Act can contain data about the three names of the entitled individuals (creditors, depositors). Without this information the list of accepted claims under Article 64(1) of the BI Act cannot achieve the objectives for which the law envisages its preparation. Any inclusion of the full PIN or the last four numbers of the PINs of entitled individuals (creditors, depositors) in the list of accepted claims under Article 64(1) of the BI Act is contrary to the principles of personal data processing under Article 2(2)(3) of the PDP Act. At the time when the opinion was expressed, the legislator had not formulated statutory prerequisites for publishing in the Internet the list of accepted claims under Article 64(1) of the BI Act. In the event that the list is published in the website of CCB AD (in bankruptcy), this will constitute an unlawful and disproportional processing of personal data regarding the economic identity of the individuals included in the list. The opinion of the CPDP is that the information in the official site of CCB AD (in bankruptcy) shall contain only a message that

the list has been prepared and where it will be available, as well as within what time period each entitled individual can access its contents.

On an additional inquiry by the receivers of CCB AD (in bankruptcy) in connection with the publishing in the website of CCB AD (in bankruptcy) of the list referred to in Article 64 of the BI Act, the Commission expressed an additional opinion clarifying that in view of the fact that the extant legislation does not contain legal grounds for the publishing of the list referred to in Article 64 of the BI Act, such grounds could arise in the event of possible legislative amendments aimed at greater publicity of information relevant to bank insolvency proceedings. In such a situation, the hypothesis of Article 4(1)(1) of the PDP Act would apply: an obligation of the personal data controller, stipulated by law, to publish specific information, including personal data.

Given the CPDP's role as a supervisory body empowered to monitor the lawful processing of personal data of citizens, during the reporting period the Commission also expressed an opinion regarding the general elections for municipal councillors and mayors held in 2015. In its opinion the CPDP gave the following instructions to all participants in the election process:

1. Municipal and regional electoral commissions are personal data controllers but are exempt from the obligation to obtain registration with a Decision of the CPDP, included in Protocol No 32 of the CPDP dated 13 August 2014.

2. Section electoral commissions are personal data processors within the meaning of Article 24(1) of the PDP Act and their legal relationships with the personal data controller (municipal electoral commissions) are regulated in a statutory instrument – the Electoral Code.

3. All parties and initiative committees, which nominate independent candidates for national MPs, municipal councillors and mayors, and which register themselves in the relevant Regional or Municipal Electoral Commission, are personal data controllers and as such they are subject to registration as personal data controllers with the CPDP. The responsibility for the actions of initiative committees in their capacity as personal data controllers lies with the individuals designated to represent them within the meaning of the Electoral Code. At the time of registration of political parties and initiative committees with the CPDP they shall apply for the personal data registers they process, such as "Subscriptions", "Members", "Staff", "Champions", "Donors", "Contractors", "Video surveillance", "Access regime", etc., depending on the different categories of individuals and the purposes for which data is processed.

4. Coalitions of political parties are personal data controllers and, as such, are subject to mandatory registration with the CPDP. In connection with the processing of personal data of individuals, at the time of their registration with the CPDP coalitions of political parties shall apply for a "Subscriptions" register or a similar register, "Candidates" register or a similar register, "Champions" register or a similar register.

5. Local coalitions are personal data controllers but due to the limited number of individuals whose personal data are processed and the short period of their existence, the Commission exempts them from the obligation to register. The exemption from the obligation to register does not relieve local coalitions of any other obligations they have in their capacity as personal data controllers pursuant to the PDP Act, including from control by the CPDP.

6. Observers in their capacity as personal data controllers are subject to registration with the CPDP and shall apply for "Observers" register.

7. The CEC should demand from political entities evidence of the current status of their registrations as personal data controllers with the CPDP as of the date on which the election is fixed, but in any case not later than the date by which the subscription lists, supporting the registration of the corresponding political entity for participation in the elections, are submitted.

8. The CEC shall develop guidelines to regional and municipal electoral committees to require from initiative committees nominating independent candidates to provide information regarding the current status of their registrations as personal data controllers with the CPDP as of the date of registration for participation in elections.

In connection with the issues relating to electoral legislation and personal data processing, during the reporting period the CPDP also expressed an opinion on a request for granting access to the full list of individuals who were registered in the 2015 local elections and submitted applications to vote with a mobile voting box for all places from a municipality. The Commission's opinion was that the information contained in the lists of the full names of the individuals who submitted applications to vote with mobile voting boxed by individual settlements and the address registration of these individuals by permanent or current address can result in the ability to identify the specific individuals and, as such, falls within the definition of "personal data" within the meaning of Article 2(1) of the PDP Act. There are no statutory grounds for granting access to these lists, as the provisions of the Electoral Code do not envisage special rules regarding the preliminary announcing and publishing of the list referred to in Article 37(4) of the Electoral Code. The provision of Article 42(1) of the Electoral Code, stipulating the general provisions regarding the publishing and announcing electoral lists, unambiguously determines what information should be

publicly available, and such information does not include information about the permanent or current addresses of voters.

Another important opinion of the CPDP the consequences of which are observed in 2015 is the opinion expressed at the end of 2014 that using PINs as part of the mandatory content of the pupil ID card, pupil credit booklet and off-campus pupil credit booklet within the meaning of Articles 65–67 of Ordinance No 4 of 16 April 2003 on the documents in the national education system, issued by the Ministry of Education and Science, is unlawful and must be terminated. In connection with it, the CPDP issued a compulsory instruction within the meaning of Article 10(1)(5) of the PDP Act, which requires the Minister of Education and Science to take the necessary steps for the removal, starting from the next school year (2015/2016), of the PIN from the content of pupil ID cards, pupil credit booklets and off-campus pupil credit booklets. The compulsory instruction was delivered for implementation on 23 December 2014. In view of the time period for implementation as a result of the opinion expressed in 2014 and the compulsory instruction issued at the same time, as of the beginning of school year 2015/2016 the PIN is not a compulsory element of the templates of pupil ID cards, pupil credit booklets and off-campus pupil credit booklets.

In 2015 the CPDP considered a case at the request of the Chairperson of the State Agency for Child Protection, in connection with which an expert working group comprising representatives of the Ministry of Justice, Ministry of Foreign Affairs, Ministry of Labour and Social Policy, the Social Assistance Agency, the State Agency for Child Protection and the State Agency for National Security was set up at the end of 2014. SACP approached the Commission with a request to express an opinion on matters relating to the protection of personal data contained in the social reports on the situation of children and/or their parents, prepared by the Social Assistance Directorates at the Social Assistance Agency.

In view of the fact that social reports contain a lot of personal data, including sensitive ones, and data regarding third parties – parents and relatives of the individual subject of the report, the SACP expressed concerns that the provision of this information abroad by non-governmental organisations constitutes transfer of personal data within the meaning of the Personal Data Protection Act (PDP Act) and that the rules prescribed in the PDP Act shall be complied with for this actions to be lawfully performed. SACP states that the role of non-governmental organisations is to provide support to the child protection system, but not to directly displace the competent authorities in the exchange of the information in question under the so-called cases of children with an international element.

In order to express an opinion, the CPDP carried out a detailed analysis of the legal framework relating to child protection, including both national legislation and international

legal acts regulating this sensitive area of public relations. In view of the facts and the materials provided in the course of the administrative proceedings, is was established that there is no legal basis for the provision of social reports containing personal data by the Social Assistance Directorates or by any other state body responsible for child protection in Bulgaria to Foundation "International Social Service – Bulgaria" with regard to children, or to any other individual or legal entity, including on cases with an international element.

In the opinion of the CPDP, information from social reports on individual children can be provided only in specific cases for the purposes of the social services provided by Foundation "International Social Service – Bulgaria" in the Republic of Bulgaria only within the obtained licence for this activity, after registration in the relevant register of the SAA pursuant to Article 43b(1) of the CP Act, and then only in respect of children using these social services.

It was found that there is no legal basis for further processing or for processing of the personal data received for purposes other than these relating to the provision of social services. The Social Assistance Agency, like any other public authority, has no legal grounds to provide social reports regarding children, containing personal data, to non-governmental organisations for transfer of such data abroad.

The CPDP recommends to state bodies responsible for child protection and to any non-governmental organisation providing social services in the territory of the Republic of Bulgaria to take into account the conclusions made in the opinion in order to achieve lawful processing of personal data or children.

In connection with the particular case at issue, relating to the exchange of personal data in cases of children with an international element, the expert working group reached a decision to organise an inspection of Foundation "International Social Service – Bulgaria". The result from this inspection is presented in section "Control and Administrative-penal Activity" of this report.

Another large group of requests for opinions received from personal data controllers, namely the SACP and the Social Assistance Directorate, are related to the provision of information under the Personal Data Protection Act and the Individuals and Family Act. In their requests, parents of children request information relating to documents concerning personal data of their children. In 2015 in connection with the cases the CPDP expressed opinions that the competent authorities can provide the information requested in the application for access to personal data to individuals, in their capacity as parents of minor children, on the grounds of Article 26(1) of the Personal Data Protection Act in conjunction with Article 3 of the Individuals and Families Act. It shall be borne in mind that the opinions

expressed cannot be regarded as interpretative case law in the implementation of the PDP Act in view of the need for the CPDP to consider each case on its specifics and rule in an open session.

It is noteworthy that in 2015 the CPDP received several requests from the Consular Relations Directorate at the Ministry of Foreign Affairs to provide current addresses of Bulgarian citizens to foreign diplomatic missions. The reasons are different: most frequently in connection with the payment of child support; criminal cases initiated; on the grounds of a request for assistance from the health insurance fund; or in connection with treatment conducted in a foreign hospital. In all cases, the Commission was provided with the appropriate verbal notes of foreign diplomatic missions as the basis for the requests made. CPDP has a steady practice in dealing with such requests, which is expressed in the position that information about permanent and/or current addresses of Bulgarian citizens can be provided to foreign official missions in connection with verbal notes sent to the Ministry of Foreign Affairs on most occasions on the grounds of Article 4(1)(7) of the PDP Act and Article 106(2) of the CReg Act. The requested information regarding a permanent and/or current address shall be provided through the Ministry of Foreign Affairs after having informed the individuals in accordance with Article 20 of the PDP Act.

Another request, addressed to the CPDP by the Consular Relations Directorate at the Ministry of Foreign Affairs, states that the MFA received a letter from the Migration Directorate at the MoI in response to a letter from the Embassy of the Republic of Kazakhstan in Sofia requesting assistance for finding contact details of individuals, including confirmation of the citizenship of such individuals. The request states that there is no bilateral agreement between the Republic of Bulgaria and the Republic of Kazakhstan, regulating the provision of personal data, and there is no written consent of the individuals to whom the information relates. The opinion is expressed that the receiving country can be provided with such information only if it provides adequate level of protection of personal data within its territory and following a permission from the CPDP. A request for opinion was sent to the CPDP on whether the data received from the Migration Directorate at the MoI can be sent to the embassy of Kazakhstan in accordance with Article 55(1) of the Foreigners in the Republic of Bulgaria Act (FRN Act).

The CPDP expressed the opinion that the special law in the specific case is the FRB Act and that the rules regarding the provision of information (personal data in the specific case) have priority and derogate the general rules stipulated in the PDP Act. In the case in question, however, none of the hypotheses of Article 55(1) of the FRN Act exists. The PDP Act, which is the general law with regard to the FRB Act in the specific case, provides an

opportunity for transfer of personal data in a third country if the individuals to whom such data refer have given their consent – Article 36a(7)(1) of the PDP Act. In this case a permission from the CPDP is required to provide the data. In view of the above, there are no legal grounds for the provision of the requested data to the Embassy of the Republic of Kazakhstan.

The CPDP considered an interesting case at the request of the Mayor of Mizia municipality. The occasion was the request received in the municipality from the Director of the Institute of Ethnology at the Faculty of Philosophy of the Charles University in Prague, who has been studying for years the topic of Czechs in Bulgaria. The objective of this lengthy process, including an on-the-spot study in the village of Voyvodovo, Mizia municipality, is to study the first half of the twentieth century, when the village had Czech population. In view of the need for specific information, a request was sent to the mayor of the municipality to provide for use the registers of civil status of the village of Voyvodovo for the period 1900–1950, and, in particular, the record in these registers relating to dates of birth, death and marriage, which would contribute to the analysing of marriage models, mechanisms for choosing spouses and describing the demographic parameters of the community.

In the course of the administrative proceedings, safeguards with regard to the rights of individual data subjects affected by the research were required. The CPDP shares the understanding that the existing registers allow researchers in different areas of science obtain considerable knowledge of the long-term impact of a number of social conditions in order to understand history and culture. These are some of the objectives of the future General Data Protection Regulation. The idea is not to raise barriers to research but to promote the development by individual Member States of appropriate conditions and safeguards with respect to the processing of personal data for scientific purposes. Research in the field of cultural heritage have their social significance, and in view of the technical and organisational measures taken to protect data such research can be undertaken in accordance with the principles of personal data protection set out in the extant legislation.

It should be noted that the Commission for Personal Data Protection has the authority, in specific circumstances, to allow access to the registers of civil status on the grounds of Article 106(1)(3) of the Civil Registration Act (CReg Act). It is exactly this statutory opportunity that the CPDP used to allow access to the registers of civil status of the village of Voyvodovo for the period 1900–1950. It is important, however, to point out that the allowed access to public registers of population does not preclude the Commission’s power to exercise control of the specific data processing.

As in the case described above, traditionally CPDP receives requests for access to the Population Register – National Database "Population". It is noteworthy, however, that during the reporting period the number of requests for access pursuant to Article 106(1)(3) of the CReg Act was significantly lower than in previous years. This was due to the fact that data controllers are familiar with the consistent practice of the Commission to approve the provision of specific data on specific individuals and for specific statutory purposes, but not direct access to the entire database.

In 2015 the CPDP expressed an opinion in connection with the access of the Geodesy, Cartography and Cadastre Agency to the NDB "Population" in connection with the creation of a cadastral map and cadastral registers and in connection with the provision of electronic administrative services. The CPDP found that there are legal grounds for Chief Directorate of Civil Registration and Administrative Services at the Ministry of Regional Development and Public Works (MoRDPW) to grant access to the Population Register – National Database "Population" to the Geodesy, Cartography and Cadastre Agency after the conclusion of an agreement within the meaning of Article 106(4) of the CReg Act in conjunction with Section II "granting of Access" of Ordinance No RD-02-20-9 of 21 May 2012 on the functioning of the unified system of civil registration issued by the MoRDPW.

On the grounds of Article 106(1)(2) of the CReg Act and Article 4(1)(1) of the PDP Act, the categories of personal data in the Population Register – National Database "Population", to which Chief Directorate of Civil Registration and Administrative Services shall grant access to the Geodesy, Cartography and Cadastre Agency, are as follows: full names, personal identification number and permanent address of individuals. These data can be used only for the purposes of the cadastre – for the creation of a cadastral map and cadastral registers, and for updating the created cadastral maps and registers. No access shall be granted to data regarding the current address of individuals as well as to official data where they contain personal data.

Due to the special procedure for providing data from the Population Register – National Database "Population" stipulated in the CReg Act and due to the absence of legal grounds under the PDP Act, data concerning the full names, personal identification numbers and permanent addressed of individuals cannot be used for other activities of the Geodesy, Cartography and Cadastre Agency.

With regard to the provision of administrative services, the Geodesy, Cartography and Cadastre Agency shall be granted access to the Population Register – National Database "Population" only for the purposes of identifying the individuals requesting and/or receiving electronic services within the meaning of Article 28(1) of the Electronic Governance Act (EG

Act) and Article 55(1) of the Ordinance on electronic administrative services. The access shall be restricted to designated categories of data – full name and PIN.

In its capacity as personal data controller, the Geodesy, Cartography and Cadastre Agency is obliged to provide to the individual whose data are processed information about its obligation within the meaning of Article 28(1) of the EG Act, namely to verify the identity of the requesting individual through access to the Population Register – National Database "Population" where requests are submitted electronically.

In connection with the practice to rule on requests of MPs for access within their powers to information containing personal data, the CPDP has a constant practice and regardless of the specifics of the request always expresses its principle position. In order to ensure fair processing of data and to achieve the objective of the PDP Act – to guarantee the inviolability of personality and privacy – the CPDP expresses the position that the data controller should provide the requested documents after the personal data in them are brought in a form that does not allow identification of data subjects, for example by deletion or anonymization by initials.

A case relating to MPs, on which the CPDP ruled in 2015, was at a request for opinion from the Chairperson of the Council for Electronic Media. It was stated in the request for opinion that in connection with a weekly monitoring of a television station it was found that during a certain period a video clip was repeatedly broadcast, disseminating photographs, telephone numbers and the political affiliation of ten MPs from the Temporary Committee on the demand from the Prosecutor General of the Republic of Bulgaria for authorisation to institute criminal proceedings against two MPs. The CPDP expressed the opinion that in the specific case, based on the information provided, the publicised telephone numbers together with the data about the MPs – names, photographs and political affiliation, fall within the scope of the definition of personal data and are therefore subject to protection under the PDP Act. The processing of personal data for the purposes of journalism (Article 4(2) of the PDP Act) is not forbidden by law; on the contrary, such processing is necessary for journalistic investigations, but only insofar as it does not violate the right to privacy of the data subject. As the broadcast telephone numbers are different from those made publicly available in the website of the National Assembly for contact with the respective MP or parliamentary group, and there is no information that these numbers have been provided for office use, the conclusion shall be made that personal data has been disproportionately processed in the form of dissemination, thus violating the right to privacy of the data subjects.

An opinion of the CPDP relating to the balance between freedom of access to information and the right to protection of privacy was expressed at the request of the

Chairperson of the Anti-Corruption, Conflict of Interests and Parliamentary Ethics Committee at the National Assembly (ACCIPEC). The request states that, based on a decision of the ACCIPEC, all regional administrations were asked to provide information regarding the state housing properties sold by them during the period 1997–2015. It is also stated that the information received is processed in a tabular form with the intention to be published in the ACCIPEC website. The question asked is whether the information provided in this way contains personal data and if it can be made publicly available. The information processed in tabular form is enclosed and the table contains the following columns: sequential number, order – date and number, three names of the buyer, position held, location of the property, area in sq. m., sale price, tax assessment, seller, by regions. The CPDP opinion is that the information containing the data regarding the housing properties sold by regional administrations in the territory of Bulgaria during the period 1997–2015 and containing the number and date of the order for acquisition of the property, the names and position of the buyer the location of the property, the sale price, the tax assessment, the area and the seller of the property, allows to identify a large number of individuals – buyers of housing properties and, as such, falls within the definition of "personal data" within the meaning of the PDP Act, as it directly and substantially affects the inviolability of individuals and their privacy in the course of processing their personal data. The granting of access to the names or initials of specific individuals who acquired properties by publishing them in the ACCIPEC website is excessive and disproportionate according to the PDP Act and in view of the purposes for which this large volume of information is processed. In the specific case, in order to find the balance between the public interest and the inviolability and privacy of individuals whose data are processed, the ACCIPEC at the National Assembly can distribute through publication on its website information on transactions involving government housing property in tabular form by regions containing the following columns: capacity of the individuals at the time of acquisition of the property – "public official" or "employee of the regional administration"; area of the property; sale price; and tax assessment of the property. This information is sufficient to ensure publicity of the sales of housing properties by regional administrations during the period 1997–2015 and to assess whether the public interests were safeguarded during the sale.

An interesting opinion was expressed in 2015 by the CPDP at the request of the Deputy Minister for Health in connection with a draft Ordinance on surveying patient satisfaction with medical services purchased by the National Health Insurance Fund (NHIF) (the Ordinance). In pursuance of government health policy that is guided by the understanding that the patient is at the centre of healthcare reform and his/her opinion is important in the

studying of the activity of medical establishments, the NHIF is obliged to carry out a survey of patient satisfaction with healthcare services paid by it. This is stipulated in Article 19(7)(15) of the Health Insurance Act (HI Act), according to which the Minister of Health shall define in an ordinance the procedure, manner and criteria for patient satisfaction surveys. The draft ordinance envisages that operating activities relating to the satisfaction survey shall be carried out by a contractor with proven experience in providing services in research and analysis of public opinion, chosen by the NHIF. It is proposed to use the method of telephone interview after discharge of the patient. Interviews shall be conducted when the patient is at home so that he/she can express his/her opinion calmly and without worrying. This involves using patient data (such as initials and telephone numbers). The request states that the HI Act contains a specific provision according to which data relating to the identity of the insured individual can be used to exercise financial and medical control, and data regarding the medical care provider can be used to exercise control of contract implementation (Article 68(1)(6) and Article 68(2)(3) of the HI Act). The survey of patient satisfaction is a form of control and is mandatory in view of the implementation of the sanctions provisions of Article 59(11)(4) and Article 59(13) of the HI Act, according to which a financial penalty shall be imposed in the cumulative presence of several elements, one of which is established systematic dissatisfaction of patients with medical care.

The opinion of the CPDP is that personal data processing through studying patient satisfaction with medical activities relating to the medical care paid for by the NHIF, in accordance with a procedure, in a manner and according to criteria defined in an ordinance of the Minister for Health, is permissible in view of the need for execution of an obligation of the personal data controller (NHIF), stipulated by law (Article 4(1)(1) of the PDP Act in conjunction with Article 19(7)(15) of the HI Act). The personal data controller (NHIF) shall comply with the provisions of Article 5(2)(6) of the PDP Act by including in the contract with the contractor for research and analysis of public opinion of texts, according to which the contractor and its staff/interviewers are required not to disclose personal information that came to their knowledge in connection with the commissioned survey and that patient data received shall be used only for the purposes of the survey. The contract shall also envisage relevant liability and penalties for failure to comply with the obligation for keeping the secrecy of the personal information available. The NHIF shall also comply with the provisions of Article 19 of the PDP Act by informing the recipients of medical services of who will have information regarding the medical care provided to them, for what purpose, and what data will be provided to the contractor carrying out the survey, namely initials, medical treatment facility and hospital unit, telephone number. The personal data controller

shall decide independently on how to discharge its obligation for informing the patients in advance. For example, this can be achieved through an information campaign in the media, brochures in hospitals and doctors' offices, information boards/stickers in medical treatment facilities and offices, and any other appropriate measures, so that the information can reach a maximum number of people. Patients need to be informed in advance that the telephone interviews will be recorded. For the sake of greater legal clarity, the regulation shall include a text which explicitly refers to the PDP Act.

In 2015, in its opinions the CPDP considered specific issues relating to the lawful implementation of the provisions of the Electronic Communications Act (EC Act) in the context of personal data protection.

In an opinion in connection with a request by an undertaking providing public electronic communication services, the CPDP analysed the text of Article 252(1) of the EC Act, pursuant to which processing of traffic data shall be carried out by officials appointed by the undertakings providing electronic communications services. Uncertainties in the interpretation of this text raise some problems in practice. The Supplementary Provisions of the EC Act do not contain a definition of "official", and the entity believes that this creates difficulties in the processing of traffic data. The provision of Article 6(5) of Directive 2002/58/EC states that "processing of traffic data [...] must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services". The request contains the opinion that these can be both persons in employment relationships and other persons executing the orders of the mobile operator, i.e. persons acting under its authority. Thus, the request for an opinion asks the question whether the officials of a supplier of the undertaking can process traffic data, as far as they are under the authority of the undertaking, execute its orders and strictly observe the technical and organisational measures for protecting traffic data against accidental or unlawful destruction, against accidental loss or alteration, or unauthorised or unlawful storage, processing, access or dissemination. The request for opinion further points out, that pursuant to Article 261a(2)(3) of the EC Act only "specially authorised personnel" shall have access to traffic data. The provision of Article 261a(2)(3) of the PDP Act transposes Article 7 (c) of Directive 2006/24/EC, which states that "the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only". In connection with the above, the conclusion is reached that it is possible persons specially authorised by the undertaking to have access to traffic data, without being in employment relationships with the undertaking. The request quotes the definition of "official" pursuant to Article 93 of the Penal Code and adds that the new case law imposes the

opinion that officials are also persons performing activities under the so called service contracts.

The Commission's opinion on this case is that traffic data within the meaning of the EC Act can be processed only by officials appointed by the undertakings providing electronic communications services – workers or employees of the respective undertaking. These officials shall have access only to data required for the corresponding activity.

Another opinion with which the CPDP ruled in connection with the lawful application of the EC Act was on the following matters:

1. Confirmation that data comprising a material part of the provision of a service and are included in the exception under Article 246(2)(1) of the EC Act cannot be treated as traffic data that shall be destroyed in accordance with Article 251g(1) of the EC Act after the expiry of the time periods specified in Paragraphs (1) and (4) of Article 251b of the EC Act.

2. To clarify how to proceed with data that fall simultaneously within Article 251g(1) of the EC Act and Article 42(1) of the Accountancy Act. Pursuant to the EC Act, such data shall be destroyed after the expiry of 6 months, and pursuant to the Accountancy Act they shall be stored for periods many times many times exceeding 6 months.

3. Confirmation that it is admissible to store traffic data that shall be destroyed in accordance with Article 251g(1) of the EC Act after the expiry of the time periods specified in Paragraphs (1) and (4) of Article 251b of the EC Act, after the expiry of these time periods in the events where a court case for collecting claims will be initiated and such data will be requested as evidence by the court until the court case is closed or until the limitation period of the claim has expired.

The Commission's opinion is as follows:

1. Items 1–6 of Article 250b(1) of the EC Act explicitly list the data with regard to which the CPDP has special competencies to conduct inspections for legality of storage and destroying. Statutory texts explicitly stated in the Act and concerning the special competencies of the CPDP cannot be interpreted laterally. Therefore the question if the data referred to in Article 246(1) of the EC Act constitute a material part of the provision of a service by undertakings providing public electronic communication networks and/or services is outside the competence of the CPDP.

2. Data under Items 1–6 of Article 251b(1) that fall simultaneously within Article 251g(1) of the EC Act and Article 42(1) of the Accountancy Act shall be treated as data processed by the personal data controller for different purposes stipulated by law: in the first case for the purposes of providing electronic communications, and in the second case –

for the purposes of accounting for business transactions. Provided that the purpose of data processing is stipulated by law, data controllers are obliged to comply with the statutory time periods for storage of data.

3. It is inadmissible to store data under Items 1–6 of Article 251b(1) of the EC Act, that shall be destroyed after the expiry of the six-month period provided for in the EC Act, for other purposes and for time periods other than these specified in Article 251b(2) of the EC Act (i.e. for the needs of national security and for prevention, detection and investigation of serious crimes).

In 2015 the CPDP also expressed an opinion considering both issues of technological nature and issues relating to statutory prerequisites for eligibility of the processing of personal data. First, the request for an opinion states that the provision of Article 2(1) of the PDP Act sets as a precondition for classifying certain information as "personal data" that such information shall relate to an individual who is identified or identifiable, directly or indirectly, i.e. whose identity is or can be unambiguously ascertained. It expresses the view that, by contrary inference, the reasonable assumption can be made that, within the meaning of the commented provision, information, collected in a manner by which it is impossible to determine unambiguously its holder, should not fall within the scope of the concept of personal data. It also points out that regardless of the fact that the PDP Act does not give a legal definition of "identification number", it could be assumed that according to Article 2(1) of the PDP Act this number is only the number through which the identity of the person, using it or appearing in the registration system under it, can be established beyond doubt and definitely. The view is expressed that similarly, by contrary reference, information about a number, by which it is not possible to identify the person who uses it, shall not be treated as personal data within the meaning of Article 2(1) of the PDP Act. For example, using an identification number such as a barcode, a unit of goods and its manufacturer but not the purchaser of the end product can be identified.

In connection with the above, in the request the CPDP is asked to rule on whether the Media Access Control address (MAC address) falls within the scope of the definition of "personal data" and whether grounds exist to make an analogy between the concepts of MAC address and IP address.

The opinion of the CPDP on the case is that, pursuant to the legal definition given in Article 2(1) of the PDP Act, personal data refers to any information relating to an individual who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific features, i.e. any information and data which, on their own or in combination with other data, could and would in specific circumstances identify and/or

result in an unambiguous identification of a specific individual. As far as the MAC address can, on its own or in combination with other additional information and/or data, result in an identification of a specific individual, it can fall within the category of “personal data” within the meaning of Article 2(1) of the PDP Act. In view of the specific nature and features of the two identifiers (Media Access Control address and IP address), no analogy should be made between them. In all cases where a Media Access Control can, on its own or in combination with other additional information and/or data, result in an identification of a specific individual, it can fall within the category of “personal data” within the meaning of Article 2(1) of the PDP Act and, in this connection, also falls within the scope of the specific supervision exercised by the Commission for Personal Data Protection.

VII. Provision of Personal Data to Third Countries

The reporting period saw a sustained trend of a lower number of requests for permission of personal data transfers to third countries within the meaning of the PDP Act. This was due to the amendments made in 2012 to the Rules on the activity of CPDP and its administration, with resulted in a simplified authorisation regime. In most cases, data controllers are only obliged to notify the Commission of all cases of transfers based on standard contractual clauses or decisions of adequacy. In connection with the above, during the reporting period the Commission received 15 notifications and 11 requests for authorising the transfer of personal data to third countries. Compared to this, in 2013 the CPDP received 13 notifications and 12 requests for authorising transfers, and in 2014 – 11 requests for authorising the transfer of personal data to third countries (Figure 13).

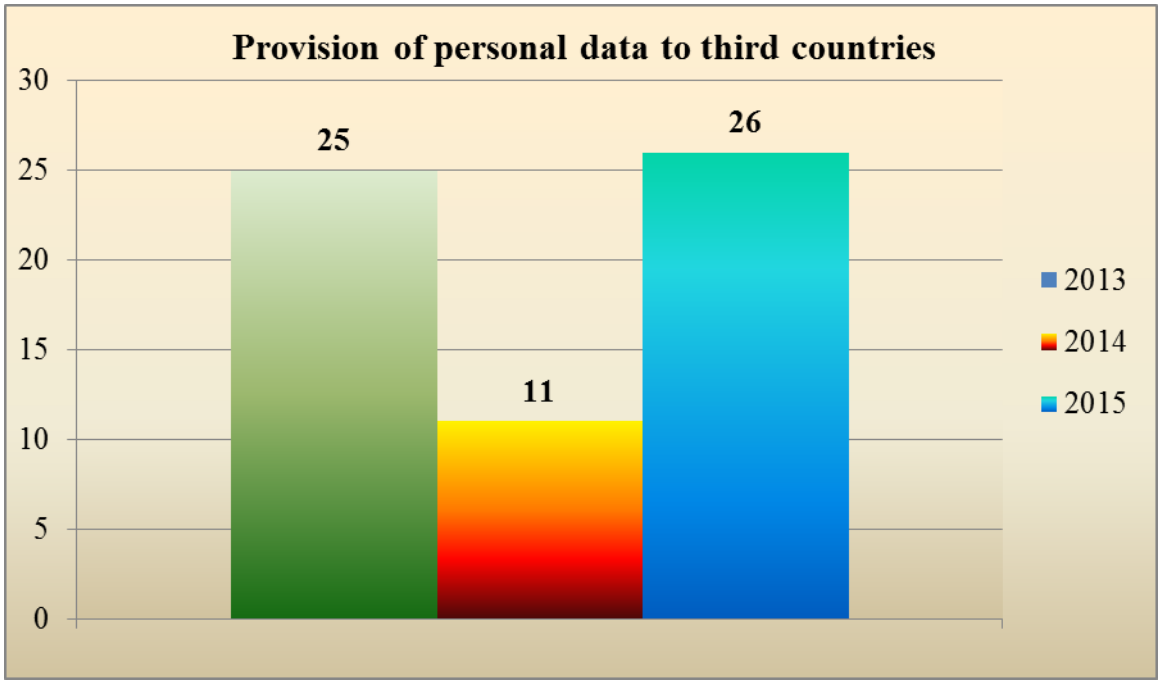

Figure 13

One of the interesting cases on which the Commission ruled during the reporting period was referred by a commercial representation office – part of a multinational corporate group. The applicant requested the CPDP to express an opinion on whether permission for transfer is required, provided that the data is transferred to Switzerland by a commercial representation office located in Bulgaria, and whether a subsequent transfer of data from the Swiss company – data controller – to third parties outside the EU and EEA is in place. The

question was also asked whether transfer of personal data exists in the event that the commercial representation office in Bulgaria transfers personal data to Switzerland by entering such data directly into a server of the American company to which the Swiss company has entrusted the storage of data in a cloud.

The CPDP expressed the opinion that after the transfer of personal data from the commercial representation office in Bulgaria to the Swiss company, the recipient data – the Swiss company – data controller – is responsible for the lawful and proper processing of data in accordance with the criteria stipulated in Directive 95/46/EC and the statutory regulations of the Swiss law. In the event that the Swiss company – data controller – needs to subsequently transfer the data, this shall be done in accordance with the Swiss law and under the supervision of the Swiss personal data protection authorities without the need for additional authorisation by the CPDP of any subsequent transfer of data. An important obligation of the data controller – commercial representation office in Bulgaria (Article 4(1)(2) of the PDP Act and the text to the same effect of Article 10 of Directive 95/46/EC) is to obtain in advance the informed consent of the individuals whose data it will transfer to Switzerland and inform such individuals in advance of the purpose for which the data will be transferred. In addition, it shall also provide individuals with information about the recipients and the categories of recipients of the data, which can include the persons processing the data and their contractors (including information about the processing in a cloud and the fact that the server is in the USA). The presence of informed consent ensures proper processing in terms of data subjects.

In its opinion the CPDP expressed the view that each data controller has the right to determine the purposes and the means for personal data processing. In the event that the data controller does not have the technological ability to store the database in electronic form, it is allowed to conclude a contract with a person as a "data processor" which can undertake on behalf of the data controller to store the electronic database in a cloud mode. This, however, does not mean that the entering of the personal data into the server of the American company is a transfer to the USA. The data subject to the transfer are provided to the Swiss data controller which has determined the means through which it will process the data (storing the personal data in a cloud).

As in previous years, in 2015 were received requests for permitting the transfer of personal data on the basis of the so-called binding corporate rules, which represent a global code of good practices based on European data protection standards. Large multinational corporations develop their own binding corporate rules, complied with on voluntary basis, in order to ensure adequate data transfer environments between companies within the

corporation. These rules are developed as a tool alternative to the standard contractual clauses and are regulated by the Working Papers of the Working Party under Article 29. Since this legal tool is not known in the Bulgarian legislation, when a data transfer is requested on the basis of binding corporate rules, the CPDP authorises the data transfer on the grounds of Article 36b of the PDP Act – on the basis of the provided evidence of the existence of contractual commitments undertaken to the effect that the controller which provides the data and the controller which receives the data ensure sufficient protection.

Another important matter during the reporting period regarding the transfer of personal data is the Judgment of the Court of Justice of the European Union of 6 October 2015, whereby Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the "safe harbour privacy" principles and related frequently asked questions issued by the US Department of Commerce (the Sage Harbour Decision) was declared invalid. The conclusion of the Court that the existence of a Commission decision on adequacy cannot prevent the national supervisory authorities of Member States from considering complaints of individuals relating to the protection of their rights and freedoms in the processing of personal data pertaining to them, which have been transferred by a Member State to a third country, where individuals claim that the extant law and practices of the third country do not ensure adequate level of protection, respectively from expressing an opinion on such transfers of data, is extremely important. The Safe Harbour Decision has implications both at European level and internationally. For this reason, the Working Group under Article 29 of Directive 95/46/EC (WG 29) pays particular attention to this decision by arguing that it is absolutely necessary that Member States have a strong, collective and common position on its implementation. The importance of the decision is emphasised in view of the consideration of other similar cases, litigation of which is pending. In its position expressed in this connection WG 29 firmly holds against large-scale monitoring and uncontrolled processing of data and therefore believes that the existing legal instruments are not an appropriate solution to these problems. Data transfers shall be carried out based on decisions regarding adequacy, based on a thorough analysis of the laws of the third country.

The Working Group called on Member States and European institutions to proceed urgently to discussing the questions asked by the US in order to find the most appropriate political, legal and technological solution that respects fundamental rights for transfers of personal data within the territory of the United States. The only way to reach such a decision is through negotiations and intergovernmental agreements that provide serious guarantees for individuals with regard to the processing of their personal data. The negotiations for a new regulation on the principles of Safe Harbour that are currently underway could be a good start

to achieving an adequate level of data protection, consistent with fundamental principles of their processing, such as indispensability, transparency and proportionality, with clearly regulated mechanisms for control and traceability.

WG 29 analysed the impact of the judgement of the CJEU. In its opinion, Standard contractual clauses and Binding corporate rule can still be used as reliable instruments for the transfer. National supervisory authorities retain the ability to investigate individual cases and exercise their powers in order to protect data subjects. The Working Group under Article 29 undertook that if by the end of January 2016 no solution is found by negotiation with the US, the European supervisory authorities will take all necessary and appropriate actions, including coordinated actions, for law enforcement.

As far as the practical implications of the judgment of the CJEU are concerned, the Working Group under Article 29 believes that transfers of personal data from the European Union to the United States cannot be based on the already invalidated Commission Decision 2000/520/EC on adequacy (the so called "Safe Harbour Decision"). In all cases transfers that continue to be made based on the "Safe Harbour Decision" are unlawful. After the meeting of the Justice and Home Affairs Council held on 8–9 October 2015 in Luxembourg in view of the significant reactions and on the initiative of the European Commission, meetings with the administration and representatives of the business in the United States were held to discuss the implications of the Court judgment and the possible future actions that should be taken to ensure legal certainty.

The position of the CPDP in relation to transfers of personal data to the US has so far been in line with the judgment of the CJEU. The Commission has a consistent practice that, with regard to the entire territory of the United States, no adequate level of protection has been recognised, and that such adequate level of protection is only available to certain entities which are included in the "Safe Harbour" list and have declared before the US Department of Commerce that they will adhere to this framework, i.e. only the specific recipients ensure adequate protection measures.

VIII. International Activity

In 2015 the CPDP not only continued but also further expanded and broadened its international activity. The priority activities and initiatives in this area during the year were:

- to formulate and defend the position of Bulgaria in discussions of the legislative package to reform the legal framework for data protection in the EU, proposed by the European Commission and entering its final stage;

- to organise and host an international conference "Trust, Privacy and Security of Personal Data in the Digital Age", 17–19 November 2015, in which there was great interest;

- to participate actively in the self-assessment process to confirm the readiness of Bulgaria to fully implement the Schengen acquis;

- to start the 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.

1. Participation in international working groups and sub-groups in the field of personal data protection and in the work of joint supervisory bodies

During the year, the discussions of the two legislative amendments proposed by the European Commission in January 2012: General Data Protection Regulation and Directive for processing of personal data in policing and prosecution activity, entered a decisive stage The Council of the EU adopted a common approach on the proposal for a Regulation in June 2015 and on the proposal for a Directive in October 2015, and the negotiations with the European Parliament in the so-called trialogue started. The EU institutions reached a political agreement on the final adoption of the two documents by the end of 2015, which resulted in a great increase in the number of meetings of the leading working group "Information Exchange and Data Protection", "Data Protection" format. The CPDP made every effort to ensure timely and grounded formulation and expression of the Bulgarian position. Recognizing fully its responsibility in this area, the Commission contributed to the clear positioning of Bulgaria among Member States by consistently insisting on upgrading and improvement of the existing standards for the protection of citizens' personal data, while at the same time demonstrating the flexibility required to achieve a compromise between all participants in the process.

During the reporting period, representatives of the CPDP continued to participate in the activities of the Working Party under Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of

such data, and in the sub-parties to it, in particular “Future of Privacy”, “Borders, Travel and Law Enforcement” and “Technology”. In this way the Commission contributed to discussions and common positions of national supervisors on some of the most topical issues in the field of personal data, such as the negotiations on the General Regulation and the Directive, the judgment of the Court of Justice of the EU on transfers of personal data to the US under the Safe Harbour, the development of a European system for PNR data for combating terrorism and serious crime, the general guidelines on the implementation of the judgment of the Court of Justice of the EU on the deletion of information in Google, and others.

In 2015 the CPDP also took part in a number of meetings of the specially established joint supervisory bodies and supervision coordination groups, which are led by the European Data Protection Supervisor and consist of representatives of the national data protection authorities of the European Union Member States: the Europol Joint Supervisory Body, the Joint Supervisory Authority of Customs, the supervisory coordination groups of the Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac, the Customs Information System (CIS) and the Internal Market Information System. In view of the fact that these large-scale information systems of the EU contain personal data of a large number of individuals – citizens of the EU and of third countries, the exercising of efficient and regular supervision of these systems by independent bodies is among the main mechanisms for ensuring the lawful processing of information and respect for fundamental rights.

2. Participation in International Conferences in the Field of Personal Data Protection

International conferences in the field of privacy and personal data protection are an important tool for exchange of knowledge, good practices and ideas and for promoting partnership and interaction among different supervisory authorities, other public institutions, the business and academia. In 2015 the CPDP participated in a number of such forums, among which the 37th international conference of personal data protection authorities in Amsterdam, the Netherlands; the European conference of data protection authorities in Manchester, United Kingdom; the Conference of data protection authorities in Central and Eastern Europe in Durrës, Albania; the Annual meeting for cooperation in the field of law enforcement in Otawa, Canada; the EuroDIG conference of the Council of Europe in Sofia, and other.

We should note the steady trend, especially in the last year, for the Chairperson and Members of the CPDP to be invited not only as participants but increasingly as a key speakers

at various forums, which is a clear and objective indication of the growing international prestige of the Bulgarian supervisor.

On 18 and 19 November 2015 in Sofia the international conference "Trust, Privacy and Security of Personal Data in the Digital Age" was held on the initiative of the CPDP. Over 150 representatives of European Union institutions and authorities, national personal data protection authorities of EU Member States and countries in the region, government institutions, non-governmental organisations, Bulgarian and foreign academic institutions and the business participated in the forum. The European Data Protection Supervisor, Giovanni Buttarelli, and the Ombudsman of the Republic of Bulgaria Maya Manolova were honorary guests of the conference. The organisers – the Commission for Personal Data Protection and the Bulgarian Association for People Management – implemented the event with the partner support of Google, Vivacom, "TechnoLogica", Microsoft Bulgaria, Oracle Bulgaria, ePay, "Ruvex" AD, the Bulgarian Association of Information Technologies (BAIT), thus applying in practice the principle of public-private partnership.

The first day of the conference was dedicated mainly to legal aspects and strategic views for developing privacy in the digital age. The second day of the conference focused mainly on practices for ensuring security and gaining trust, and on personal data protection in the digital world. Special attention was paid to the accountability principle. During the conference, a business breakfast entitled "Finding a partner for a successful project" was held, where in an informal environment the possibilities for implementing joint projects in the field of personal data protection were discussed.

Complete information about the conference is available at the specially developed website: https://cpdp.bg/conference/. The conference materials will be published in 2016 in a periodic electronic edition – a CPDP newsletter.

3. Activities related to the implementation of the Schengen acquis

The CPDP activities on the issues of Schengen during the reporting period were in two main directions: contribution to the self-assessment of competent Bulgarian institutions to confirm the readiness of Bulgaria to fully implement the Schengen acquis, and participation in missions for evaluating member states of the Schengen area in the field of personal data protection.

In the course of the Schengen self-assessment activities, in 2015 the CPDP gave detailed answers to questions concerning the protection of personal data, included in the standard questionnaire in accordance with Article 9 of Council Regulation No 1053/2013 establishing an evaluation and monitoring mechanism to verify the application of the

Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen. The questionnaire contains detailed information about the supervisory body for the National Schengen Information System (NSIS) – the CPDP, its human, financial and technical resources, and the staff training activities. Statistics is included regarding the inspections completed during the past 5 years of institutions processing personal data and/or having access to NSIS data and the technical and organisational measures implemented in connection with data protection.

The interdepartmental plan of measures in the field of personal data protection includes tasks relating to conducting annual training of employees of General Directorate "Border Police" at the Ministry of Interior and the Consular Relations Directorate at the Ministry of Foreign Affairs in the field of personal data protection, updating on the websites of corresponding the institutions of the publicly available information associated with the exercise of the rights of individuals, preparation of information and educational materials for citizens to raise their awareness on the protection of personal data in SIS II. At the end of the reporting period the CPDP created internal organisation in order to implement the measures within the deadlines set in the plan.

In 2015 the CPDP got involved for the first time through its representatives in the Schengen evaluation expert teams for Belgium, Germany, the Netherlands and Lichtenstein. In this context, the appointing of Mrs Maria Mateva, Member of the CPDP, as a leader of the evaluation mission in the Netherlands, is a definite assessment of the professionalism and prestige of the Bulgarian supervisor. At the end of the reporting period Mr Tsanko Tsolov, Member of the CPDP, was elected as a member of the international Schengen evaluation team for Italy. The evaluation will take place during the first quarter of 2016.

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

The CPDP participated actively in the process of preparing the public administration to implement the commitments arising from the Bulgarian presidency of the Council of the EU in 2018. The Commission will be the leading institution in Working Group "Information Exchange and Data Protection", "Data Protection" format, and will nominate a chairperson, a deputy chairperson and a team of experts. The work on the preparation for the Bulgarian presidency will continue in the next reporting periods.

Under the Bulgarian presidency, the CPDP has declared willingness and readiness to host the 40th International Conference of Data Protection and Privacy, which will be held in

the autumn of 2018. This is one of the most important and prestigious international forums dedicated to the protection of personal data.

5. Other International Activities

In addition to participating in various working formats and coordination groups within the EU, the CPDP pays special attention to the cooperation and sharing of experience with supervisory authorities from the region. During the past year the CPDP hosted a study visit of experts from the National Agency for Data Protection of the Republic of Kosovo in the course of the implementation of the project "Support to the Kosovo institutions in the field of personal data protection", financed from the pre-accession assistance funds of the European Union. Experts from Kosovo were made familiar with the long-standing practice of the CPDP related to supervising the processing of data in the health sector, the banking sector, the implementation of the electoral legislation, and the transfer of personal data to third parties and the storage of traffic data. The representatives of the Kosovo data protection authority were introduced to the procedures and decisions of principle in the common European procedure for the adoption of new Community legislation in the field of personal data protection, a process in which CPDP experts play a key role.

At the end of 2015 the General Secretary of the CPDP was nominated as s senior short-term expert for the implementation of the project for developing the administrative capacity of the data protection authority of the Republic of Kosovo. In pursuance of project EuropeAid/133806/C/SER/XK, the General Secretary of the CPDP carried out a comprehensive review of the job descriptions of employees of the National Agency for Data Protection of the Republic of Kosovo and developed a Strategy for human resources development in the Kosovo data protection authority.

IX. Training in the Field of Personal Data Protection

In 2015, the CPDP put prevention in the focus of its activities. One of the main tools for implementing the policy of prevention is the holding of training events aimed at personal data controllers and processors. This is a statutory activity of the CPDP laid down in Article 10 of the Personal Data Protection Act, which the Commission develops systematically over the years.

In 2015, the annual training plan was intended for personal data controllers satisfying the following criteria:

- PDCs the activity of which is of high public and social significance;

- PDCs with regard to which the training needs survey identified need for professional training in the field of personal data protection;

- PDCs whose subject of activity is related to processing of sensitive personal data.

In 2015 a total of 18 training seminars with 535 participants were held. Of these, 6 were for representatives of the public administration, 3 were for representatives of private companies, and 9 training events were organised jointly with the Institute of Public Administration (IPA) (Figure 14).

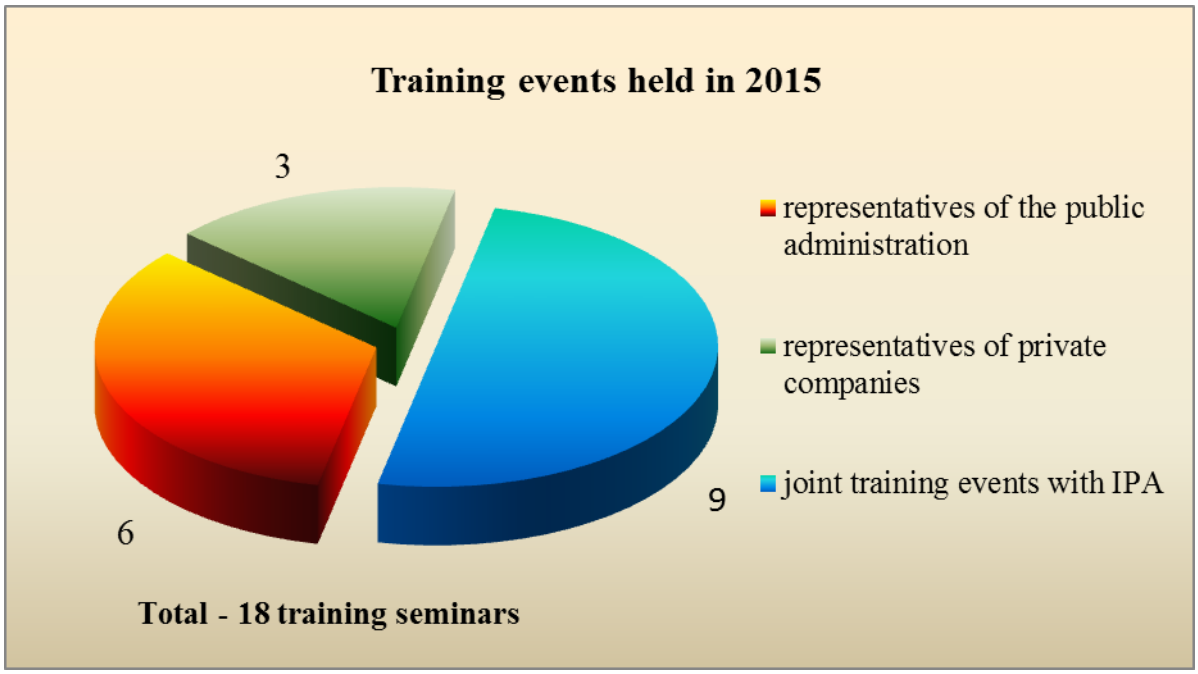

Figure 14

For comparison, in 2013 ten seminars were held, in which 372 trainees were trained, and in 2014 – 19 training events were held with the participation of 515 people (Figure 15).

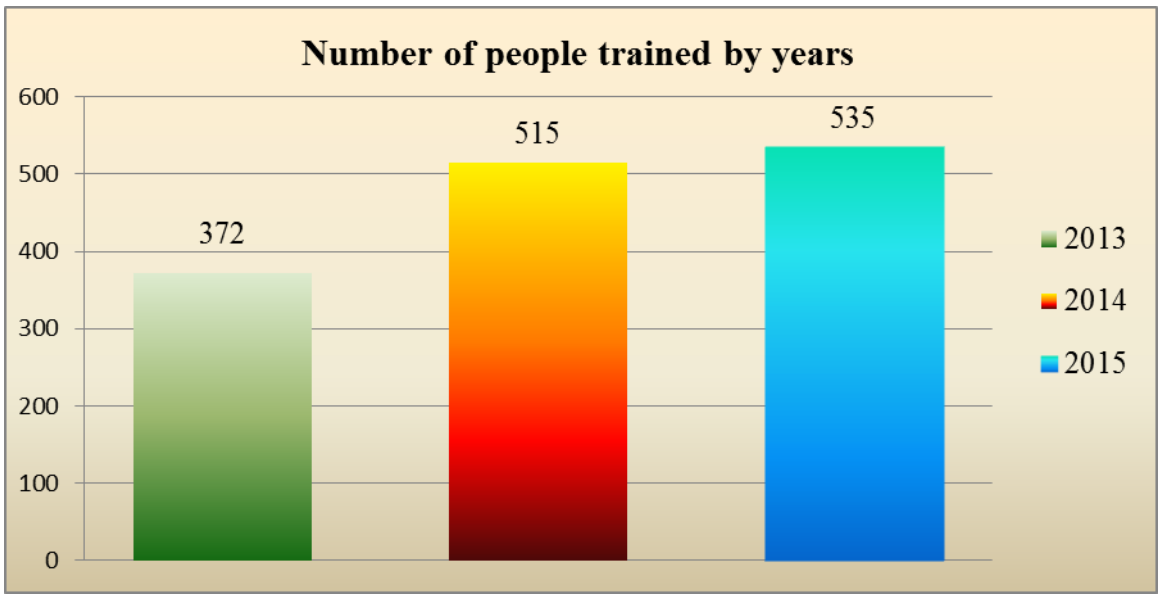

Figure 15

1. Assessment of training events and development trends

During the year, the Commission built upon its vast experience in the field of training. The training programme was enriched with topics concerning the case law of the Court of Justice of the European Union and some new developments and trends in the sector, such as issues relating to big data and Internet connected devices. Practical exercises for trainees were further developed, and the cases presented to them were enriched. This resulted in maintaining the high level of satisfaction with the issues presented, expressed by trainees in feedback questionnaires.

During the year, 138 feedback questionnaires were received by participants in training seminars (Figure 16). Half of them (50 %) assessed the training as excellent, 37 % as very good and only 13 % as good (no trainee selected the lowest grade, "satisfactory"). What trainees like most are the practical examples and cases (32 %), followed by the competence of lecturers (10 %) and the applicability of the training in practice (8 %). The recommendations in questionnaires are directed mostly to conducting follow-up training to reinforce and upgrade the acquired knowledge, and to increasing the duration of the training course.

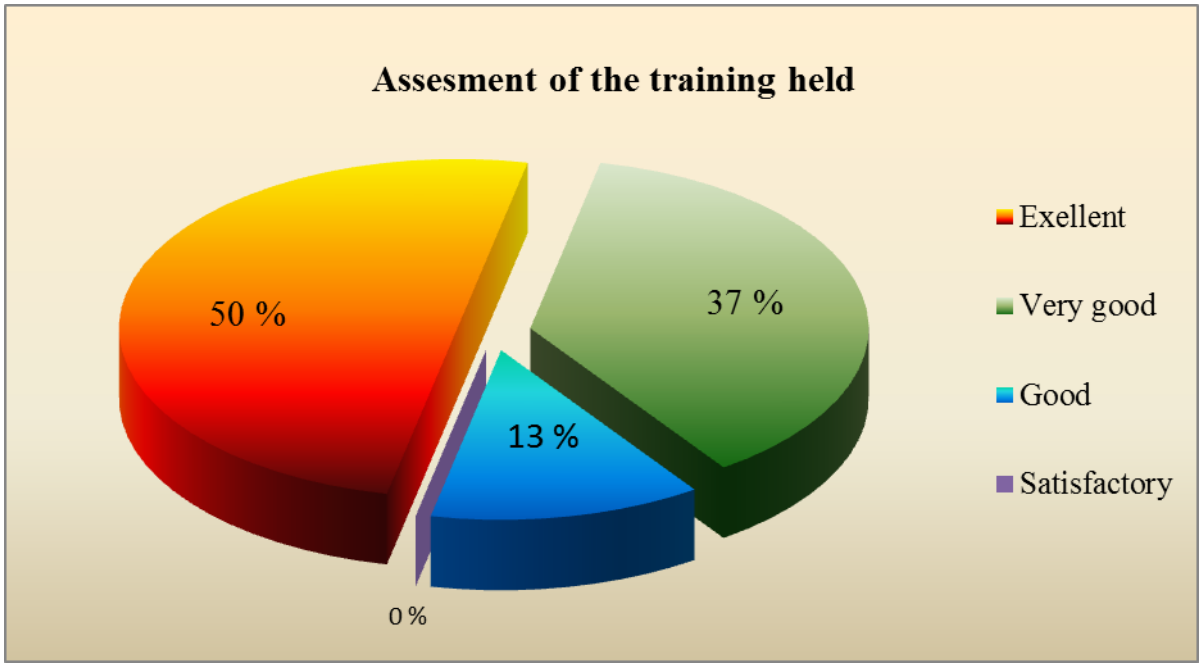

Figure 16

2. Training events for representatives of the public administration

One of the main objectives of the CPDP activities is to ensure compliance of personal data controllers with the PDP Act. In 2015, data controllers which process large volumes of personal data were trained, such as the National Revenue Agency, the Ministry of Education and Science, including data controllers processing large volumes of sensitive personal data, such as the National Health Insurance Fund and the Social Assistance Agency. An external training for data controllers from Burgas District was held, and training of employees of the Central Electoral Commission in connection with the large number of complaints against political parties received in 2014 and 2015.

3. Joint training with the Institute of Public Administration

During the year, the trend of organising training events jointly with the IPA continued. Training in personal data protection is in the Institute's catalogue and enjoys a growing interest on the part of data controllers. During the year, 9 training events were held jointly with IPA. They covered an extremely wide range of trainees, including representatives of local, municipal and district administrations, mayors of municipalities, State Agency "Technical Operations", the Labour Inspectorate, the Employment Agency. All of them were introduced to the basic issues relating to the legal framework, the rights of individuals and the obligations of data controllers, the minimum protection measures, as well as practical cases from the work of the Commission.

4. Training events for private companies

In 2015 training events were held for big data controllers from the private sector and for data controllers processing specific datasets. Employees of "Mobiltel" EAD, "Visa Handling Services" and representatives of companies for fast loans, united in the Association for Responsible Non-bank Lending, were trained.

5. Training needs analysis for personal data controllers and citizens

One of the activities of the Commission during the recent year, in parallel to holding training events, is to study the training needs of personal data controllers and citizens. The results of this activity are used in the development of the annual training plan and in the shaping and adapting the training programme to the needs of the target groups.

- Training needs analysis for personal data controllers

With regard to having knowledge of the Personal Data Protection Act, the majority of data controllers said they were familiar with it in detail (52 %), and only 5 % admitted that they do not have even a vague idea of its provisions. Over 3/4 of the data controllers are aware of their obligations by law and of the rights of individuals in relation to their personal data. Although only 1/3 of the respondents have encountered difficulties in the processing of personal data, 84 % of the respondents to the CPDP surveys believe that training on personal data protection needs to be held for their employees. Data controllers state that training needs to be in the form of lectures and seminars and have a duration of at least one day. They also wish to receive information materials and prefer electronic media for receiving them.

- Training needs analysis for citizens

The results from the study among citizens are similar, but some differences exist. Only 35 % of the citizens claimed that they were familiar with the PDP Act in detail compared to 49 % who have only a vague idea of its provisions. Still, 60 % believe they know what "personal data" includes, and 47 % have general knowledge of how to protect their personal data. Against this background, 72 % of the responding citizens were aware of their rights regarding the protection of personal data, but only 15 % have invoked them in their contacts with data controllers, although 40 % believe that at some point their rights were violated. A considerable portion of citizens (66 %) would like to receive information materials relating to personal data protection, and 62 % prefer to receive such materials by electronic means. The majority of respondents (80 %) are of the opinion that the Commission for Personal Data Protection needs to have wider media presence.

X. Implementation of nationally and internationally funded projects

The reporting period covering year 2015 was still another year in which the Commission was involved actively in project work. Two of the projects of the Commission financed under Operational Programme "Administrative Capacity" were successfully completed. Work on the project entitled "Creation of a national unit for collection and processing of Passenger Name Record (PNR) data in the Republic of Bulgaria", financed under the specific Programme for the Prevention of and Fight against Crime of the European Commission (ISEC), continued.

1. Projects under Operational Programme "Administrative Capacity" (OPAC)

Operational Programme "Administrative Capacity" is the main programme within which the Commission develops its project activities. The total number of projects implemented by the CPDP under OPAC is five, two of which were completed in 2015.

"**Improving the qualification and building on skills and competencies of the CPDP staff for more effective and efficient performance of their duties**"**, Operational Programme** "**Administrative Capacity**"

The project is part of the CPDP policy for investing in human resources and improving services to businesses and individuals provided by the administration. Its objective is to provide training to the Commission employees to improve their professional competencies. The project builds on two other projects, under which most of the CPDP employees were trained in 2013 and 2014. The project includes training events that shall meet specific new challenges and problems in the sector of personal data protection and help the employees of the Commission increase the level of their professional training. Training topics include risk management, strategic planning, communication with EU institutions, budget programming, administrative regulation, implementation of comprehensive administrative services.

The total project duration is 12 months, and the project activities were completed at the end of the tenth month. The total value of the financing contract is BGN 158 068.40, of which BGN 130,191.01, or 82 % of the contract value were utilised (i.e. the economy amounts to almost 1/5 of the contract value). 57 of the employees of the Commission took part in different training events. This accounts to over 3/4 of the administration of the institution (many employees took part in several training events).

The following activities were performed in the course of the project:

- Setting up a project management team.

- Organising and holding of training (training of trainers) for 50 employees of the specialised administration of the CPDP in the field of risk management for the purpose of these employees subsequently providing introduction and training to personal data controllers. Under this activity, 39 people were trained and the amount spent was BGN 44 226.

- Organising and holding of training for 30 employees of the specialised administration of the CPDP in the field of strategic planning, analysis and assessment of the development and implementation of legislation in the field of personal data protection. Under this activity, 26 people were trained for BGN 21 684.

- Organising and holding of 2 (two) training events for a total of 25 employees of the specialised administration of the CPDP in the field of more efficient communication with European Union institutions, development of communication strategies and conducting information campaigns, as well as in work with databases – work with database management software (MS Access). Here, 24 people were trained for BGN 40 176.

- Organising the participation in training events organised by the Institute of Public Administration for 26 employees of the general administration of the CPDP to increase their qualification and competencies in the performance of their direct duties. Training within this activity is provided by the Institute of Public Administration and relates to human resources management, comprehensive administrative services, annual closing of accounts, etc. The costs of this activity amounted to BGN 2 920. Under the activity, 16 employees in the general administration of the Commission were trained.

- Information and publicity – under this activity, 2 press conferences were held, 2 publication in national media were published, and advertising materials for the project were developed and distributed.

- Activities relating to the overall project management and reporting – they include all work done by the team for the successful implementation of the project: planning and management, reporting, monitoring, promotion

"**Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services**"

The implementation of this project constitutes part of the actions of the CPDP in pursuance of the government policy on development of e-government. The overall objective of the project is to improve administrative services provided by the CPDP to businesses and citizens by expanding the offered electronic services, by optimisation of the existing ones and

by their integration in the Single point of access to administrative e-services. The specific objectives include:

- To develop and introduce new modules and functionalities of the Information System for Electronic Registration of Personal Data Controllers;

- To improve and optimise the existing functionalities of the information system of electronic registration of data controllers to ensure integration with the Single point of access to administrative e-services and interoperability with other systems of public administration;

- To help citizens and businesses fulfil their obligations relating to the protection of personal data by optimising and automating critical processes relating to the implementation of the legal requirements for data protection.

The project duration is 18 months. The contract value is BGN 391 089.38, and the project activities were fully completed for BGN 337 794.01 (i.e. BGN 53 295.37 were saved). The project implementation included the following activities:

- Project organisation and management;

- Developing a toolbox to assess the level of impact, to determine measures for data protection by personal data controllers and to conduct inspections by the CPDP;

- Developing and introducing new and updated functionalities of eRALD;

- Information and publicity;

- Audit of the project.

The project is innovative for the administrative structure of the CPDP as it includes integration of electronic services provided by the Commission in the Single point of access to administrative e-services. E-services provided by the CPDP via the Single point of access to administrative e-services are as follows:

- Information regarding registered personal data controllers;

- Information regarding personal data controllers exempt from registration;

- Information regarding refusals of registration;

- Submission of applications for registration of personal data controllers;

- Submission of notifications to update the data entered in the electronic register of personal data controllers;

- Submission of applications for deregistration of personal data controllers;

- Filing of complaints;

- Submission of alerts;

- Submission of requests for opinion.

2. Project under the Programme for the Prevention of and Fight against Crime

Since 2014 the CPDP is a partner of the State Agency for National Security in the project entitled "Creation of a national unit for collection and processing of Passenger Name Record (PNR) data in the Republic of Bulgaria", financed under the specific Programme for the Prevention of and Fight against Crime of the European Commission (ISEC). The project aims at establishing and providing statutory and technical support for the functioning of a specialised unit within the agency, which shall collect and process PNR data in order to protect national security. The Commission participates actively in the development of the statutory rules for the functioning of this unit in order to ensure compliance with the European and national legal framework in the field of personal data protection.

The project will be completed in 2016.

XI. The 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 CPDP 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 the Commission for Personal Data Protection 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 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 83 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 March 2015 was 1 160. It should be noted that during the period the trend that the number of undertakings that fulfil their obligation to provide annual statistics to the CPDP does not correspond to the total number of obligated entities remained unchanged. This steady 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.

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) were 10 7769**;**

- the time elapsed from the initial date of storage until the date on which the competent authorities requested the transmission of data was 3 (three) months in most cases;

- the cases where the request for provision of traffic data could not be responded to were 705**.**

During the reporting period the CPDP was approached by the Chairman of the Commission for control over the security services, implementation and use of special intelligence means and access to data under the Electronic Communications Act (KKSSPISRSDDZES) to the National Assembly of the Republic of Bulgaria with a request for opinion on the Act Amending and Supplementing the Electronic Communications Act, enclosed with the letter. The draft act concerns amendments and supplements in connection with the provisions of Articles 250a–250f, Article 251 and Article 251a of the EC Act, declared unconstitutional by the Constitutional Court. Taking into account the motives in the judgement of the Court of Justice of the European Union (CJEU) in Joined cases C-293/12 and C-594/12, whereby Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Directive 2006/24/EC) is declared invalid, and Ruling No 2 in constitutional case No 8/2014 of the Constitutional Court of the Republic of Bulgaria, the CPDP expressed an opinion on the need for and admissibility of retention of personal data, the proportionality of the measures proposed in the draft law, the purposes for which traffic data is stored, the scope of the measures with regard to persons, the terms and conditions for access to the data, the period of retention of the data, the obligation to destroy traffic data and information sheets based on them, the measures for efficient control of traffic data processing.

2. New powers of the CPDP after the entry into force of the amendments and supplements to the EC Act

With the entry into force of the amendments to the law, the CPDP obtained powers and obligations in connection with the destroying of the data stored after the expiry of the statutory period (Article 251g of the EC Act). In pursuance of this obligation, the CPDP adopted a standard form of a protocol under Article 251g(1) of the EC Act regarding data destroyed by undertakings providing electronic communication networks and/or services. For the purpose of exercising effective ongoing and ex-post control, the CPDP developed and maintains a register of the protocols regarding destroyed data received by undertakings.

Figure 17 presents statistical information regarding the protocols received after the amendments to the EC Act became effective (31 March 2015). It can be also noticed that the number of undertakings that fulfil their obligation to provide the CPDP with 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.

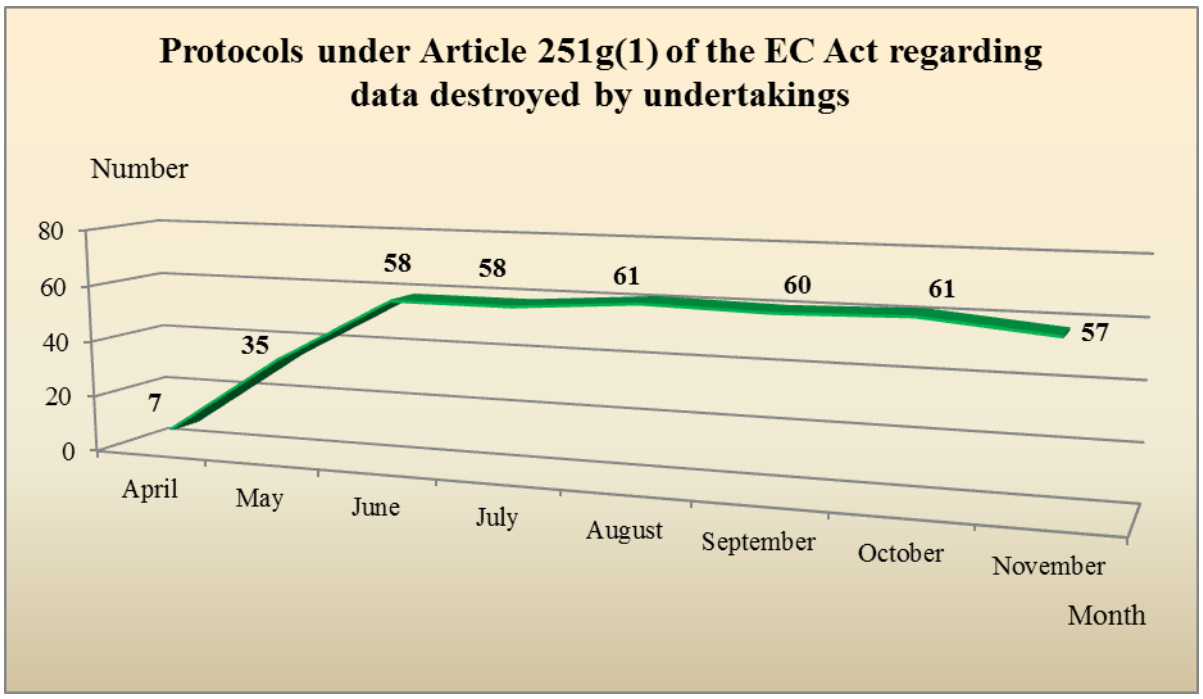

Figure 17

In accordance with its policy of openness and partnership, in 2015 the CPDP held a series of meetings with undertakings providing electronic communication services, during which the changes in the EC Act and the measures to implement the obligations deriving from them were discussed.

3. Implementation of Commission Regulation (EU) No 611/2013 on the measures applicable to the notification of personal data breaches

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 Commission for Personal Data Protection 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.

XII. Institutional collaboration. Partnership with media representatives and information activity

1. Institutional collaboration

In 2015 representatives of the CPDP participated in different interdepartmental expert working groups, including groups regarding amendments to legislation.

The collaboration with the SANS within the project for creation of a national unit for collection and processing of Passenger Name Record (PNR) data in the Republic of Bulgaria (known as the PNR unit) continues. In connection with this, during the reporting period the CPDP approved proposals of texts of provisions regulating the establishing and operation of the unit. The Daft Act Amending and Supplementing the SANS Act was adopted at first reading by the National Assembly.

In 2015, the CPDP maintained regular interinstitutional interaction with the NRA in connection with the implementation of the Agreement between the Government of the United States of America and the Government of the Republic of Bulgaria to Improve International Tax Compliance and to Implement FATCA (Foreign Account Tax Compliance Act) signed on 5 December 2014. The Agreement obliges Bulgaria to exchange automatically once a year with the US information regarding financial accounts of American citizens.

In view of the fact that the agreement with the US does not set out the procedure in which individuals, whose data will be shared, are to be informed of this fact, as well as other issues regarding the exchange of information (e.g. the mechanisms of interaction between the NRA and Bulgarian financial institutions), including personal data protection, amendments to the Bulgarian national law were required. These amendments were also necessitated in connection with Directive 2011/16/EU, amended with Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation – a legal instrument regulating the administrative cooperation and automatic exchange of information between Member States, containing obligations similar to those under FATCA, but taking into account the European context of implementation. The provisions of the amended Directive need to be transposed in the national legislation by the end of 2015 and their implementation shall start on 1 January 2016. In this connection, the CPDP approved texts of provisions concerning data protection, included in the draft Act Amending and Supplementing the TSIPC, which transposes the obligations in question. At this stage the act has already been passed by the National Assembly.

In 2015 the fruitful cooperation with the Institute of Public Administration (IPA) for training of employees from the public sector, established for several years, continued. During the reporting period we witnessed an increased interest in the training course on data protection, included in the Training Programme Catalogue for 2015. In 2016 representatives of the CPDP will continue participating as lecturers on this topic if the public administration demonstrates interest. Detailed information about the training events held with the IPA in 2015 is presented in section "Training in the Field of Personal Data Protection" of this report.

In 2015, on the initiative of the Ministry of Transport, Information Technology and Communications, an interdepartmental working group was set up with the task to prepare the draft Electronic Identification Act and an Act Amending and Supplementing the Electronic Document and Electronic Signature Act. In view of the fact that these laws also discuss 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 Electronic Identification Act was tabled in the National Assembly and was passed in first reading. The work of the interdepartmental group will continue in 2016.

The good institutional interaction between the CPDP and the Ministry of Transport, Information Technology and Communications was also reflected in the participation of Veselin Tselkov, Member of the Commission, as a permanent member of the Council for Network and Information Security and the Council for Intelligent Transport Systems in Road Transport and Interfaces with Other Modes of Transport. During the reporting period this representative of the CPDP was appointed as a participant in the interdepartmental group for drafting a National Strategy for Cyber Security with a horizon until 2020. In the course of the work of the interdepartmental group, the CPDP interacted with representatives of the State Commission on Information Security, the Ministry of Defence, SANS, MoI, the Ministry of Justice, the Ministry of Foreign Affairs, State Agency "Technical Operations", the Bulgarian Academy of Sciences and the Communications Regulation Commission.

The CPDP also cooperated with the Communications Regulation Commission in a number of complaints and requests for information relating to the Electronic Communications Act and the Personal Data Protection Act. The two institutions regularly exchange opinions on matters of their competence, referred to them by other organisations or citizens. Mutual acquaintance with the current case law of the two regulatory bodies is essential for the clarification of a number of borderline cases related to their work.

It should be noted that as a result of the good institutional cooperation with the Research Institute of Criminology and Forensics in 2015 the Commission for Personal Data Protection closed the proceedings relating to complaints filed in connection with the elections held in 2014. The Research Institute of Criminology and Forensics carried out the examinations of signatures requested by the Commission by preparing over 200 expert reports which clarified the facts and circumstances of the complaints and determined their merits. In addition to the complaints above, the Research Institute of Criminology and Forensics prepared expert opinions on 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 contracts or other documents.

In 2015 a joint working group prepared a draft Instructions for Interaction between the NRA and the CPDP aimed at establishing closer cooperation between these institutions in the implementation of actions for collecting public claims according to the procedure established in the TSIPC. The interaction between the CPDP and the NRA is organised on a functional basis or on the occasion of their functions for securing and enforced collection of public claims, established by the CPDP. The main part of this document regulates the rules and mechanisms of the new electronic service "Accepting instruments giving rise to a public claim by external creditors", introduced in the NRA operations in 2015, and the ensuing rights and obligations of the two institutions. After the document is signed and its implementation starts, the speed and efficiency of the CPDP activities in this area will improve considerably.

In 2015, the Commission for Personal Data Protection continued its consistent policy of development and sustainable positive institutional publicity, transparency and openness in the implementation of its activities, beneficial partnership and interaction with other state bodies, with representatives of the civil society and the media.

In 2015 for the 9th consecutive time the CPDP commemorated the Day of Personal Data Protection – 28 January, by organising and implementing a series of events and activities in the interest of citizens and businesses. The Commission believes that raising public awareness is a key preventive measure in safeguarding security in modern society.

Last year the CPDP commemorated the Day of Personal Data Protection with a press conference to present to officials and media its annual report for 2014, and informed the participants about initiatives it planned to implement in 2015 under the motto "Commission for Personal Data Protection – a candidate to host the 40th International Conference of Data Protection and Privacy, planned for the second half of 2018. The event was attended by representatives of the National Assembly, the Ministry of Interior, the Central Electoral Commission, the Ministry of Education and Science, the Registry Agency, the Agency for

Child Protection, etc., as well as by representatives of NGOs – "Access to Information Programme" and "Law and Internet" Foundation. Following the established tradition, every year on this day the CPDP has an "open day" for citizens, personal data controllers and media representatives, who are given the opportunity to visit the institution and receive answers to their questions, as well as updated information on issues relating to the protection of privacy.

On the occasion of the Day of Personal Data Protection and on the initiative of the Commission, meetings and discussions were held with national organisations representing employers in Bulgaria. The Commission held meetings with representatives of the governing structures of the Bulgarian Chamber of Commerce and Industry, the Bulgarian Industrial Capital Association and the Confederation of Employers and Industrialists in Bulgaria (CEIBG). In these discussions they were introduced to the main trends in the processing of personal data, the threats to the processing, and the ways to ensure adequate protection. The needs of employers' organisations for training events for companies and data controllers were discussed. Main directions and instruments for future cooperation were identified, namely holding of regular meetings on issues of mutual interest and competence, exchange of information and good practices, and developing a strategic vision for fruitful cooperation in the field of personal data protection.

During the reporting period the CPDP continued the successful implementation of the Programme for holding a series of meetings of the Commission outside its headquarters, in district centres of Bulgaria, adopted in 2012. Along the line of open dialogue and interaction with citizens, data controllers and media representatives, in 2015 the CPDP held its fourth planned meeting outside the headquarters in Burgas. In order to raise the awareness of the general public and various target audiences on issues relating to the protection of personal data, the programme of ongoing events included additional consultations and an open reception for citizens and personal data controllers, training of data controllers and briefing with representatives of regional media and correspondents of national media.

2. Media policy and coverage

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.

In 2015 the Commission for Personal Data Protection continued to implement successfully its consistent policy for sustainable development and positive institutional publicity, transparency and openness in carrying out its activities.

The CPDP official site is an essential tool for information and public outreach. Materials are regularly published in the individual sections reflecting the activity of the Commission and the monthly media monitoring. The aim is to achieve comprehensive awareness of the broad public with the CPDP activity and full operational transparency.

In 2015 the initiatives for protecting privacy were also supported by maintaining sustainable and beneficial relationships with the Bulgarian media. During the reporting period, due to the already established and facilitated personalised contacts between the Commission and media representatives, over 100 interviews and materials were realised with the participation of the Chairperson, members and experts from 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, "News 7" TV, the Bulgarian National Radio (Horizon and Hristo Botev Programmes), "24 Hours" newspaper, "Trud" newspaper, "Novinar" newspaper, "Politics" newspaper, "Monitor" newspaper, etc. The Commission for Personal Data Protection provided promptly information to journalists on their written or oral request. This resulted in the publication of a significant number of information materials and journalistic investigations concerning various aspects of the protection of personal data. Through constant communication with the media and multiple events, valuable and practical information reaches the population, which is part of the overall policy of the institution to achieve publicity, transparency and open dialogue with the Bulgarian society.

The consistent policy of the CPDP to provide to the public information about its activities and about the personal data protection in Europe and globally is reflected in the maintaining of an institutional website and the issuing of a newsletter. 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 CPC is presented – anonymised decisions on complaints, opinions, compulsory instructions, decisions of the SAC and the SCAC on

appeals against decisions of the CPDP are published. Decisions and opinions regarding requests for transfer of personal data to third countries are published. The website contains a section with updated information on the protection of personal data, divided by topics – topical issues of public interest, questions relating to the implementation of the Personal Data Protection Act with an emphasis on the obligation for registration of data controllers and the registration process, issues relating to the processing of personal data in the electoral process, transfer of personal data, processing of traffic data, etc.

Special forums for filing complaints through the website of the Commission and for asking questions are operational. There is an area for personal data controllers, which can find in the website detailed information about the registration process and have access to the information system eRALD through the CPDP website. The published information about the institution – presentation (history, powers, composition, administrative structure), financial information (daily reports on payments, monthly reports, annual financial statements, budget), is supplemented and updated. In the "Buyer's Profile" section information can be found about all public procurement procedures, public invitations under the Public Procurement Act, and preliminary notices. Information is provided about the work under CPDP projects under different programmes. To study the public awareness and attitudes, questionnaires are provided for filling and expressing opinions.

In connection with the International conference "Trust, Privacy and Security of Personal Data in the Digital Age", organised by the CPDP, a special website was developed as a sub-site of the institutional website of the CPDP. The application has the full functionality of a site accompanying an event of this magnitude – with modules for registration and registering for accompanying events, complete information about the programme, speakers, participants, documents of the event, photo gallery.

Another information tool for the benefit of public awareness is the issuing of a bimonthly newsletter. It contains information about the two months preceding the month of its issuing. 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 Working Group under Article 29, important judgments 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 the CPDP, statistics and analyses of control activities and the activities relating to the registration of PDCs are published. The newsletter has its own ISSN 2367-7759. Currently the newsletter has 600 subscribers. Subscriptions are made through the CPDP website, in the section where the newsletter is published.

3. Sociological Survey "**Personal data protection – public attitudes and raising public awareness"**

In order to outline a longer horizon of actions of the supervisory authority, the Commission periodically resorts to external surveys of public opinion which examine in depth the problems and expectations of society. The first survey of this type was carried out in 2012 in connection with the 10th anniversary of the establishing of the Commission. In view of the expected finalisation of the European legislative reform in the field of personal data protection and the current challenges, the Commission initiated a second survey in 2015.

The objective of the survey was:

1. To establish the levels of visibility, efficiency and credibility of the Commission for Personal Data Protection among citizens and businesses. To identify the expectations regarding the future activity of the CPDP.

2. To establish the level of knowledge about the rights, obligations and responsibilities of citizens and businesses in the field of personal data protection.

3. To identify problem areas relating to the provision of administrative services (including electronic services provided), the control function and the implementation of the legal framework by the Commission for Personal Data Protection with regard to individuals and businesses, that serve to formulate statutory and/or administrative and organisational measures.

4. To identify problem areas and sectors of public relations relating to the protection of personal data according to citizens, holders of personal data.

The main conclusions were that the majority of the adult citizens participating in the survey are aware of the problems of personal data protection, recognise the CPDP as a competent authority and have confidence in it. The comparison with the data from the previous survey in 2012 shows a considerable increase in the confidence in the CPDP, which has almost doubled in 2015 compared to 2012. The majority of respondents are of the opinion that the CPDP has created the conditions necessary for unimpeded access to its services.

However, given the nature of the subject matter, the survey shows that there is a strong correlation between the educational level and the knowledge of personal data protection. The same applies to the social status of the citizens who participated in the survey. Managers and employers are more familiar with the issues. This can be also attributed to the fact that, in their capacity as data controllers, they have a greater awareness due to obligations to protect the data combined with the respective legal sanction mechanism. On the other hand, lower degree of awareness was found with regard to data subjects who only have rights in the field

of personal data protection. These differences in the degree of awareness could result not only from differences in social status but also from differences in the capacity and role of individuals participating in the processing of personal data.

Data from the second survey indicate that in recent years the CPDP enjoys a growing reputation among the population, and its activity is perceived by the public as useful and well organised. This can also result from the degree of awareness. The knowledge of the CPDP as the competent authority under the PDP Act is most clearly expressed among respondents in the age groups of 31 to 60 years, and most poorly among the respondents aged 18–30 and over 61.

The study showed that there is scope for greater communication penetration of various information materials issued by the CPDP or published on the website of the institution or in the media, according to specific target groups in society with different social and educational status and age. Only 4 % of the respondents stated that they have read such materials – brochures, newsletters, and 17 % have come across publications about the CPDP in mass media.

The sociological survey showed sustainability of the established legal culture of the population in relation to the main types of personal data subject to legal protection. The results demonstrated that citizens recognise categorically as personal data the information most frequently used in daily activities and identifying them conclusively (name, PIN, address).

The data from the survey showed that citizens trust most government institutions, including the NSSI and the NSI, which collect and process personal data – 87 %. The trust in health institutions (36 %) and banks (30 %) is also relatively high. Least credible from this perspective, according to respondents, are outlets and malls – 3 %, telecommunication companies – 5 %, and social networks – 1 %.

The prevailing part of the respondents believe they know the main risks associated with the providing of personal data in the Internet. However, the conclusion of the CPDP is that citizens recognise as risk issues related to information security on the web, but do not demonstrate knowledge of specific contemporary risks such as disclosure of personal information, dissemination of personal data, identity theft, profiling for direct marketing and other.

Asked about the need for additional safeguards to protect the personal data, that would be good to be introduced, the view prevails that the growth in the use of Internet, social networking and e-commerce calls for the introduction of more reliable safeguards.

Regardless of the declared high awareness of the risks to personal data, the high proportion of passive behaviour among citizens in the actual recourse to exercising the rights relating to personal data is striking.

XIII. Administrative Capacity and Financial Resources

1. Administrative capacity

The Commission employs 56 members of staff under civil service relationships and 16 under employment relationships, and 8 of these (6 under civil service relationships and 2 under employment relationships) were appointed during the reporting period. The employment relationships with 6 members of staff were terminated. During the period January–December 2015, 19 members of staff were promoted in rank and position.

During the reporting period four recruitment competitions were held to fill vacancies in the specialised administration of the CPDP. For three of these, the competitive procedures were launched at the end of 2014 and were completed in 2015, and 4 new members of staff were appointed under civil service relationships. In 2015, one competitive procedure for a vacant position in the CPDP administration was launched and was also completed with an appointment.

For the CPDP, staff training is an important element of the human resources management function. During the reporting period, the CPDP project "Improving the qualification and building on skills and competencies of the CPDP staff for more effective and efficient performance of their duties" under OPAC, contract No 14-22-45 of 26 September 2014, was used as an essential tool to enhance the professional qualifications of employees of the CPDP administration. Under the project, 11 employees from the general administration who participated in 4 courses and 47 employees of the specialised administration who participated in three courses were trained.

During the year, seven newly appointed civil servants on expert positions passed mandatory training – training of employees entering the civil service for the first time.

Where needed, CPDP administrative staff also took part in trainings on specific topics related to the activities of the Commission outside those provided in the annual plan and the project, namely:

- "Closing of accounts and taxation of budget entities for 2015", "Solution" – 1 employee;

- "Preparation for an examination in professional project management", "Projecta BG" – 2 employees;

- "Efficient counteraction of corruption practices" under a project of the Inspectorate General of the Council of Ministers – 4 employees;

- "Assessment of institutional performance", Institute of Public Administration – 1 employee;

- "Ex-post assessment of the impact of statutory instruments and programmes", Institute of Public Administration – 1 employee;

- "Training of end users for work with UISCHURDA", "TechnoLogica" – 1 employee;

- "Training of end users for work with IISDA", "Information Services" – 1 employee.

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.

In order to prevent new risks and threats in the field of protection of personal data resulting from the development of information technology, the Commission for Personal Data Protection identified a need for additional experts with a high level of competence and qualification in the field of law and information technology. Another justification of the need to increase the number of experts in these fields stems from the fact that the Commission for Personal Data Protection, unlike other collegiate bodies in the Republic of Bulgaria, has no territorial structures to support its work on the ground. This requires the available expert staff to perform its functional responsibilities relating to control activity and training throughout the country, including in the course of inspections in the field of protection of personal data processed by missions of Bulgaria abroad. The same applies to the procedural representation before the courts in the entire country.

In order to fulfil its obligations at national level in the field of personal data protection and the international commitments arising from the expected new general regulation, Regulation 611/2013, and the future accession to the Schengen area, when preparing the draft budget for 2016 the CPDP stated the need to increase personnel costs and open 8 new positions for high-level experts in the field of law and information technology. As the 2016 State Budget of the Republic of Bulgaria Act did not reflect the requested additional funds for staff positions, the Commission will continue its efforts in this direction in the coming periods.

2. Administrative services

In 2015, in order to enhance the quality of administrative services provided by the Commission for Personal Data Protection, on the grounds of Article 21(1) of the Ordinance on the general rules for the organisation of administrative services (OGROAS) the Commission for Personal Date Protection developed and approved a "Customer Charter"

outlining the framework of the relationships and the parameters of the provision of administrative services to citizens. The Charter sets out the key rules in accordance with which the Commission wishes to work on improving administrative services, introduces addressees to the principles and standards for the provision of administrative services and the level of service, on which citizens can rely from the staff of the Commission, and what they can expect from the administration and what they can do in the event that they are dissatisfied with the administrative service.

By approving the Charter, the Commission for Personal Data Protection made a step towards increasing public confidence in the professionalism and ethics of Commission staff through constant and open communication with citizens using administrative services and raising the prestige of the administration, ensuring compliance of its employees with ethical standards of behaviour in accordance with the provisions Code of Conduct for Civil Servants.

Compared to the volume of correspondence processed in previous years, in 2015 a trend towards increasing the number of files processed in the record-keeping office of the CPDP was established. For the period from the approval of the Charter till 31 December 2015 the Commission did not receive any complaints, alerts or objections relating to irregularities and deficiencies in the administrative services provided by the CPDP staff.

3. State of play of the implemented information and communication systems in the CPDP in 2015

During the reporting period, the information and communication infrastructure of the CPDP was further improved, thanks to which at present modern means of communication and exchange are available to the CPDP.

The contracts for maintenance of the information systems critical to the activities and processes of the 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 the CPDP.

4. Public procurement

Public procurement procedures conducted to ensure the implementation of CPDP projects under Operational Programme "*Administrative Capacity*"

In 2014 three public procurement procedures were conducted in the Commission for Personal Data Protection through open invitations according to the procedure established by Chapter Eight "A" of the Public Procurement Act under OPAC projects of the CPDP, the implementation of which ends in 2015, with the following subjects:

- "Information and Publicity" under project "Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services" under OPAC, financing contract Reg. No 13-32-13 of 11 February 2014, Priority Axis III "Quality administrative services and e-government development", Sub-priority 3.2 "Standard information and communication environment and interoperability", budget line BG051PO002/13/3.2-04;

- "Auditing" under project "Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services" under OPAC, financing contract Reg. No 13-32-13 of 11 February 2014, Priority Axis III "Quality administrative services and e-government development", Sub-priority 3.2 "Standard information and communication environment and interoperability", budget line BG051PO002/13/3.2-04;

- "Information and publicity activities" under project "Improving the qualification and building on skills and competencies of the CPDP staff for more effective and efficient performance of their duties" under OPAC, financing contract No 14-22-45 of 26 September 2014, Priority Axis II "Human Resources Management", priority 2.2 "Competent and efficient public administration", budget line BG051PO002/14/2.2-16.

In 2015 two public procurement procedures were conducted in the Commission for Personal Data Protection through open tenders according to the procedure established by Chapter Five of the Public Procurement Act under OPAC projects of the CPDP, as follows:

- "Organising and holding of training events for the staff of the specialised administration of the Commission for Personal Data Protection", allocated in 3 (three) lots, under project "Improving the qualification and building on skills and competencies of the CPDP staff for more effective and efficient performance of their duties" under OPAC, financing contract No 14-22-45 of 26 September 2014, Priority Axis II "Human Resources

Management", priority 2.2 "Competent and efficient public administration", budget line BG051PO002/14/2.2-16;

- "Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services" under project "Improving and expanding the electronic services to businesses and individuals provided by the Commission for Personal Data Protection, and integrating them with the Single point of access to administrative e-services" under OPAC, financing contract No 13-32-13 of 11 February 2014, Priority Axis III "Quality administrative services and e-government development", Sub-priority 3.2 "Standard information and communication environment and interoperability", budget line BG051PO002/13/3.2-04.

The procedures were successfully completed in 2015, and the contracts concluded were executed with good quality and within the deadlines.

Public procurement procedures conducted in connection with the working environment of the CPDP in 2015

In 2015 seven public procurement procedures were announced and conducted in the Commission for Personal Data Protection through open invitations according to the procedure established by Chapter Eight "A" of the Public Procurement Act with the following subjects:

- "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 charge cards for cashless payment";

- "Subscription service of vehicles owned by the Commission for Personal Data Protection after the expiry of the warranty period and supply of spare parts";

- "Supply by purchase of a new car for the needs of the CPDP";

- "Selecting a provider of telecommunications services according to the GSM standard";

- "Upgrading to a new version of the licensed software NetBackup, supply of additional software for protecting information, and their installation".

The procedures described above were completed successfully. Contracts were concluded with execution periods 2015 and 2016.

Public procurement procedures conducted to ensure compliance with international requirements

In 2015, on the grounds of Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches and Article 251g(1) of the Electronic Communications Act, the Commission for Personal Data Protection conducted a public procurement procedure according to the procedure established by Chapter Eight "A" of the Public Procurement Act with the subject: "Development and implementation of a software system for monitoring, reporting and processing of events relating to personal data breaches for the needs of the Commission for Personal Data Protection". The procedure was completed successfully, and the performance of the contract resulted in the setting up at the Commission for Personal Data Protection of a "System for monitoring, reporting and processing of events relating to personal data breaches", which fulfils the requirement of Regulation (EU) No 611/2013 of the European Commission of 24 June 2013 to make available a secure electronic means for all providers of publicly available electronic communications services to notify personal data breaches.

The files relating to all completed procedures are completed and stored in accordance with the statutory requirements of the Public Procurement Act and the Internal Rules on the Conditions and Procedure for Planning, Preparation and Conducting of Public Procurement Procedures, adopted by the Commission for Personal Data Protection. Up-to-date information about the conducted procedures was published and is available in the "Buyer's Profile" section of the website of the institution in accordance with the Internal Rules for Maintaining a "Buyer's Profile" at the Commission for Personal Data Protection.

5. Financial resources – general information on budget spending of the CPDP for 2015

In accordance with the 2015 State Budget of the Republic of Bulgaria Act (SBRB Act) and Council of Ministers Decree No 8 of 16 January 2015 on the implementation of the 2015 state budget of the Republic of Bulgaria, the approved operating budget of the CPDP was BGN 2,256,000. This budget was not amended during the year.

The operational expenditures of Commission for Personal Data Protection and its administration amounted to BGN 2,243,544, or 99.45% 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	1,034,084
02-00	Other remunerations and staff payments	91,993
05-00	Mandatory social insurance contributions paid by employers	271,641
10-00	Running costs	544,723
19-00	Taxes, fees and administrative sanctions paid	9,928
52-00	Acquisition of long-term tangible assets	127,304
53-00	Acquisition of long-term intangible assets	163,871
	Total budget expenditure	**2,243,544**

XIV. CPDP Goals and Priorities in 2016

Given the finalising of the new European legal framework for data protection in 2016 and the ensuing increased responsibilities of the personal data protection authorities, the Commission for Personal Data Protection has set the following goals for the upcoming reporting period:

1. Increased international activity at all levels and in all areas and ensuring the fulfilment of international obligations

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

- Preparing the Republic of Bulgaria for the introduction of the new legal framework nationally and synchronising the national legislation with it, with regard to both the public and private sector, and to the "Police" and "Justice" sectors.
- Mandatory training and preparation by the CPDP of data protection officers (after this figure is introduced in the national legislation) of personal data controllers.
- Maximum contribution to the development of European policies and setting up of new structures, and consolidating the position of the Republic of Bulgaria as an active member of the EU.
- Continuing the preparation for the Bulgarian presidency in 2018 in the "Personal Data Protection" format, and creating the necessary preconditions for the selection of the CPDP as a host of the 40th International Conference of Data Protection and Privacy in the autumn of 2018.
- Continuing the efforts in the field of personal data protection for Schengen accession and maintaining the Schengen acquis in the complicated international situation.

2. Coordinated approach in areas of high public importance

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

- Active activities 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.
- Strengthening the already established good cooperation with the MoI for ensuring a smooth transition to the higher requirements of the new EUROPOL Regulation, which will enter into force as from 2017.

- Carrying out a sectoral inspection of the Education sector in accordance with the Methodology for Carrying out Sectoral Inspections, adopted with a decision of the CPDP, and creating conditions for uniform application of the data protection rules and formulating good practices in this sector.

- Establishing clear rules for the processing of personal data on the course of video surveillance, respectively creating safeguards for individuals – subjects of surveillance.

- Publishing and updating the Open data portal for public information of public interest collected, created and maintained by the CPDP.

3. Policy of active dialogue with citizens and personal data controllers

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

- Initiating a national campaign to explain the new standards for the protection of privacy resulting from the new European legal framework, both among personal data controllers and among individuals.

- Deployment of information activities among target groups of the society according to their social and educational status, taking into account public expectations outlined during the sociological survey in the field of personal data protection carried out in 2015.

- Deployment of an active training programme among data controllers in relation to the increased requirements in the field of personal data protection and the increased responsibility of PDCs in the event of violation of the rules for personal data processing.

- Active contribution to the successful finalising of the initiative of the Bulgarian government for introducing complex administrative services nationwide.

The goals above and the ensuing priorities will be realised through continuous policy of enhancing the professional training and specialised expertise of the CPDP administration. To find an adequate response to the threats to privacy arising from the development and use of information technologies, the CPDP needs to create new jobs and recruit personnel with high level of expertise in the field of law and information technology.

The implementation of a comprehensive and purposeful policy for human resources development is an essential prerequisite for ensuring the implementation of all aspects of the activities which will arise for the Commission for Personal Data Protection as a result of the entry into force of the new legal framework at European level.

The Annual Report of the Commission for Personal Data Protection for its activities in 2015 was adopted by a Decision of the Commission at a meeting held on 20 January 2016 (Protocol No 3).

CHAIRPERSON:

Ventsislav Karadjov (signed)

MEMBERS:

Tsanko Tsolov (signed)

Tsvetelin Sofroniev (signed)

Mariya Mateva (signed)

Veselin Tselkov (signed)