REPUBLIC OF BULGARIA

COMMISSION FOR PERSONAL DATA PROTECTION

ANNUAL REPORT

of the Commission for Personal Data Protection

for 2014

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

TABLE OF CONTENTS

List of the acronyms used in this document

AA	–	Accounting Act
ACSC	–	Administrative Court of Sofia City
APC	–	Administrative Procedure Code
APIA	–	Access to Public Information Act
APP	–	Administrative-penal procedure
BNB	–	Bulgarian National Bank
GD GRAO	–	Chief Directorate of Civil Registration and Administrative Services
CEC	–	Central Electoral Commission
CPC	–	Civil Procedure Code
CPDP	–	Commission for Personal Data Protection
CPP	–	Coalition of political parties
CrPC	–	Criminal Procedure Code
DC	–	Data controller
ECA	–	Electronic Communications Act
EGN	–	Personal identification number of a Bulgarian citizen
eRALD	–	CPDP's electronic system for registration of data controllers
EU	–	European Union
IC	–	Insurance Code
IPA	–	Institute of Public Administration
LAVP	–	Law on Administrative Violations and Penalties
LBID	–	Law on Bulgarian Identity Documents
LCR	–	Law on Civil Registration
LDPCCLG	–	Law on the Direct Participation of Citizens in Central and Local Governance
LE	–	Legal entity
LMAML	–	Law on the Measures Against Money Laundering
LPPD	–	Law for the Protection of Personal Data
LSBRB	–	Law on the State Budget of the Republic of Bulgaria
M/V	–	Motor vehicle
MEC	–	Municipal Electoral Commission

MFA	–	Ministry of Foreign Affairs
MoI	–	Ministry of Interior
MoIA	–	Ministry of Interior Act
MTITC	–	Ministry of Transport, Information Technology and Communications
DL	–	Driving license
NDB “Population”	–	National Database “Population”
NGO	–	Non-Government Organisation
NRA	–	Natural Revenue Agency
OP	–	Obligatory prescription
OLAF	–	European Anti-Fraud Office
PB	–	Private bailiff
PD	–	Penal decree
PP	–	Political party
PPA	–	Public Procurement Act
PSA	–	Private Security Act
QES	–	Qualified electronic signature
RACPDPA	–	Rules on the activity of the CPDP and its administration
REC	–	Regional Electoral Commission
RILMAML	–	Rules on the Implementation of the Law on the Measures Against Money Laundering
RTA	–	Road Traffic Act
SAC	–	Supreme Administrative Court
SACP	–	State Agency for Child Protection
SANS	–	State Agency for National Security
SEAV	–	Statement establishing an administrative violation
SF	–	Statement of Findings
SP	–	Supplementary Provisions (of a law)
SPA	–	State Property Act
ST	–	Sole Trader
TD NRA	–	Territorial Directorate of the National Revenue Agency
TPA	–	Territorial Planning Act
TSIPC	–	Tax and Social Insurance Procedure Code

I. Introduction

The present Annual Report of the Commission for Personal Data Protection (CPDP) is drawn up in accordance with Article 7(6) of the Law for Protection of Personal Data (LPPD) and encompasses the period 1 January 2014 to 31 December 2014.

The Report presents information and analysis of the main areas of the institution's activity in the reporting period, the main focuses being the registration of data controllers (DCs) and of the registers maintained by DCs, checks initiated on received irregularity reports (alerts), review of complaints lodged by citizens, the Commission's supervisory activities and its opinions on data protection issues. Due attention has been paid to activities related to international cooperation, training in the area of data protection and implementation of EU-funded projects.

The CPDP's administrative capacity and financial status in the year 2014 are also reported.

II. Registration of data controllers and of registers maintained by DCs

In fulfillment of its statutory obligation laid down in Article 10(1)(2) of the LPPD, the CPDP keeps a Register of data controllers (DCs) and of the registers maintained by DCs ("DC Register"). The DC Register is public and is maintained on electronic media.

The CPDP's activity for maintaining the DC Register is consistent with the e-Government concept and aims to provide to citizens a highly efficient and user-friendly service based on the "one-stop shop" mechanism. It comes in the form the eRALD system – a web-based application accessible from CPDP's website, which supports all DC registration functions. The system enables data controllers submit electronic applications for registration as well as update the already uploaded data in accordance with the LPPD requirements. The public registers can be queried about registered DCs and personal data registers maintained by them, DCs exempted from the registration requirement and DCs the registration of which is refused by the CPDP.

In 2014, DCs 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 2014 the number of system users reached 343 292, of which 312 804 applied for DC registration and 30 488 requested an exemption from the registration requirement (Fig. 1).

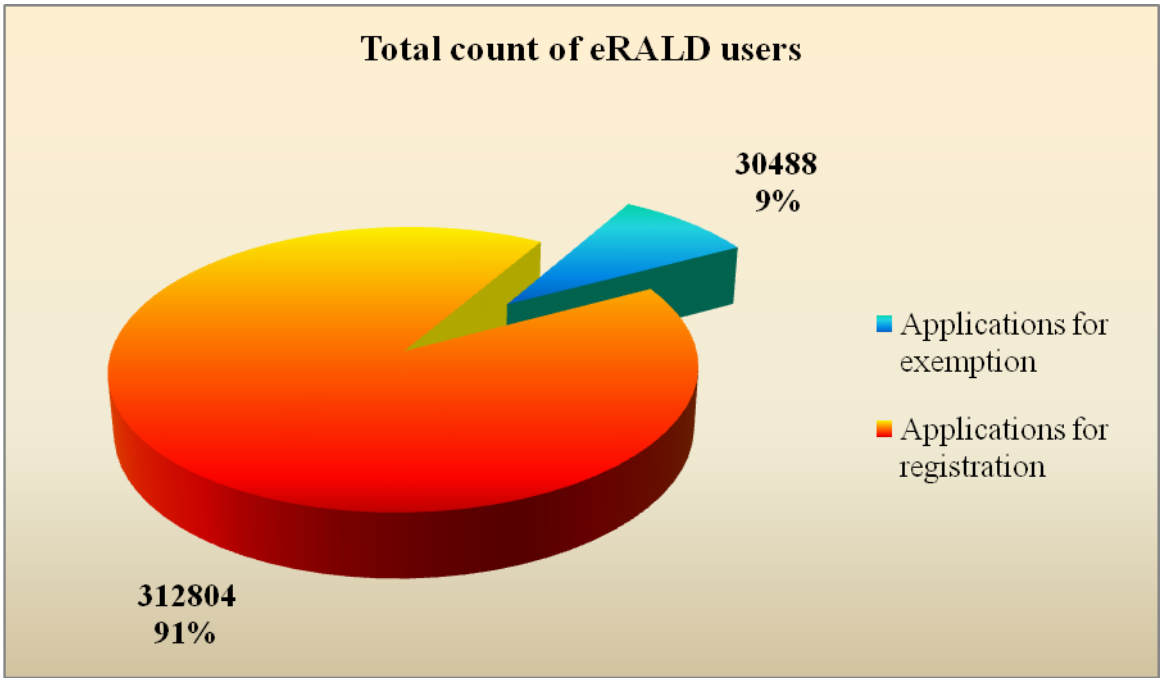

Fig. 1

In 2014, the CPDP registered 26 687 DCs in the DC Register. Thus, the overall number of registered DCs became 273 069 (Fig. 2).

Some eRALD users still make mistakes during the registration procedure, most often by choosing the wrong form or by failing to submit all mandatory documents. In these cases the registration procedure cannot be completed.

Of the 30 488 DCs which have applied for exemption from the registration requirement by 31 December 2014, the CPDP has by its decisions exempted 27 497, including 146 during the reporting period (Fig. 3). In the other cases the DC submitted a registration and an exemption application at the same time. In these cases the CPDP refuses the exemption request and registers the DC.

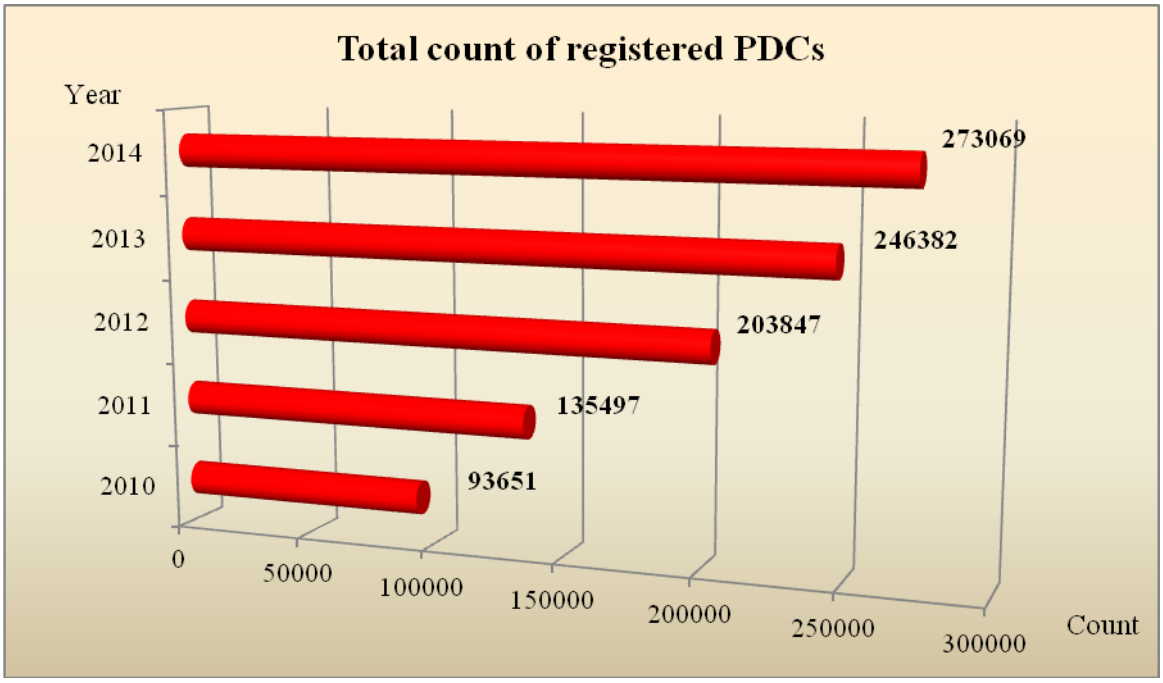

Fig. 2

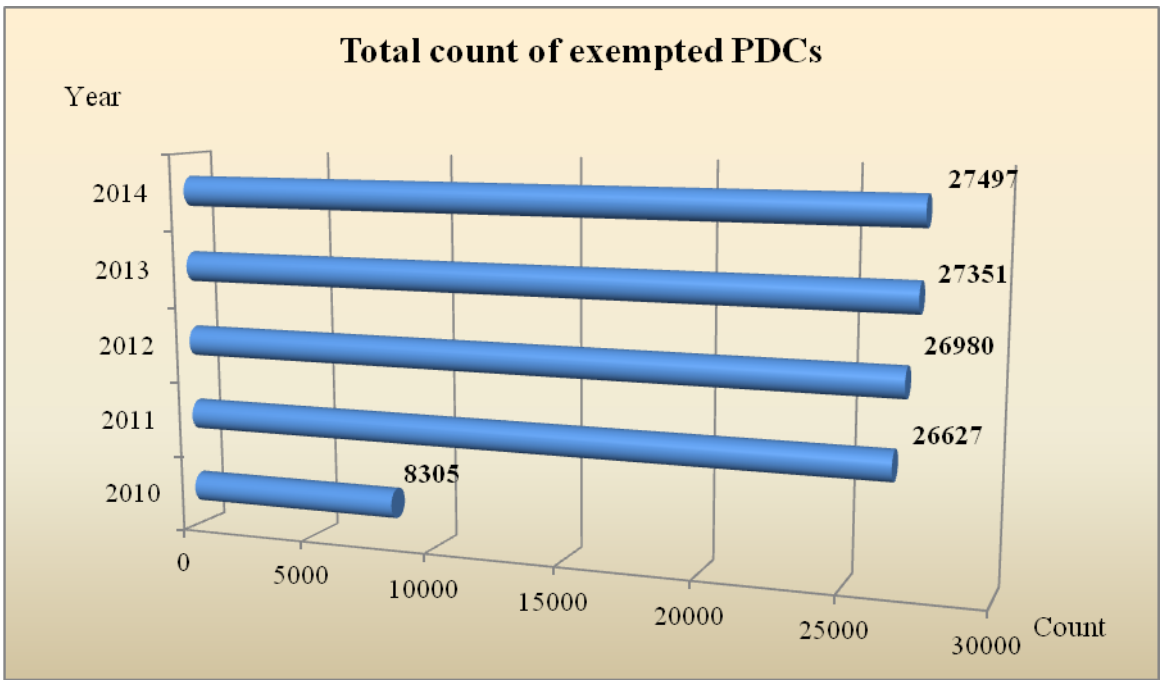

Fig. 3

In the reporting period, the CPDP received 62 applications for deregistration of DCs and adopted decisions for delisting these applicants from the DC Register.

Where a DC applies for processing of data falling within the scope Article 5(1) LPPD or 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* check in accordance with Article 17b LPPD before it can be registered in the Commission.

During the reporting period, 2194 data controllers were subjected to an *ex ante* check before registration as per Article 10(1)(2) LPPD. On the grounds of Article 17b(3)(3) LPPD, the CPDP by its decision refused to register 293 data controllers in the DC Register.

In 2014, the CPDP processed 28 078 paper-based documents related to the registration of DCs. 56 888 electronic messages were sent to DCs from the eRALD system, while the eRALD inbox received 325 emails, which were forwarded for processing by staff members according to their competence.

III. Protection of the rights of natural persons in relation to the processing of their personal data

1. Proceedings related to the examination of complaints and requests. Replies to enquiries received from citizens. Statistics and analysis of the complaints and requests received by the CPDP:

1.1 Comparative analysis of the complaints received by the CPDP in previous years and in the reporting period by DC types and overview of the key areas of public life, in which violations in the area of personal data protection were most frequently observed

As part of its supervisory remit in the area of personal data protection, the CPDP has the power to examine complaints lodged by natural persons against DCs over alleged violations of their rights laid down in the LPPD. Complaints or requests for protection of violated rights can be lodged within one year after the applicant obtains knowledge of the violation, but not more than five years after the occurrence of the violation.

The procedure is regulated by the Administrative Procedure Code and is provided for in Article 38 and seq. of the LPPD. The procedure concludes with an administrative act issued by the CPDP, which is subject to judicial review.

If the applicant's request does not relate to violations of his or her rights, the CPDP carries out checks and issues obligatory prescriptions for the DCs in relation to the protection of the personal data of natural persons.

Depending on the area of activity of the DC against which the complaint is lodged or on the type of personal data processed, the complaints and requests received by the CPDP in 2014 can be divided in three broad categories:

The first category includes **complaints against DCs operating in the area of telecommunications**. These DCs are most often accused of misusing the applicants' personal data. The complaints in this category can be provisionally divided in two subcategories: allegations that a mobile operator has processed unlawfully the applicant's personal data by transferring the data to a debt collection company and complaints over usage of personal data for the conclusion of contracts, which the individual is unaware of and unfamiliar with, and has never signed.

In comparison to previous years, there has been a rise of the **complaints against courts, prosecution offices, private bailiffs, etc.**

Part of the complaints against courts concern the processing of personal data in relation to initiated court cases. In these situations the CPDP deems that processing of personal data for the purposes of a court case is appropriate and lawful insofar as the DCs have legitimate reasons for such processing, namely an obligation imposed on them by law. The Civil Procedure Code (CPC), the Administrative Procedure Code (APC) and the Criminal Procedure Code (CrPC) do impose on the court the obligations to collect a certain scope of personal data for the parties to the procedure, which is specific to each case. Another part of the complaints lodged at the CPDP are directed against particular courts in relation to enforcement actions under Article 410 CPC. In most cases the applicants deny either the existence or the amount of their debt, and therefore assert that the enforcement action violates their LPPD rights. In these situations, the processing of personal data is also deemed lawful, provided that there is a legitimate reason for this. It should be noted that the CPC allows anyone to file an objection against the initiation of an enforcement action against him or her, however this is not subject to control by the CPDP.

Similar are the complaints lodged against private bailiffs (PBs). In these cases it is for the CPDP to assess whether the DC, that is the particular PB, has a legitimate reason to process the data. The CPDP does not review the lawfulness of the orders issued within the enforcement procedure. Where an individual believes that an order or action of the private bailiff violates his or her rights, the individual can challenge the order or action before the competent body.

Another DC category **challenged at the CPDP were central and local authorities**. Most of the complaints were about unlawful dissemination of personal data, usually on the official website of the relevant authority. In the prevailing majority of cases the CPDP established that the DC had committed an administrative violation and accordingly imposed an administrative penalty or gave a binding instruction to the DC.

The year 2014 saw an increasing number of **complaints against the managing boards (managers) of condominium buildings**. The main complaint is about the installation of cameras, which according to the complainants violate their rights to personal immunity and privacy laid down in the Constitution and in the LPPD. Among the complaints lodged at the CPDP there were ones against neighbours who on their initiative installed cameras in the common areas of the building, most often in order to protect their property.

It should be noted that an indispensable condition precedent for the initiation of an administrative procedure at the CPDP is that the respondent party to the complaint has the capacity of a DC in accordance with the legal definition provided in Article 3 LPPD. The

position of the Commission, available on the Practice section of its official website, is that condominium building managers are DCs in the meaning of the LPPD, therefore their personal data processing activities fall within the scope of the Commission's control on compliance with the LPPD. Since condominium building managers are appointed for a certain period of time, the CPDP has by its decision exempted them from the obligation to file applications for registration at the CPDP, which the LPPD imposes on each DC. However, the exemption from the registration obligation does not exempt the obligated person from the obligation to comply with the provisions of the LPPD.

In the last year there were many complaints against political parties (PPs) and coalitions of political parties (CPPs). The first category of complaints pertained to unlawful processing of personal data by including the complainants' full names, personal identification number (EGN) and signature in PP lists for the purposes of the registration of the political party at the Central Electoral Commission (CEC). A detailed analysis is provided in Section V – Control on political entities.

Most of the complaints from natural persons in 2014 related to DCs in the following domains (Fig. 4):

- Political entities – 549 complaints
- Telecommunications – 137 complaints
- Banks and credit institutions – 36 complaints
- Judicial system, notaries, bailiffs – 17 complaints
- Media outlets and Internet – 14 complaints
- Local authorities – 6 complaints

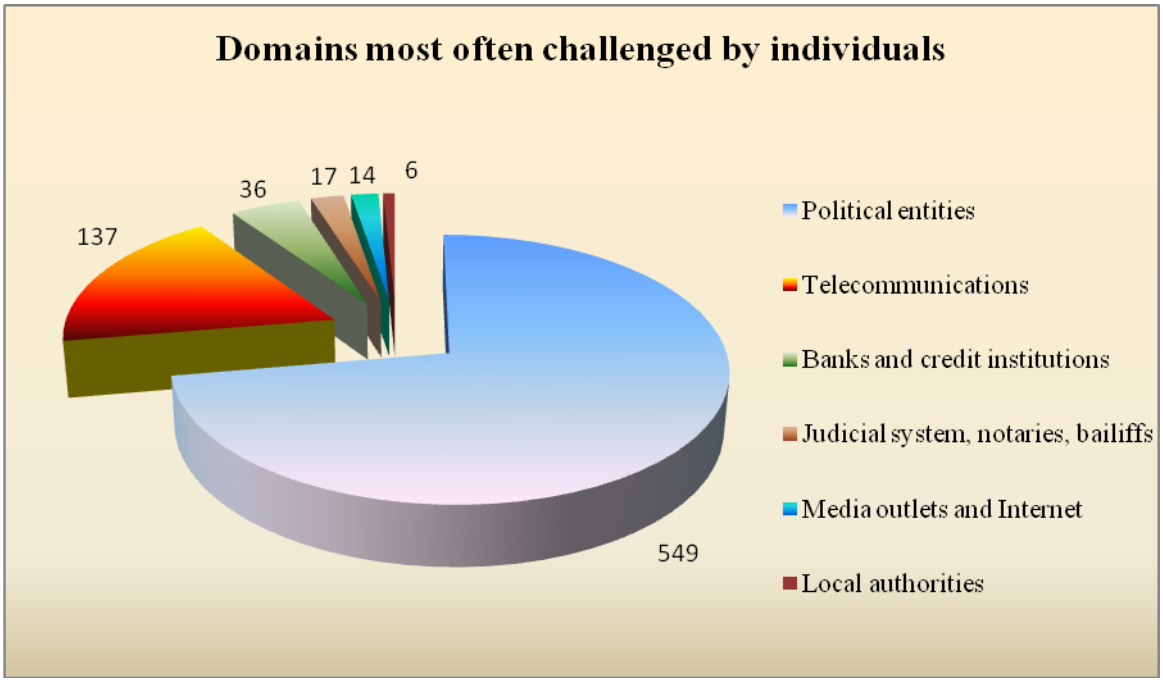

Fig. 4

In 2014 the CPDP received 1100 complaints related to the processing of personal data. Of this total count, 496 complaints concerned the usage of voters' personal data in lists submitted to the CEC for the registration of political parties and coalitions of political parties for the election of European Parliament Members, and 53 complaints were related to usage of such data for the national parliamentary elections. 596 complaints were examined in public hearings.

In comparison, the complaints lodged in 2013, 2012 and 2011 were 550, 548 and 458, respectively.

The next chart (Fig. 5) illustrates the increasing number of complaints lodged at the CPDP in the past four years:

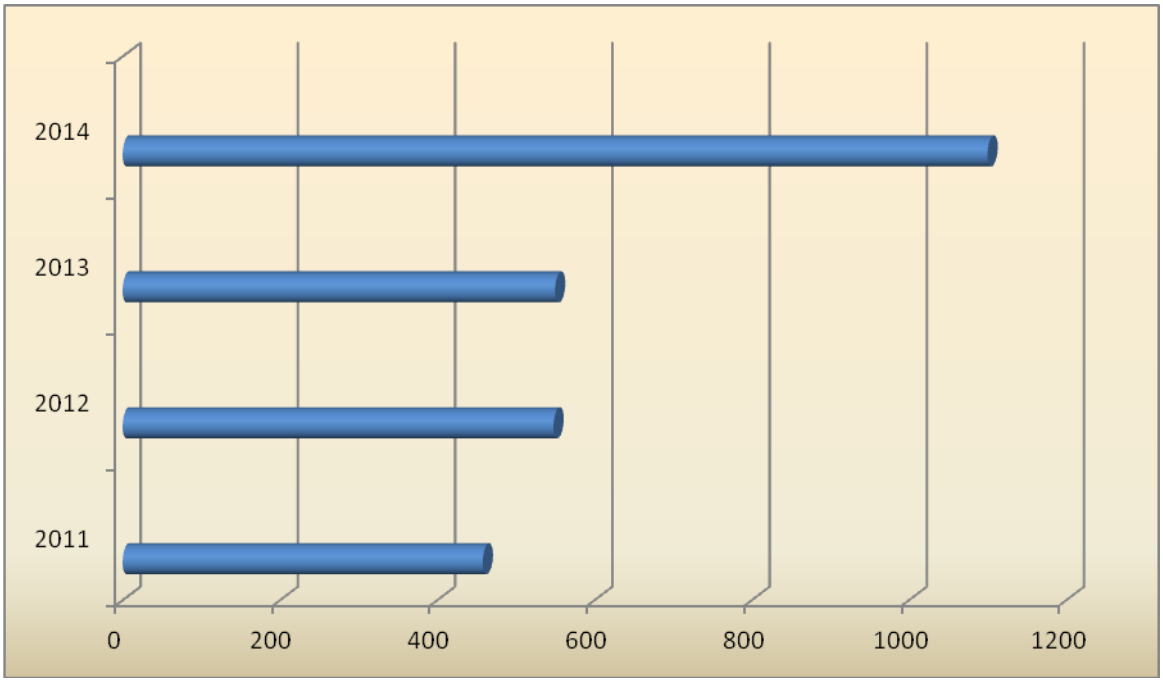

Fig. 5

During the reporting period the CPDP, acting as a collective body in the procedures under Article 38(1) LPPD, issued 161 decisions, which can be divided in several categories on the basis of the following criteria:

1. Decisions by which the complaints were found justified, accordingly the complaints were well-founded and administrative penalties were declared: 45 decisions, including 6 decisions with obligatory prescriptions for to the DCs;

2. Decisions by which the procedure was suspended due to the existence of a parallel procedure at the MoI or prosecution authorities: 18 decisions;

3. In 25 decisions the complaint was found inadmissible;

4. In 18 decisions the complaint was found defective;

5. In 2 decisions the CPDP approved settlement agreements reached between the parties to the administrative procedure.

Fifty-three complaints were rejected as unjustified since the Commission did not find violations of personal data processing rules or of complainants' rights.

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

The established violations committed by DCs can be assigned to 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) LPPD), in respect of which the CPDP imposed sanctions in the total amount of BGN 88,000;

- Processing of personal data in the absence of a lawful reason for the data processing operation (Article 4 LPPD), in respect of which the CPDP imposed sanctions in the total amount of BGN 181,000;

- Processing of personal data, wherein the DCs 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 LPPD), in respect of which the CPDP imposed sanctions in the total amount of BGN 28,000;

- Failure of the DCs to assist the CPDP exercise its supervisory powers (Article 22(5) LPPD), in respect of which the CPDP imposed sanctions in the total amount of BGN 1,300;

- Sanctions in the total amount of BGN 15,000 were imposed for violations of Article 5 LPPD, namely processing of sensitive personal data;

- Sanctions in the total amount of BGN 11,000 were imposed for violations of Article 20 LPPD, namely failure by the DC to provide information to the natural person.

Five thousand one hundred thirty-five BGN in lawyer fees were awarded to the CPDP of which BGN 2,825 were paid on voluntary basis.

The total amount of the penalties imposed by CPDP administrative acts in 2014 was BGN 476,400. The amounts collected and payable pursuant to CPDP decisions in 2014 came to BGN 206,205 (BGN 37,672 of these were collected coercively by the National Revenue Agency).

1.2. Specific cases and case-law of the CPDP in 2014:

The CPDP is seized on complaints related to the processing of personal data in various spheres of public live such as access to services (telecommunication, banking, credit, utilities), education, healthcare, local authorities, judiciary, debt collection, access to and dissemination of information, etc. This being said, the case-law of the CPDP is very broad in

terms of the diversity of the complaints received. The Commission's decisions on the various cases are available at the Practice section of its website. Some of the more specific cases dealt by the CPDP in 2014 are discussed below:

1. The CPDP received a complaint concerning unlawful processing of personal data in the form of copying the complainant's identity card and driving license (DL), and storage of these documents in relation to the complainant's use of a "test-drive" service. It was established during the procedure that for the purpose of testing the performance a new vehicle the respondent company had copied the complainant's identity card and DL, and had retained copies of these documents.

It was established from the evidence collected in this administrative case that processing of the complainant's personal data in the form of copy his DL is legitimate, therefore the CPDP held that part of the complaint to be unjustified. In case the driver commits a road traffic offense, which is detected and documented by a technical device, rather than in the presence of a road police officer and the offending driver, then the DC, in the capacity of owner of the motor vehicle, has a legal obligation (Article 189(5) of the Road Traffic Act, RTA) to present to the relevant territorial unit of the MoI written statement, including details of the offender and copy of the offender's DL.

The CPDP held that the complaint is justified in respect to the processing of the complainant's personal data by photocopying his identity card for the purposes of the "test drive" service used by the complainant. The evidence collected in this administrative case leads to the conclusion that the processing of the complainant's personal data is unlawful since it is not compliant with the requirements for admissibility of the personal data processing operation laid down in Article 4 LPPD. By copying the complainant's identity card for the purposes of the "test drive" service, the company has also violated the provisions of Article (2)(2)(3) LPPD, as the collected personal data is irrelevant and disproportionate to the objectives for which the data is processed. The ID card contains more details of the natural person than necessary for identification of that person as a user of the service offered. Moreover, in the presented standard "test drive" agreement and its annexes, including in the document signed by the complainant, the user is required to identify himself/herself by his/her full name, personal identification number (EGN) as well as number and date of the DL. In these situations the identity card should be used only for verification purposes, it has to be checked by the company and then immediately returned to the user.

In its decision on the complaint the CPDP imposed on the company an administrative penalty in the form of BGN 12,000 pecuniary sanction for violation of Article 4(1) LPPD. The decision was not appealed, it entered into force and the penalty was paid by the company.

2. The CPDP was referred with a complaint stating that an article published on a news website contained a document showing personal data, names, EGN, address and identity card number. The published document was a loan repayment plan.

It was established from the evidence collected in this administrative case that personal data was processed for journalistic purposes, meaning that the processing of the data was admissible and lawful.

However, Article 23(1) LPPD required the DC to undertake the necessary technical and organisational measures in order to protect the data against accidental or illegal destruction, or against accidental loss, unauthorised access, modification or dissemination, or against other illegal processing. In its administrative ruling the CPDP held that the DC had not taken the necessary measures to protect the data from unauthorised access.

3. A complainant lodged a complaint with the CPDP alleging that a municipal administration had processed his personal data by writing his EGN three times in a Statement of Findings (SF). The SF was glued on the complainant's property and was also posted on a dedicated notice board in the town. The complainant was told by people who knew him that he was wanted by the police and his personal data is posted around the town and on his property.

Based on the evidence collected in the administrative case the CPDP held that the DC had violated the provisions of LPPD Article 2(2) points 1 and 3, namely the principles of propriety, lawfulness and proportionality. The CPDP did not agree with the respondent's assertion that the person was notified about the SF in accordance with the requirements of paragraph 4(1) of the Supplementary Provisions of the Territorial Planning Act (TPA). In fact the person's current address was known to the DC, hence it wasn't necessary to deliver the SF in the said manner.

4. A complainant informed the CPDP that on 31 January 2014 he received an audit report and annexes from the Territorial Directorate of the Natural Revenue Agency (TD NRA). The complainant was subject to a tax audit as a natural person and during the audit procedure the tax officers requested documents and written statements from three

accountancy firms the business of which was similar to that of the complainant. Seen from the copies of these requests, they contained the complainant's name, EGN, postal address, place of living as well as email address.

When considered on the merits, the complaint was found to be justified since the evidence collected in this administrative case reveals that the DC had processed the complainant's personal data in violation of the principle of proportionality, namely by disseminating the data in the information requests sent to the three accountancy firms. The amount of the personal data disseminated enables the straightforward identification of the complainant. Moreover, the request for information sent to the three firms also contained details on the audit, which does not include personal data *per se*, but combined with the full name and EGN of the natural person enables the unmistakable identification of that person.

Dissemination of personal data is a form of personal data processing in accordance with the legal definition in paragraph 1 of the Supplementary Provisions (SP) to the LPPD. By disseminating the complainant's personal data for the purpose of collecting information about the usual fees for accounting services provided to legal entities (LEs) and sole traders (STs), both registered and not registered under the Value Added Tax Act, in the period 2009-2011, the TD NRA had breached the principle of proportionality laid down in Article 2(2)(2) LPPD.

On the grounds of Article 38(2) and Article 42(1) LPPD, the CPDP decided to impose an administrative penalty in the form of pecuniary sanction on the TD NRA amounting to BGN 21,000 (twenty-one thousand) on account of the fact that in its capacity of DC the TD NRA had processed the complainant's personal data in violation of Article 2(2)(2) LPPD.

5. After having married, a complainant had to change her family name, thus obtaining a new ID card. In order to change her name in its data base, the bank she is having a contract with bank asked the complainant to produce, besides the new ID card, a certificate of civil marriage, which the complainant believes to be a violation of her rights as per the LPPD's provisions.

The complainant was provided with a letter from the CPDP Chairperson regarding precautions against the usage of the financial system for money laundering, achieved by measures set out in the Law on the Measures Against Money Laundering (LMAML), which are binding for the obligated parties, namely the credit institutions.

It was explained that in pursuant Article 4(1) LMAML, when the banks, in the capacity of credit institutions, initiate business relations with their clients, they are required to

identify the clients by asking them to produce identity documents. In order to avoid identification errors, the LMAML provides an option for verification (cross-checking) against other documents (Article 3(1)(1) LMAML with regard to Article 1(2) of Rules on the Implementation of the LMAML, RILMAML). Article 9(2) of the LMA RILMAML provides that upon any change of circumstances related to their identification, natural persons are obligated to notify accordingly the persons referred to in Articles 3(2) and 3(3) of the LMAML, and produce the appropriate supporting documents.

It was indicated that in accordance with Article 3(1) with regard to Article 13(1) from the Law on Bulgarian Identity Documents, by the details shown thereon the identity card confirms the holder's identity and, where appropriate, citizenship. The identity card does not certify the change, if any, of the holder's names, because it shows only the holder's new name without the holder's old name, meaning that the change cannot be established from the identity card.

In the case at hand the change can be established from a certificate of civil marriage or a certificate of identity of names, could be provided by the relevant municipal administration.

The bank's internal rules for relations with clients are written in accordance with the LMAML and the RILMAML. The bank's internal rules establish that the details entered in the bank's data base are the type, date and number of the certificate of civil marriage, and these are not personal data in the meaning of the LPPD.

As the complainant had changed her name, the DC asked her produce appropriate documents in order to confirm that she is the same person as the one described on her identity card where her names were different. The bank had acted in accordance with the requirements of Article 2(2) LPPD since the documents it required for identification of the person undoubtedly contain personal data, however such data was required for concrete, clearly defined and legitimate purposes, i.e. the measures laid down in the LMAML.

6. A complainant referred the CPDP with allegations on unlawful processing of his data by a consumer cooperative.

The complaint indicated that each year the consumer cooperative sends out notices of annual meeting to its members, which include their personal identification numbers (EGN) and addresses, without placing them in envelopes, thus putting their personal data on display.

On the basis of the facts collected in relation to the complaint the CPDP found that the complaint is justified and imposed an administrative penalty in the form of pecuniary sanction on the consumer cooperative, which has the capacity of a DC, for violation of Article 23(1)

LPPD, namely failure to apply technical and organisational measures in order to protect the personal data against accidental or unauthorised access.

1.3. Comparative analysis of the inquiries received from citizens based on the type of the questions received

In 2014 the CPDP received many questions of diverse nature. Citizens have been actively seeking assistance and explanations in relation to the application of the LPPD. This is equally confirmed by the statistical analysis of the 374 answers given by the Commission.

The most frequently asked questions (FAQs) and the most interesting cases are reflected in the following analysis:

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

Most of the FAQs concern the lawfulness of the mandatory fields in the registration forms, whereby users are required to fill in their personal data such as full name, EGN and address. Following each particular inquiry the CPDP in the first place checks the online game operator in the eRALD system, provided however that the inquiry contains sufficient information about the operator.

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

If the *ex-officio* check in the eRALD system establishes that the operator is not registered as a DC or has not applied to the CPDP for registration in the eRALD system, the case is referred to the Commission's Legal Procedures and Supervision Directorate for them to take appropriate steps.

The CPDP also receives an increasing number of questions related to courier companies requiring EGN in relation to the sending or receiving of cash on delivery (CoD) consignments. The position of the CPDP on these cases is related to the reporting of these services in the books of account as a basis for admissibility of personal data processing. Article 7(1) of the Accounting Act defines the scope of information required for primary accounting documents. Article 7(1)(3) of the Accounting Act specifically provides that the primary accounting document 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 the natural persons who are not registered in the Commercial Register or in the BULSTAT register are identified by their EGNs if they are Bulgarian citizens or Foreigner ID Numbers if they are foreigners.

Continuing the trend from previous years, the most numerous questions in 2014 related to the transfer of personal data by various service providers (electricity suppliers, water and sewerage utilities, telecoms) to debt collection companies. Article 24(1) LPPD provides that DCs (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 DC and the data processing organisation are regulated by a regulatory act, by a written contract or by another act of the DC, which defines the scope of the obligations remitted by the DC to the data processing organisation. Another reason for the transfer of data from one DC to another DC can be the consent of the person which the personal data relates to. According to the LPPD, 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 natural persons give their consent for the transfer of personal data from one DC to another at the conclusion of service contracts.

The CPDP is often asked about the provision of personal data (full names and EGN) when amounts of cash are deposited at or drawn from banks. The client identification procedure is a mandatory one for banking institutions in accordance with the Law on the Measures Against Money Laundering (LMAML). The CPDP's case-law 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) LPPD, and the absence of this precondition does not prejudice the acts of the DC (the

bank). The reason is that simply one of the preconditions set out in points 1 to 7 of Article 4(1) LPPD 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), i.e. in fulfillment of obligations imposed on them by the law.

The citizens continue to question the right of shop cashiers to require shoppers to produce their ID card when they choose to pay a debit card. In reply to these questions, the CPDP informs the citizens that the so-called debit card is a payment card in the meaning of Article 25 of *Regulation No 3 of 16 July 2009 on the terms and conditions for the performance of payment transactions and for the usage 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 Regulation No 3, the merchant holding the POS terminal used for making the payment can reject the payment card if the holder fails to produce a document confirming his or her identity or if the merchant finds that the payment card is used by an unauthorised person.

A large group of questions in 2014 were related to video monitoring systems, which individuals are increasingly using in order to protect their properties. In these cases the CPDP considers that such video monitoring is processing of personal data for domestic and personal purposes in the meaning of Article 1(9) LPPD, meaning that such personal data processing does not fall within the scope of the LPPD.

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. According to Article 24(2)(6) of the Private Security Act (PSA), for each protected site the security service provider must draw up and maintain a site security plan, including a regime for accessing and leaving the site, which must be approved by the customer to the security services contract or by a person authorised by such customer. Points (a) and (b) of Article 30(1) PSA obligate the security staff 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 obligatory prescriptions 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 the 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 Law on Bulgarian Identity Documents, which clearly prohibits the giving or taking of an identity document for the purposes of securing the performance of an obligation (pledge), the usage of another person's Bulgarian identity document or the surrender of a Bulgarian identity document in the possession of another person.

2. Analysis of the case-law of the administrative courts

In 2014, the Administrative Court of Sofia City (ACSC) initiated 60 cases on appeals against administrative acts issued by the CPDP. The Supreme Administrative Court (SAC), in the capacity of appellate court, dealt with 37 cases.

During the reporting period (2014) the ACSC invalidated only one decision of the CPDP. The Court's reason for declaring the decision null and void was that the complainant party to the administrative case had withdrawn its complaint. In the case at hand, at the time of issuing its decision the CPDP had not been informed that the complainant had opted to withdraw the complaint. The request for withdrawal of the complaint was filed after the decision was issued and while the review of the appeal against the decision, submitted through the CPDP, was pending at the ACSC.

An analysis of the administrative case-law of the ACSC leads to the conclusion that when CPDP decisions are rescinded, the most frequent reasons are failure to comply with the administrative procedure rules and with the substantive provisions. Seen from the case-law, the breaches of the administrative procedure rules come in the form of failures to collect sufficient evidence for the administrative body to be able to clarify all facts and circumstances of relevance to the case. The non-conformities with the substantive rules as established by the ACSC boil down to whether the administrative body has correctly identified which provision of the LPPD has been breached. The Court's reason for modifying the level of the sanctions imposed by the CPDP is the absence of sufficient arguments for the imposition of sanctions above the minimum level set in the LPPD. It is held that the sanctions must contribute to achieving the educational, deterrent and dissuasive objectives of the punishment, rather than create economic difficulties for the DCs that had committed the violation.

It should be noted that when the courts rescind an administrative act of the CPDP, their judgments do not indicate whether the administrative case is remanded to the CPDP for a new examination. Such case-law creates uncertainty for the CPDP and renders the Commission unable to exercise its powers as per the LPPD, and thus imparts a defect in these

judgments. The only body in the Republic of Bulgaria, which is competent to decide whether or not there is a breach of the LPPD, is the CPDP. The Court is not competent to rule on the merits of the dispute. A rescission of a CPDP decision, combined with the lack of instructions as to whether the administrative case is remanded to the CPDP for a new examination, makes it impossible to solve the specific case, this in turn introduces instability in the relations between the DC and the natural persons which the data relates to, and accordingly destabilizes the protection of the individuals' rights.

IV. Statistics and analysis of the Commission's control and administrative-penal activities

1. Control activity

The procedure and methods for carrying out the overall control activity are governed by the provisions of the LPPD, the Rules on the activity of CPDP and its administration (RACPDPA), Regulation No 1 dated 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection (Regulation No 1), the Instruction on the control activities and other internal regulations.

The Commission exercises control in the following areas:

- Direct control on DCs in the public and in the private sector;
- Assisting data controllers with consultations and guidance on the compliance with the regulations, and on measures taken to protect the personal data processed;
- Ongoing assessment of DCs' work to ensure compliance with the legislation in the area of personal data protection;
- Establishment of violations and imposition of sanctions on the basis of and in accordance with the procedures set out in the LPPD and in the Law on Administrative Violations and Penalties (LAVP).

The controls laid down in Article 12 LPPD are exercised directly by the Chairperson and by the members of the Commission who are assisted by the specialised administration. According to Art. 26 of RACPDPA, the Legal Procedures and Supervision Directorate (LPSD) through its Control and Administrative-Penal Proceedings Department supports the Commission's control activity. This activity includes checks of data controllers to establish the facts and circumstances and collect evidence.

The purpose of these checks 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 extent to which the protection of the personal data processed is compliant with Ordinance No 1.

The control is exercised by carrying out ex-ante, current and ex-post checks as provided for in Article 12 LPPD. Each check ends with the issuance of a statement of findings (SFs) and in the event that an administrative violation of the provisions of LPPD is established, the Commission initiates administrative penal proceedings pursuant to the LAVP.

The total number of checks carried out in 2014 was 2340, including:

- 2242 ex-ante checks;
- 21 current checks;
- 77 ex-post checks.

It is seen from the above data that the largest number of checks were ex-ante checks pursuant to Article 12(2) LPPD. Two thousand three hundred and forty checks were completed in 2014 and resulted in the issuance of 2335 SFs and only of five statements establishing administrative violations (SEAVs).

The specific environments in which personal data is processed mean that there is a need to differentiate the checks by sector. In performing its activities in 2014, the CPDP carried out checks in the following sectors:

No	SECTOR	COUNT
1	Healthcare	1250
2	Commerce and services	256
3	Education and training	254
4	Legal and consultation services	122
5	Political entities	63
6	Building and architecture	45
7	Non-profit organisations	40
8	Manufacturing	36
9	Tourism	28
10	Financial and accounting security	27
11	Transport	25
12	Insurance	21
13	Sports activities	19
14	Social activities	18
15	Agriculture and forestry	15
16	Real estates	13

17	Financial sector	12
18	Central, regional and local authorities	10
19	Telecommunications, information technology and services	10
20	Repair and maintenance works	8
21	Human resources	7
22	Security and detective activities	7
23	Justice	6
24	Advertising and market surveys	5
25	Other	43

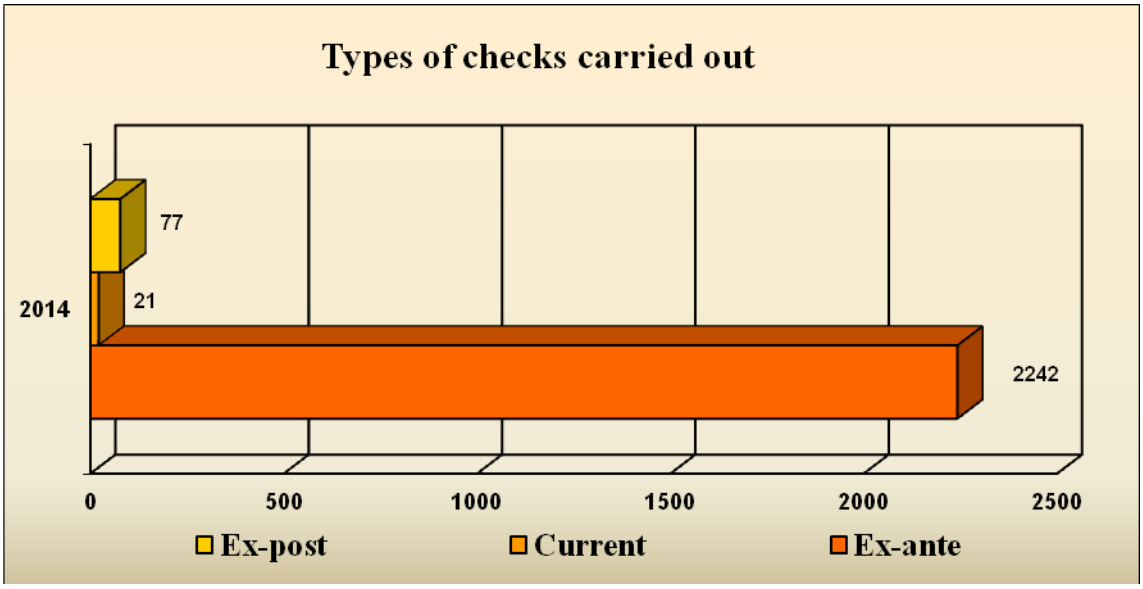

Fig. 6

1.1 Ex-ante checks

According to Article 17b LPPD, these checks are required prior to the DC is entered in the register under Article 10(1)(2) of LPPD in the cases where the data controller has declared processing of data subject to special protection as per Article 5(1) LPPD (related to health, sexual live or human genome, data revelling 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 checks aim to establish the technical and organisational measures undertaken in the context of personal data processing operation and the admissible type of

protection provided by data controllers and their compliance with the requirements of Regulation No 1.

2242 ex-ante checks were carried out in 2014 (Fig. 6).

All the ex-ante checks in 2014 ended with entry of the DCs in the register referred to in Article 10(1)(2) LPPD. The main problem with these checks, similar to previous years, has been communication with the DC for provision of the documents required to finalise the check. The most frequent difficulties include uncollected correspondence, change of address, inaccuracies in the applications submitted and failure of the DC to submit the required documents requested by a letter duly received by the DC. Due to the impossibility to finalise such checks, in 2014 the CPDP by its decision refused, on the basis of Article 17b(3)(3) LPPD, to enter in the register 293 DCs and the registers maintained by them. Following the publication of CPDP's decision, 25 DCs submitted the documents required to finalise the check and were accordingly entered in the register referred to in Article 10(1)(2) LPPD.

The same approach will be applied in respect of the checks which remained unfinished in 2014.

1.2. Current checks

Although the number of current check under Article 12(3) LPPD is much lower, these checks present larger legal complexity. Twenty-one current checks were carried out in 2014 (Fig. 6).

According to the LPPD these checks are carried out at the request of interested persons or at the initiative of the Commission on the basis of monthly control plans adopted by the Commission.

These checks ended in the issuance of five obligatory prescriptions and three SEAVs, while 13 checks did not detect violations of the LPPD provisions.

In the end of 2013, the CPDP adopted a "Plan for carrying out current checks at the initiative of CPDP in 2014" (the Plan). The Plan aims at enhancing the efficiency of the Commission's control activity through its further administrative strengthening, better organisation of the controls and improvement of the methods for providing guidance to DCs and other natural persons.

According to the Plan, DCs are selected for current (scheduled) checks on the basis of the following criteria:

1. DCs operating in structures and areas of priority for the CPDP:

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

- DCs the activity of which underwent significant structural changes resulting from a change in the law and the internal regulations, including newly established DCs;

2. Categories and volume of personal data processed by DCs:

- DCs processing personal data pursuant to Article 5(1) LPPD;
- DCs the activity of which threatens the rights and legal interests of natural persons;

3. DCs which have not been subject to scheduled checks;

4. DCs which have not submitted applications for registration/updates in the register under Article 10(1)(2) of LPPD.

5. DCs in administrative districts not covered by previous scheduled checks.

The main tasks of the scheduled checks are related to DCs' compliance with their obligations under the provisions of LPPD concerning the registration and update of DCs in the register referred to in Article 10(1)(2) LPPD and the obligations under Article 19(1), Article 23 and Article 25 of LPPD, and the establishment of technical and organisational measures to protect personal data. The checks mainly look at registers containing personal data of individuals, in particular DC personnel and clients (business partners) specific to their main activity (predominantly of nationwide scope) in the following areas: central government and institutions, the judiciary system, healthcare, education, banking and credit activities, insurance, commerce, services, etc.

In accordance with the criteria adopted in the Plan, the Commission appointed checks of 23 DCs operating in different sectors of the social and economic life.

DCs in the following sectors were checked:

- Central administration (4 checks): the State Agency for Child Protection, the Military Police service with the Minister of Defence, the State Agency for Technical Operations and the Financial Supervision Commission;
- Financial sector (3 checks): Direct Credit Bulgaria EOOD, Trace Expert EOOD and Credator OOD;
- Healthcare (2 checks): Regional Health Inspectorate Varna and Multi-profile Hospital for Acute Treatment Sta. Marina, Varna;
- Justice (2 checks): Regional Court Sliven and Administrative Court Sliven;
- Insurance (1 check): Insurance Company Lev Ins AD

The scheduled checks ended with the issuance of 12 statements of findings and two obligatory prescriptions .

In addition, three scheduled checks appointed in the end of 2013 were finalised in the beginning of 2014, namely the checks of Insurance Company Lev Ins AD, European Polytechnic University, Pernik and Regional Inspectorate for Education, Pernik. The findings from these checks led to the issuance of three obligatory prescriptions .

Since many CPDP staff were engaged in the fulfillment of the Commission's decision to carry out checks on political entities which submit documents to the Central Electoral Commission for participation in the elections of European Parliament Members, held in Bulgaria on 25 May 2014, the CPDP had to postpone the checks scheduled in August, September, October and November of 2014.

1.3 Ex-post checks

The third type of checks are those under Article 12(4) LPPD, namely ex-post checks carried out to verify compliance with CPDP's decisions or obligatory prescriptions as well as checks undertaken on CPDP's own initiative upon receipt of irregularity reports (alerts).

Seventy-seven ex-post checks were carried out in 2014 (Fig. 6). The methodology employed in these checks is similar to the one used for the current checks, as described above, the only difference being the legal basis on which they are carried out.

These checks ended with the issuance of 29 obligatory prescriptions and 36 statements establishing administrative violations, while 28 checks did not detect violations of the LPPD.

1.4. Examination of requests

Pursuant to Article 36(2) RACPDPA when a request does not contain details about violation of the applicant's right, action can be taken under Article 10(1) points 3, 5 and 6 and Article 43 LPPD. In 2014, the Commission examined 134 requests from individuals, including topical inquiries on personal data protection issues. The examination of such requests includes review of the relevant legislation, requesting the DCs concerned to provide written replies and/or opinions, prescription of certain measures, consultations, etc.

In the requests to the Commission for exercising its controlling power examined in 2014, most of the alleged violations of rights afforded by the LPPD were in the following sectors: Internet (59), healthcare (11), commerce and services (8), central administration (8), etc. Significantly less were the alleged violations in the following areas: justice, regional and local authorities, education and training, telecommunications, video monitoring, etc.

In 2014 the CPDP received an elevated number of alerts from natural persons concerning dissemination of personal data without their consent, including usage of such data for direct marketing, penetration in their accounts in the social networks and/or in their email accounts.

The examination of the requests led to the issuance of nine SEAVs and one binding instruction, while 14 requests were referred to other competent authorities such as the Communications Regulation Commission, the Consumer Protection Companies, the Prosecution Offices, etc. Appropriate replies were returned to the senders.

2. Administrative-penal activity

2.1 Obligatory prescriptions

Pursuant to Article 10(1)(5) LPPD and with regard to the control activity under Article 12(1) LPPD, the Commission issues obligatory prescriptions (OPs) to DCs regarding the protection of the personal data processed.

The BIs aim to afford adequate protection of the personal data in the relevant registers by maintaining the minimum scope of appropriate technical/organisational devices and protection measures as per the LPPD and the said Regulation No 1.

In 2014, obligatory prescriptions were issued to 38 DCs. Most of these were addressed to political entities in relation the elections for European Parliament Members held on 25 May 2014, to education and training organisations and to central administrations. Less BIs were issued to entities in the financial, commercial and services sectors.

The distribution of the BIs by type of the violation to be remedied is presented on the next chart (Fig. 7).

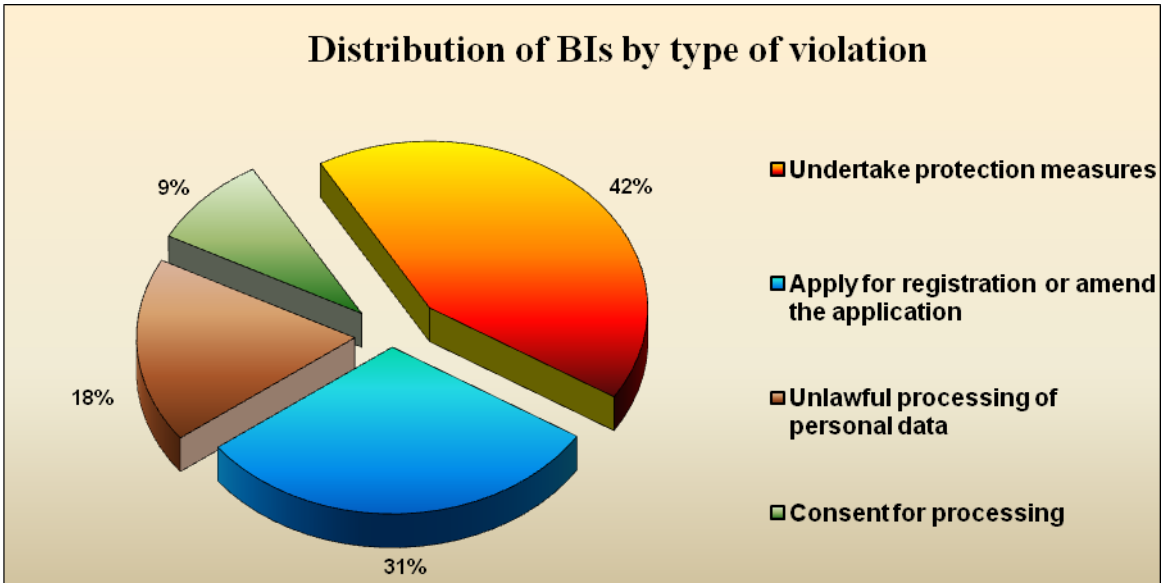

Fig. 7

The majority of the obligatory prescriptions were designed to remedy violations of Chapter Three of the LPPD, related to DCs obligations laid down in Article 17, Article 17b and Article 18(3) for registration and/or update of the registration in the register referred to in 10(1)(2) LPPD. The CPDP's check often come across DC failures to notify registers related to the processing of personal data of natural persons by installed video monitoring systems. According to an official opinion of the CPDP, videotaping and storage of information from video cameras is "processing of personal data" for the purposes of a separate "personal data register" in the meaning of paragraph 1(1)(2) of the Supplementary Provisions (SP) to the LPPD.

Other frequently encountered violations emerge from findings concerning the processing of copies of the identity documents of individuals when they enter into employment contracts or into civil service. Practice has shown the employers are increasingly making copies of their employees' identity documents (ID cards). When concluding an employment contract, each employer is required to comply with the requirements of Article 66(1) of the Labour Code and *Regulation No 4 of 1993 on the documents required for the conclusion of employment contracts*, which provides that at the conclusion of an employment contract the employee must produce a personal passport or ID card, which is used only for verification, whereupon it must be immediately returned to the holder. The said Regulation does not provide for the submission of an identity document copy at the time of applying for a job 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 *Regulation on the documents required for employment in civil service*. Therefore, the processing of personal data by retaining copies of natural persons' identity documents in their employment and office records when signing the employment contracts or respectively when creating an employment relation, is unlawful and any such practices are inconsistent with the principle set out in Article 2(2)(1) LPPD.

Bindings instructions were also issued in relation to assessments of the impact of the personal data registers processed by DCs with regard to the requirements laid down in the aforementioned Regulation No 1.

Last but not least, obligatory prescriptions were issued for application of specific measures to ensure the required level of personal data protection.

18 of the 38 BIs issued in 2014 were complied with within the time-limits set by the CPDP, while the other 20 BIs are under implementation.

2.2 Administrative-penal procedures

Article 43(4) LPPD provides that the establishment of violations and accordingly the issuance, appealing and enforcement of the penal decrees (PDs) are regulated by the Law on Administrative Violations and Penalties (LAVP).

Statements establishing administrative violations (SEAVs) of the LPPD provisions are issued by a Commission member or by officials authorised by the institution according to the requirements of Article 43(1) LPPD. PDs are issued by the Chairperson of the Commission in accordance with Article 43 (2) LPPD.

In exercising the controlling powers under Article 12(1) and Article 12(8) LPPD by carrying out checks on compliance with the personal data protection legislation, in 2014 the CPDP established 50 violations of various LPPD provisions and issued 48 SEAVs, on the basis of which the CPDP Chairperson issued 48 PDs.

Similar to previous years, in 2014 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 Article 43(4) LPPD. Sometimes the SEAVs are delivered to persons not having representative powers, in other cases the recipients do not sign the receipts, by which the DCs acknowledge that they are informed of their right to raise objections to the decision within three days, whereupon the documents are returned and another attempt to deliver them is made, and in other cases the written evidence accompanying the Commission's act cannot be delivered. Although not as a regular practice, the CPDP requests and receives assistance from the Ministry of Interior for detailed search and delivery of SEAVs and PDs to addressees in various part of the country.

One of the most frequent violations of the LPPD is the failure of data controllers to submit applications for registration at the CPDP before they begin any processing of personal data (Article 17(1) LPPD). Another violation, which has led to the issuance of many PDs, is DCs' failure to comply with the obligations imposed on them by Article 18(3) CPDP, namely to keep updated the originally supplied information about the personal data registers maintained by them.

The third most numerous group of PDs are those for non-compliance with Article 23(1) LPPD, i.e. failure 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 (6 PDs).

48 PDs were issued in 2014, including 9 PDs on SEAVs issued in the end of 2013. The total amount of penalties imposed by PDs is BGN 108,700. The amount of PD-imposed penalties collected in 2014 is BGN 99,438 (including BGN 30,188 collected coercively by the Natural Revenue Service).

Appeals against 21 PDs issued in 2014 are pending in courts. 8 PDs were not contested and the offenders paid a total of BGN 6,000 in penalties, all of them near the minimum level envisaged in the LPPD.

Once a PD enters validly into force, calls for voluntary payment are sent to the offenders on the basis of and in accordance with the Tax and Social Insurance Procedure Code. If the offender does not pay within the time appointed, the case is transferred to the National Revenue Agency (NRA). At present 21 PDs are being enforced by the NRA.

In 2014, the outcomes of the court cases initiated on appeals against PDs issued in previous years were as follows: 3 PDs were rescinded in their entirety and 16 PDs were confirmed, wherein in 4 cases the size of the penalty was reduced. At present, 30 appealed PDs are under judicial review.

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.

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 to higher courts.

Thus, for violations of Article 2(2)(3) LPPD, in respect of which the legislator provides the highest level of sanctions (from BGN 10,000 to BGN 100,000), in 2014 the court confirmed two PDs (by which pecuniary sanctions of BGN 15,000 and respectively BGN 11,000 were imposed), in one PD case the pecuniary sanction was reduced from BGN 20,000 to BGN 10,000 and one PD was rescinded in its entirety.

In one of the cases in which the PD was confirmed, the DC (Bulgarian Telecommunication Company EAD) was penalized for retaining, among other things, copy of the identity documents of persons who submit applications for portability of their telephone numbers, meaning that the personal data of individuals is processed in a scope exceeding the objectives of the number of the applications for portability and of the concluded contract. In the other case (Prophy Credit Bulgaria EOOD), when concluding employment contracts and

cooperation contracts with natural persons, the data controller retained copies of the identity documents of employees and contractors, however the data contained therein is not proportionate, relevant and limited to the objectives for which it is processed, meaning that there is breach of Article 2(2)(3) LPPD.

The Administrative Court of Razgrad explained its judgment to rescind a PD by which a data controller (Autobus Trans EOOD) was sanctioned by BGN 11,000 for a breach of Article 2(2)(3) LPPD in the form of retaining identity documents, by stating that the SEAV and the PD did not identify exactly the processing of which data contained in the identity documents was not proportionate, relevant and limited to objectives of the company's business. Accordingly the Court held that such imprecision had prejudiced the rights of the appellant and the appellant's ability to organise properly its defence.

In respect to a sanction imposed on a DC for violation of Article 17(1) LPPD, the Court held that for such a violation to be imputed to the data controller, there is a need to establish beyond doubt the exact date of occurrence of circumstances different from those that had led to the exemption of the DC from the registration obligation. It is exactly that date, argues the appellate court, on which the obligation for registration would have arisen. In the case at hand only the date of the check carried out by the CPDP was indicated, rather than the specific date on which the violation was committed.

One PD was rescinded as unlawful due to "incorrect qualification" of the committed violation. The data controller NSB-Engineering OOD was issued with a PD for violation of Article 17(1) LPPD, while in the Court's opinion the circumstances described in the SEAV and in the PD are consistent with a violation of Article 17(3) LPPD.

All court judgments and especially their reasons have been analysed in depth with a view to integrating them in the lawful performance of the control activities, but first and foremost with a view to resolving existing weaknesses and omissions in the establishment of LPPD violations and to ensuring that they are properly documented in accordance with the LAVP. 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.

V. Control on political entities

The new Electoral Code adopted in March 2014 provided to all voters the opportunity to check in the website of the Central Electoral Commission (CEC) the lists containing the names, personal identification numbers (EGN) and handwritten signatures of voters who support the electoral registration of political entities. As a result, during the reporting period the CPDP received hundreds of complaints and alerts over abuse of personal data during the registration of political entities for the election of European Parliament Members from the Republic of Bulgaria (MEP elections), which were held on 25 May 2014.

In this connection, the CPDP promptly initiated and held a working meeting with the CEC. The objective was to improve data security levels and prevent unauthorised access to the data. The CPDP issued a binding instruction and the CEC introduced additional protection measures to ensure a higher level of personal data protection. The CPDP verified the compliance with the BI by carrying out an ex-post check on the CEC in the capacity of DC.

In the meantime 1380 complaints and alerts in which citizens asserted that their personal data appeared without their consent in subscription lists of political entities were either sent directly to the CPDP or referred to the Commission by the CEC and the Prosecution Office.

1. Checks (methodology used for the checks, activities performed in the context of the checks and associated results)

In the context of its supervisory work, in parallel with the administrative procedures on the complaints received, the CPDP took a decision to carry out checks on all political entities that submitted to the CEC documents for registration in the MEP elections held on 25 May 2014.

In order to carry out these checks, the CPDP set up four teams led by the CPDP members Tzanko Tzolov, Tsvetelin Sofroniev, Mariya Mateva and Veselin Tselkov. For the purposes of these checks, by its decision the CPDP adopted a methodology laying down rules on how to practically carry out the tasks associated with the controls on all political entities that had applied for registration in the MEP elections of 25 May 2014. The methodology aims to lay down common criteria, approaches and modalities for the checks and controls as well as to define the scope of the associated rights, obligations and responsibilities. It sets out all

the activities that the teams have to carry out during the checks. Furthermore, the experts participating in the checks received additional training during the reporting period. Lawyers and IT experts were part of all teams. CPDP-approved questionnaire and checklist were also part of the toolbox used for the checks.

In addition to the facts and circumstances related to the specific complaints and alerts lodged against the various political entities, the CPDP also checked how the parties and the initiative committees collect, reprocess and destroy personal data in relation to the elections. Another objective of the checks was to verify whether the personal data of other individuals involved in the functioning the political parties as legal entities, including subscription activists, champions and supporters of political parties, counterparties to employment and outsourcing contracts, donors and contractual partners, was processed in accordance with the LPPD.

To ensure transparency and publicity of information, the CPDP invited observers from the non-government organisations (NGO) represented at CEC's Public Council as well as other organisations involved in the protection of civil rights and in the monitoring of institutions. The observers were familiarised with their rights and with the methodology to be used for the checks. To this end they signed non-disclosure agreements (NDAs) and received special certificates legitimizing them during the checks. Representatives of the Institute for Public Environment Development, the Bulgarian Institute for Legal Initiatives and the Institute for Modern Politics Foundation joined part of the checks selected at their discretion.

Between 2 July and 25 July 2014 the teams checked 54 political entities (44 parties and 10 initiative committees). The main objective of the CPDP was to prevent possible misuse of the personal data of citizens participating in subscription lists and to verify whether the political entities comply with the LPPD. The methods used for the checks were completion of questionnaires, interviews and inspection of personal data registers in the various security aspects.

The checks carried out revealed that 13 political entities are compliant with the personal data protection requirements. To address various irregularities in fulfillment of the LPPD requirements, the CPDP issued 23 obligatory prescriptions to 24 political parties and initiative committees, in the capacity of DCs, giving them not more than 1 month to rectify the irregularities. 32 SEAVs were issued to political entities for these irregularities/violations.

The largest number of violations were found in respect to Chapter Three of the LPPD, namely failure of political entities to comply with the obligations laid down in Article 17 and in Article 18(3) for registration in the register referred to in Article 10(1)(2) LPPD before they

start any processing of personal data and/or failure to update the entries in the register upon any change of the circumstances stated in the initial application for registration.

14 SEAVs were issued for violations of Article 17(1) LPPD and 18 SEAVs for violations of Article 18(3) LPPD. The violations boil down to the fact that the political entities concerned either did not file any application for registration at all or did file an application, but did not notify a register related to the processing of personal data of signatories to subscription lists supporting the registration of the political entity for the elections, for the purposes of their registration as per the Electoral Code.

13 political entities were issued with BIs to notify registers related to the processing of personal data of other categories of individuals such as contractors, video monitoring operations, etc.

Nine political entities were issued with BIs to perform mandatory assessment of the impact of the personal data registers maintained by them, i.e. to perform an ex-ante assessment of the potential risks and dangers that may affect the personal data processed by them, in order to undertake adequate technical and organisational measures for the protection of such data. The obligatory prescriptions were linked to the requirements of *Regulation No 1 dated 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection (Ordinance No 1).*

Six political entities were instructed to discontinue the practice of taking and retaining copies of the identity documents of natural persons at the conclusion of employment contracts.

It was found during the checks that five political entities continue to keep copies of the subscription lists and they accordingly issued with BIs to destroy these lists and provide appropriate evidence of destruction.

To address violations of Article 19 LPPD, three political entities were instructed to furnish the candidate members of the relevant party with written information, which identifies the data controller and its representative as well as the purposes for which the candidate member's personal data is processed in the context of the candidacy process.

One political entity refused to cooperate with the checking team, as is required by Article 22 LPPD, and was issued with a SEAV.

Of the 23 BIs issued, nine were fulfilled within the time-limits set by the CPDP and work is ongoing to fulfill the remaining ones.

By the date of this report, 26 penal decrees (PDs) have been issued on the basis of the 32 SEAVs.

The CPDP Chairperson issued written instructions, on the grounds of LPPD 34(3) and Article 54 LAVP, for discontinuation of two administrative-penal procedures (APPs) against initiative committees set up in accordance with the Law on the Direct Participation of Citizens in Central and Local Governance (LDPCCLG) and the Electoral Code. The LDPCCLG and the Electoral Code provide that initiative committees are formed for a specific purpose and function for a certain period of time, which is fixed in the relevant law. Having regard to the circumstances and to the fact the committees had been dissolved, the administrative-penal body discontinued the APPs due to the absence of addressee of the potential PD.

Twelve of the delivered PDs are presently under appeal.

2. Examination of complaints under Article 38 LPPD

This is how the CPDP acted on the 1380 complaints and alerts against political entities received in 2014:

The received complaints were grouped by political entities for the purposes of the administrative procedures under the LPPD and the Administrative Procedure Code (APC). The CPDP requested and received from the CEC evidence confirming that the personal data of the complainants indeed appears in the relevant lists of voters supporting the registration of political parties and coalitions of political parties.

An analysis of the complaints revealed that more than two-thirds of the complaints do not contain information required to identify the submitter of the complaint or the alert. Despite the steps undertaken to resolve these deficiencies, not all citizens provided their EGN or address, while others did not sign the complaints/alerts sent to various institutions.

It turned out that as little as 496 of the 1380 complaints and alerts were eligible for examination and search of evidence by the CPDP. All of them were examined in public hearings during the reporting period.

During the examination of the complaints the CPDP decided to obtain forensic verification of the signatures of the natural persons appearing in the relevant lists of voters supporting the registration of parties and coalitions for participation in the elections. For this purpose, the Ministry of Interior (MoI) was requested to perform graphological assessments. By the end of the reporting period 156 citizens had provided the required graphological specimens. The results from four regional MoI directorates are expected. The specimens received are being grouped by parties and provided in batches to the Research Institute of Criminology and Forensics (NIKK) for them to perform the assessments requested by the CPDP.

As of the end of the reporting period these procedures were still pending and the CPDP will be taking its decisions once it receives the assessment reports from the NIKK.

The CPDP acted in a similar manner on the 53 complaints over alleged misuse of personal data during the registration of political entities for the national parliamentary elections held on 5 October 2014.

3. Analysis and recommendations

On the basis of the checks carried out on political entities and with a view to establishing an LPPD-compliant case-law in the area of personal data processing by this type DCs in relation to elections held under the Electoral Code, the CPDP identified the following weaknesses and omissions in the functioning of political entities as data processors:

1. Non-compliance with the obligation for initial registration with the CPDP;

2. Non-compliance with the obligation to notify new personal data registers to the CPDP;

3. Failure to produce or update personal data protection manuals in accordance with the new Regulation No 1 of 30 January 2013;

4. Retention of copies of documents containing personal data, such as subscription lists, ID cards, etc.

In the course of its checks the CPDP identified the following factors that facilitate misuse of personal data electoral context:

1. In the case of coalitions of political parties, it is not possible to identify the exact political party, which signed up supporters of the coalition;

2. It is not possible to identify the exact representative of the political party who witnessed the affixing of the signatures.

On the basis of its checks related to elections held under the Electoral Code, the CPDP issues the following recommendations to the entities involved in the electoral process:

Recommendations addressed to political parties, initiative committees and registered observers of the elections:

- All parties and initiative committees, which nominate candidates for national MPs, President and Vice-President of Bulgaria, Members of the European Parliament, municipal councillors and mayors, and which register themselves in the CEC or in the relevant Regional or Municipal Electoral Commissions (REC/MEC), are DCs and as such they are liable to DC registration with the CPDP.

- Coalitions of political parties are not DCs. However, the parties which take part in elections held under the Electoral Code in a coalition with other parties are DCs in the meaning of the LPPD and as such they are liable to mandatory registration.

- All political entities that have the capacity of DCs should notify in the register referred to in Article 10(1)(2) LPPD a register related to the processing of personal data of individuals that subscribe to lists for the registration of the political entity in elections held under the Electoral Code, or in referenda, and should introduce exact and clear rules and procedures for the collection and storage of subscription lists, including rules for clear identification, access to the data, corrections of the personal data collected, storage periods and destruction methods.

- All parties and initiative committees should ensure that the information in the register referred to in Article 10 (1)(2) LPPD is kept up-to-date. These political entities should notify beforehand the personal data registers which they process for the various categories of natural persons. All changes of the circumstances described in the initial registration should also be notified.

- All parties and initiative committees should perform an assessment of the impact of the personal data registers maintained by them, i.e. an ex-ante assessment of the potential risks and dangers that may affect the personal data processed by them, in order to undertake adequate technical and organisational measures for the protection of such data. The CPDP has adopted Ordinance No 1 on the minimum protection measures, which the DCs should comply with and apply.

- The members of initiative committees are DCs, however by its Protocol Decision No 32 of 13 August 2014 the CPDP has exempted them from the registration obligation.

- Registered NGO observers of parliamentary elections are also DCs in the meaning of the LPPD and as such they are liable to registration as per Article 10(1)(2) LPPD. They should notify a register related to the processing the personal data of the individual observers.

Recommendations addressed to citizens:

- Citizens that sign up to subscription lists supporting the registration of political parties and initiative committees in elections falling within the scope of the Electoral Code should actively exercise their rights, including that they should require from the political entities information about the purposes for which their personal data is processed (collected, stored and transferred) as well as details about the deletion of the collected data and the correction of incorrect data. Citizens should address their requests for deletion or correction of personal data directly to the parties or the initiative committees, as the case may be.

- If they come across violations of their individual rights, voters should send their complaints and alerts directly to the CPDP to help expedite the Commission's procedures. A complaint form with the required particulars is available from the CPDP website (www.cpdp.bg).

- The law also enables citizens seek redress in court or report any suspected crimes to the relevant prosecution office.

Recommendations addressed to the CEC:

- The CEC should take steps to identify which are the exact parties within political coalitions that raise subscription lists on behalf of their coalitions, because these parties have the capacity of DCs.

- The CEC should demand from political entities evidence of the current status of their DC registrations with the CPDP as of the date on which the election date is fixed, but in any case not later than the date by which the subscription lists are submitted to the CEC for registration in the elections.

- In respect to elections for national MPs and of municipal councillors/mayors, the CEC should instruct the regional/municipal electoral commissions (REC/MEC) demand from local initiative committees evidence of the current status of their DC registration at the time of their registration for the elections.

Throughout its work on the complaints received and during its checks of political entities, the CPDP received assistance from the CEC, the Prosecution Office of the Republic of Bulgaria, the political parties checked, NGOs and mass media that report the activity of the CPDP and thus contribute to achieving transparency and public awareness.

The CPDP is opened for future joint initiatives with all stakeholders in order to perform in-depth analysis, including proposals for improvement of the electoral legislation.

4. Conclusions

The positive impact of the measures undertaken by the CPDP to forestall the misuse of personal data in signing up supporters of the registration of political entities for the two elections can be seen from the different numbers of complaints and alerts received by the CPDP before and after the checks:

- 1380 complaints and alerts were received during the MEP elections held on 25 May 2014;

- 53 complaints were received during the national parliamentary elections held on 5 October 2014.

Of note is the significant decrease of improperly submitted complaints and alerts after the CPDP published a model complaint on its website. This standardized approach allows the affected individual to seek efficient protection of his/her right and also makes it easier for the CPDP to verify the facts and circumstances stated in the complaint.

CPDP's understanding is that the focus should be placed on raising individuals' awareness of their rights and obligations under the Electoral Code and on the compliant behaviour of those responsible for signing up supporters in order to avoid use of personal data in ways that are inconsistent with the LPPD.

Another notable observation is that following the checks on political entities participating in the MEP elections, in the end of the reporting period 90% of the political entities eliminated the violations for which they were sanctioned by the CPDP. These violations were in the form of failure to submit an application for registration with the CPDP and/or notify a register related to the processing of personal data of individuals signed up to subscription lists. The 10% that have not yet resolved the violations will be subject to ex-post checks in 2015 (Fig. 7 and 8).

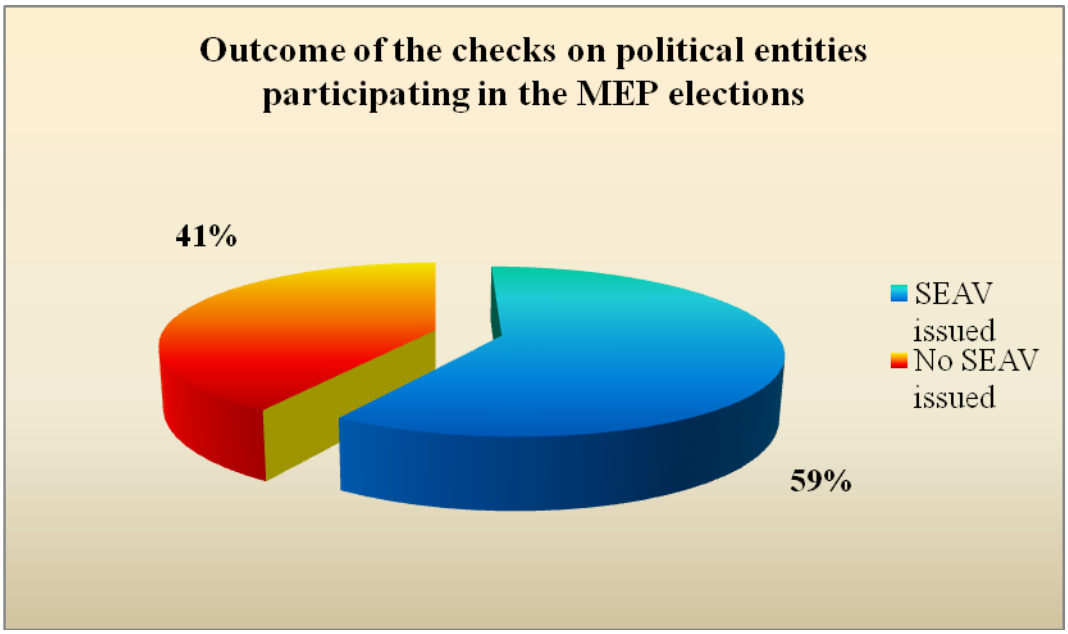

Fig. 8

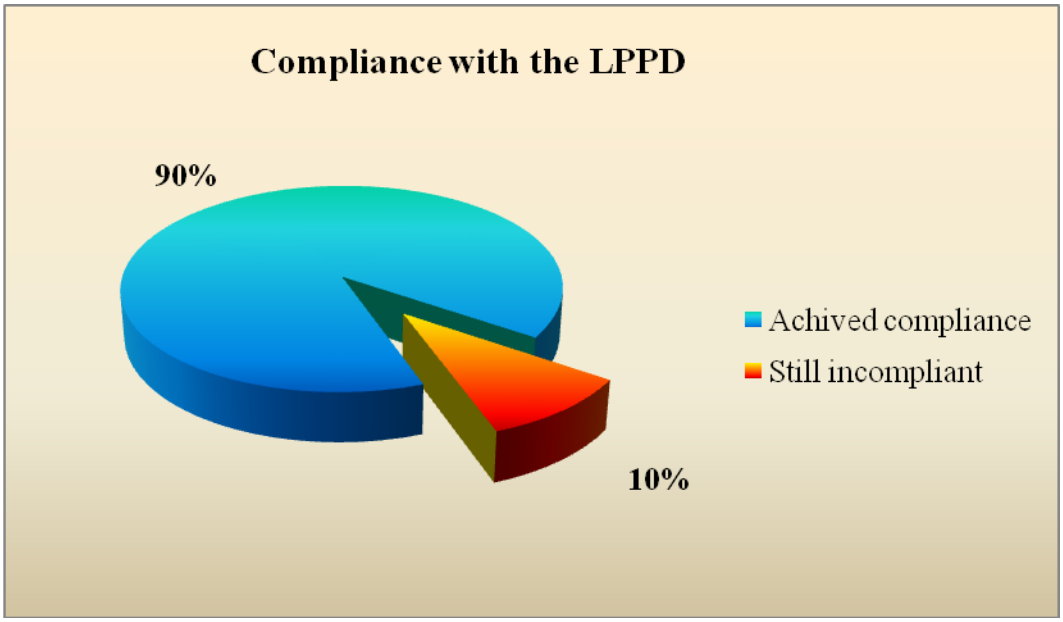

Fig. 9

On another positive note, the checks have also led to a high rate (90%) of political entities that obtained registration as data controllers for the national parliamentary elections in October 2014 (Fig. 10).

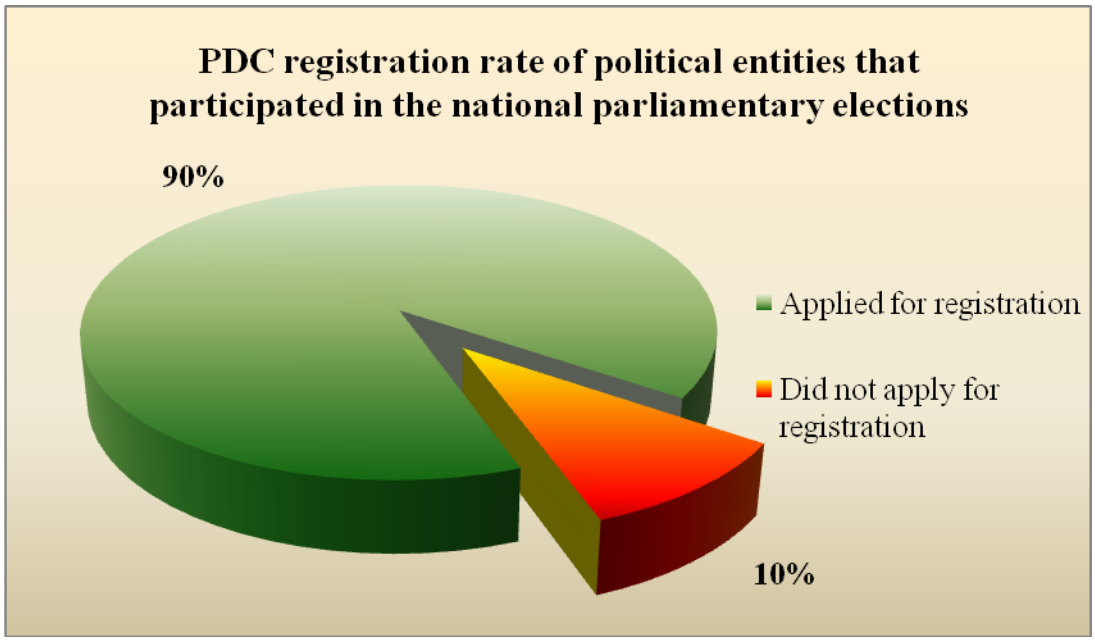

Fig. 10

Having analysed the identified loopholes for misuse of personal data in the course of the election process, the CPDP deems that legislative changes are needed along the following lines:

1. Introduce arrangements that enable the exact identification of the political party which signs up citizens in a subscription list, when the party is part of a coalition. At present, the absence of such arrangements impedes the enforcement of administrative-penal liability on the political party acting as a DC when the party is part of a coalition.

2. Ensure that the activists that sign up citizens in the field can be identified. In addition to the disciplinary effect on the political entity, this measure will also create guarantees against misuse by activists.

3. A DC registration in the register kept by the CPDP, including notification of a register of personal data of voters that support the electoral registration of a political entity, should be a precondition for the electoral registration of that political entity.

4. In the case of initiative committees, define which member of the initiative committee bears responsibility as a DC. At present the Electoral Code creates a fictitious situation where initiative committees are considered as DCs, however these DCs are not personified and they vanish after the election (an initiative committees exists only for a limited period of time, i.e. until the registration of the independent candidate nominated by the committee), which leaves little scope for the CPDP to enforce administrative-penal liability in the context of checks and examination of complaints.

5. A DC registration in the register kept by the CPDP, including the notification of a register related to the processing of the observers' personal data, should be a mandatory condition for the registration/admission of NGOs as observers of the elections.

VI. Official opinions and permissions for the transfer of data to third countries

1. Opinions

In 2014 the CPDP responded to 80 requests by issuing official opinions pursuant to Article 10(1)(4) LPPD. The present report presents a summary of the opinions delivered on issues of major concern to the broad public or on cases frequently encountered in practice.

Requests for opinion from municipal administrations in the capacity of DCs maintaining civil records at local level

Municipal mayors request CPDP's opinion about cases where banks ask municipal administrations to provide information about the heirs of deceased debtors. The in-principle opinion of the CPDP in this case is the following: On the basis of Article 4(1)(7) LPPD (processing is required to serve legitimate interests of the DC or of a third person, to whom the data is disclosed), with regard to Article 106(1)(3) of the Law on Civil Registration (data from the civil register (GD GRAO) is provided to Bulgarian legal entities on the basis of a CPDP decision), municipal administrations can provide information from their registers concerning the heirs of deceased persons, so that the banks can lodge claims to these heirs pursuant to Article 124(2) of the Civil Procedure Code (CPC). For this purpose the bank needs to provide evidence and details confirming that there has been a contractual relation between it and the deceased person, and the existence of a valid and due liability amounting to the disputed sum of money. If the persons whose data is requested are also deceased, then the administrations should provide details about family members which come next in the order of succession of the deceased person.

Municipal administrations also ask the CPDP about the disclosure of personal data requested by various insurance companies. The documents that insurers request from municipalities are certified copies of death notifications or death certificates. The insurers base these requests on Article 106(1)(2) of the Insurance Code. On the basis of the existing legal framework in the Republic of Bulgaria, the CPDP holds that such personal data (notification or certificate of an individual's death) from Local Databases "Population" kept at local level by municipal administrations can be provided on the basis of Article 4(1) points 1 and 6 of the LPPD and Article 28(1)(8) of the Health Act with regard to Article 106 of the Insurance Code and *Ordinance No RD-02-20-6 of 24 April 2012 on the issuance of*

certificates on the basis of population registers, for the purpose of certification of an insured event and the damages caused by the event.

The CPDP is often asked to provide guidance in respect to the increasing number of requests from owners/co-owners of residential properties for the personal data (names, EGN) of persons who have registered residence addresses in their properties and have made these registrations before Article 92 of the Law on Civil Registration (LCR) was changed on 20 May 2011, i.e. under the previous registration regime. The question in these cases is to what extent Article 106(1)(1) of the LCR can be relied on as a basis for the disclosure of personal data to third parties and what evidence should property owners present in proving legitimate interest, so that the data can be lawfully provided. The opinion of the CPDP is that on the basis of Article 4(1)(1) LPPD with regard to Article 106(1)(1) LCR, the municipalities can provide to property owners information about the persons that have registered residential addresses at their property upon production of evidence confirming that the requester is the owner of the property concerned (such as title deeds or court rulings by which provisional property purchase contracts are declared to be final contracts as per Article 19 of the Obligations and Contracts Acts (COA), etc.).

Various municipal administrations often approach the CPDP on the matter of whether individuals' personal data can be provided to the Road Infrastructure Agency for the purposes of land acquisition procedures under the State Property Act (SPA). In its opinions the CPDP holds that municipal administrations can provide to the Road Infrastructure Agency personal data (full name, EGN, permanent address, familial relation with the predecessor) of the property owners or the heirs of deceased owner, from the Local Database "Population" kept at local level by the relevant municipality, on the basis of Article 4(1) points 5 and 6 with regard to Article 106(1)(2) LCR.

In 2014 the CPDP was also asked by the Mayor of Omurtag Municipality about the procedure, modalities and conditions, and the permissible scope of information and possibly personal data that can be exchanged between Omurtag Municipality and the City of Munich, Federal Republic of Germany in relation to upcoming conclusion of a tripartite Memorandum of Understanding between Omurtag Municipality, Pazardhik Municipality and the City of Munich. The overall objective of the MoU is to explain and protect the rights of the Roma populations from the two Bulgarian municipalities that reside permanently and/or temporarily in Munich, and facilitate the integration of these populations in both countries by collaboration among central/local authorities and NGOs. The CPDP held that for the processing/disclosure of personal data to be lawful, it should meet at least one of

the alternative criteria in Article 4(1) LPPD with regard to Article 106 LCR, and should be carried out in strict compliance with the principles of appropriateness, proportionality and up-to-date validity of the data. It is for the DC that provides the data to decide whether the lawfulness criteria are met on case-to-case basis if a need for such disclosure arises. All obligations and responsibilities related to deciding the format and method by which the requested information will be sent as well as the technical and organisational measures to maintain the security of the shared information entirely rest on the DC that provides the data.

Both central and local administrations are increasingly deploying various e-administration services. The provisions of such services to citizens raises a few questions about the applicability of the LPPD. For example, in the past year the CPDP received requests for opinions from Sofia Municipality and from the Bulgarian Food Safety Agency related to EU-funded projects, the final aim of which is to expand the scope of administrative services to be offered to citizens. The two institutions wish to receive a permission to access the "Population" register of the National Database "Population" (NDB "Population") in order to check the identity of applicants who submit electronic applications for using the relevant e-administration services. On the grounds of Article 4(1)(1) LPPD with regard to Article 106(1)(2) LCR, the Chief Directorate of Civil Registration and Administrative Services (GD GRAO) at the Ministry of Regional Development should provide free of charge automated access to the "Population" register of NDB "Population". However, in its opinion the CPDP held that such access should be limited to the categories of data necessary for the purposes of the particular services. Since in these two similar cases the automated data exchange function will be using a software infrastructure maintained by the Ministry of Transport Information Technology and Communications (MTITC), the projects in question should be implemented on the basis of tripartite agreements with GD GRAO and the MTITC.

Each time when the CPDP expresses an opinion related to the provision of electronic services, the Commission stresses on the importance of the information about the processing of personal data, which the DC concerned should provide to the users in accordance with the LPPD.

An interesting query came from **a bank, which was requested by an insurance company to provide names and EGNs of certain clients of the bank**. When an insurer pays insurance claims, in the payment orders the insurer specifies the IBAN of the beneficiary's account to which the compensation should be transferred. In accordance with the Law on Payment Services and Payment Systems, the bank must execute the payment exactly to the IBAN specified in the payment order. In executing the payments the banks are not required to

check whether the IBAN matches the name of the account holder. If the IBAN is valid, but the account belongs to a person other than the intended recipient, the bank will nevertheless execute the transfer, whereupon the funds will be credited to the account identified by the unique identifier (IBAN) specified in the order.

The bank explained that this is what happened in the case at hand and because of the wrong IBAN specified in the payment order the funds ordered by the insurer were credited to other clients of the bank, who were not the intended recipients. As a result, these third persons have obtained undue gains in the form of payments they were not entitled to. The CPDP was asked to provide guidance as to whether the bank has a lawful reason to provide the personal data requested by the insurer, namely full names and EGNs of the account holders to whose accounts the fund were wrongly credited, in order to enable the insurer protect its legitimate interests by court action for undue gains against the individuals whose personal data the insurer had requested.

The opinion of the CPDP is that personal data (full names and EGN) of bank clients whose accounts are credited with funds ordered by an insurance company because of wrong IBAN specified in the payment order can be provided on the basis of Article 4(1)(7) LPPD with regard to Article 55 OCA (undue gains acquired by certain persons), in order to enable the insurance company initiate court action.

In 2014 the CPDP also delivered an opinion regarding voice recording of incoming calls to a call centre. Adhering to the basic personal data processing principles, the CPDP reiterated that in these cases the individual's consent must be expressed explicitly rather than inferred from circumstantial acts. The call centre should also offer non-recordable calls to the callers. The associated information should be provided by a warning message before the actual call. According to the Commission's conclusions it is not acceptable to announce the terms of the conversations between users and the call centre only in the general terms of business of the relevant company and on the company's official website. The call centre should in each case provide to the caller an opportunity to object to the processing of his/her personal data by recording the telephone conversation, after the centre informs the caller of this option in each call.

Another interesting CPDP opinion relates to situations where a money lending company is unable to contact a defaulting debtor by telephone or letter. The question in this case is whether it is appropriate to post notices on the entrance door of the debtor's property (home) reading that the debtor has outstanding payments under a loan agreement or simply that a representative of the lender has tried to visit the debtor.

The opinion of the CPDP is that the public announcement of the liabilities of debtor, when they are natural persons, by posting notices on the entrance door of the debtor's home or on the debtor's post box, amounts to a violation of Article 2(2) LPPD if it contains either of the following sets of information:

- The debtor's first and family name, notice of delayed payments and contact phone of the lending company;
- Identification number of the debtor's apartment, notice of delayed payments (including their exact amount) and contact phone of the lending company;
- Identification number of the debtor's apartment, notice of delayed payments (without mention of their exact amount) and contact phone of the lending company.

Another noteworthy opinion of the CPDP is about a study project aiming to find out how foreigners who have acquired or reinstated Bulgarian citizenship by virtue of a Vice Presidential Decree have contributed to the national economy or to other specific areas. The request for opinion came as the Office of the Vice President of Bulgaria launched a project, one module of which aims to find out how foreign nationals who have acquired or reinstated Bulgarian citizenship by decree of the Vice President have contributed to the national economy or to other specific areas related mainly to their residence or employment in Bulgaria. For the purpose of such study it was necessary to use information involving personal data of the said group of natural persons as well as to send such information for reference to other state institutions, which are also DCs. In this context, the Vice President's Office asked the CPDP whether it would be appropriate for other DCs to receive information about the individuals included in the study and can such information be provided to other institutions for achieving the objectives of the project, subject to the terms of Article 4(1)(5) LPPD (existence of public interest).

After an analysis of the case the CPDP held that personal data can be processed within the framework of the project mentioned above on the grounds of Article 4(1)(2) LPPD provided that the persons whose data will be processed give their informed consent. An important requirement for the validity of such consent is that it must be given before the processing for the purposes of the project has begun. The institutions involved in the project should provide a choice to the persons who obtain or reinstate Bulgarian citizenship, by informing them beforehand about the project objectives, the categories of data to be processed, the persons who will have access to the personal data processed and the processing arrangements. In this specific case, if the new or reinstated Bulgarian citizen refuses to give

informed consent, the institutions from which information is requested can only provide data in the form of statistical information after de-personification of the personal data.

In 2014 the CPDP also delivered an opinion in relation to a public discussion on the topic "Is there a need to change the access to information legislation", hosted by Foundation "Access to Information Programme". One discussion topic was the eventual setting up of an independent body with a mandate to supervise the application of the Access to Public Information Act (APIA), wherein one of the proposed options was to collocate the data protection and access to information functions at the CPDP. The Commission's position on this issue is that the CPDP is an independent body created to serve a specific objective, namely to afford institutional protection to persons whose right to privacy has been breached in violation of the personal data processing principles. The two constitutional rights – to access to information and privacy, along with personal data, exist in a conflict, that have to find its balanced resolution on case-to case basis. Vesting the CPDP in powers to examine complaints lodged both under the LPPD and the APIA would impart a serious bias in the resolution of disputes, only to the prejudice of those who seek fair remedy of their breached right. The CPDP deems that the existing Bulgarian legislation has indeed set up an independent institution in the face of the National Ombudsman, who has sufficient regulatory mechanisms to effectively enforce the protection of Bulgarian citizens whose APIA rights are breached.

Following the amendments to the Public Procurement Act (PPA), published in State Gazette No 40 of 13 May 2014, during the reporting period the CPDP was asked on multiple occasions to provide guidance concerning the deletion of data in accordance with the requirement set in Article 22b(3) PPA. The position of the CPDP is that the said Article 22b(3) PPA clearly defines the cases in which information from the published profile of the buyer is to be deleted. Such information should only be deleted in the Article 22b(3) cases, namely when a declaration of confidentiality as per Article 33(4) PPA is submitted and when the information is protected by law. Information regarding natural persons is protected by law, namely by the LPPD, because it is personal information about the individual. Details such as EGN, ID card number, permanent or current address, which identifies the individual in the documents referred to in Article 22b(2) PPA, should be published only with the individual's consent in the meaning of § 13(1) SP LPPD. Such consent must be willingly expressed, specific and informed and in it the individual should unequivocally agree to the processing of the data. That said, although the LPPD does not explicitly require a written

consent, the consent should preferably be expressed in a written document for there to be solid proof of the existence of such consent.

The publication of the documents referred to in Article 22b(1), one of which is CPDP's record of a public procurement procedure, aims to achieve publicity and transparency. Since the personal data of a certain category of persons is shown in the records referred to in Article 22b(1)(7) PPA because such persons are employees or consultants involved in a public procurement procedure, the names of these persons have to be published in order to achieve the objective of the public procurement register, which is to ensure publicity and transparency of the assignment and implementation of public contracts. Furthermore, according to Article 72 PPA this data is an integral part of the records of the committees appointed to examine, assess and rank the tender offers. As concerns the personal signatures, the CPDP reiterates its position that their publication is disproportionate to the objective of the law, since the publication of the content of the record and the names of the above-mentioned categories of individuals is sufficient for achieving the publicity and transparency objectives.

On motion of the CPDP member Mr. Tsvetelin Sofroniev, in 2014 the CPDP discussed an issue related with the use of personal identification numbers (EGN) in the documents most widely used in the national education system: pupil ID card, pupil credit booklet and off-campus pupil credit booklet. These documents, being part of the mandatory requirements as per the *Peoples' Education Act*, are kept by every pupil in the national education system, therefore the range of affected individuals is very large.

The CPDP performed a detailed analysis of the legislation in force. Since the documents in question are used and kept by children, the Commission also examined certain specific provisions related to the status and to the protection of children as well as the international standards related to this specific category of personal data subjects.

It was found that the use of EGN in the templates of pupil ID cards, pupil credit booklets and off-campus pupil credit booklets breaches some fundamental personal data processing principles:

- The use of the EGN is irrelevant to the objectives for which these documents are created;
- The principles of reducing the data processing to the minimum required for the achievement of the objectives set;
- The principle of proportionality is breached, while the safety of the children in terms of their personal data is not guaranteed to a sufficient extent.

The legal analysis demonstrated that *Regulation No 4 of 2003 on the documents in the national education system*, which determines the content of the above documents, is inconsistent with the LPPD, the latter being an act of higher hierarchy as per Article 15 of the *Law on Legislative Acts*.

Having regard to the foregoing, the CPDP held that use of the EGN as part of the mandatory content of the pupil ID card, pupil credit booklet and off-campus pupil credit booklet in the meaning of Article 65-67 of *Regulation 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. The CPDP issued an obligatory prescription (OP) in the meaning of Article 10(1)(5) LPPD, 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 EGN from the content of pupil ID cards, pupil credit booklets and off-campus pupil credit booklets.

The BI was delivered to the addressee for their follow-up on 23 December 2014.

In 2014 the CPDP issued a general opinion on the issues related to video monitoring. The CPDP has been asked on multiple occasions to rule on the theme of the lawful performance of video monitoring operations in accordance with the competences vested on the Commission by the LPPD. The Commission's practice on video monitoring issues during the past years demonstrates that as technologies develop on national and global scale, there are increasing opportunities for remote observation of various objects by the usage of video cameras. These technological advancements and their direct impact on public and private life cannot be disregarded by the CPDP when it considers issues related to the lawfulness and permissibility of video monitoring. Given the fact the Bulgarian legislation does not contain detailed provisions on video monitoring as a form of processing of personal data, in assessing the various cases the CPDP also takes into account the international legislation and practice in the area of personal data processing by means of video monitoring.

The issues can be examined in several aspects, including protection of individuals, protection of property, public interest, discovery, prevention and control of offenses/crimes and other legitimate interests. A conclusion can be made that the strict application of the adequacy and proportionality principles is extremely important in the processing of personal data by the use of video monitoring equipment.

In principle, those who have the right to carry out video monitoring in buildings, offices, state and public enterprises are businesses or legal entities, as well as their self-protection units, provided that they hold private-security licenses, as well as state institutions

if they have to perform video monitoring in exercising their functions. In all other cases video monitoring can be carried out only if there is a valid legal reason for this or with the consent of the videotaped individuals.

In its practical work the CPDP aims to ensure that citizens are informed by notice boards posted at well-visible places about the use of technical equipment for monitoring and control of the site. Unless they inform the controller that they refuse to have their personal data processed, it is assumed that they have given their consent in the meaning of the LPPD to have their personal data processed by video control devices.

When the CPDP deals with video monitoring issues, it informs the persons concerned that they have the right to notify the controller that they refuse to have their personal data processed (unless the controller proves a valid legal reason in the particular case). The Commission also reminds citizens of their right to access the data relating to them. Where the exercising of the latter right by one individual may lead to the disclosure of personal data of a third person as well, the data controller must provide only the part of the data related to the person requesting the access. To this end the controller must delete/mask the images of the other videotaped persons by appropriate technical means. If such deletion/masking is technically impossible, then access to video records can be provided only with the consent of all videotaped persons.

When the videotaping operations are carried out by security companies licensed in accordance with the Private Security Act, the CPDP informs the citizens that these operations are supervised by Chief Directorate "Security Police" of the MoI and by the Regional Directorates of the MoI. Citizens can contact these MoI units unless there a breach of the LPPD is involved.

In addition to the general opinion on video monitoring issues, in 2014 the CPDP issued opinions on particular cases. One of these opinions was requested by the MoI and concerned the forthcoming introduction of an automated information system "Videotaping of roadside checks" and in particular the compliance of that system with the personal data processing rules – a theme of major interest to the broad public. The system is used for the processing of personal data (video images) of persons/objects captured by the videotaping devices, namely police officers performing the roadside check and the drivers and the vehicles checked. The objective of these checks is verify compliance with the road traffic rules.

In order to deliver its opinion, the CPDP examined the provisions of two special acts, namely the Ministry of Interior Act (MoIA) and the Road Traffic Act (RTA).

Having analysed the legal framework, including the *Organisational and technical rules for operation of the automated information system "Videotaping of roadside checks"* approved by the Minister of Interior, the CPDP found that the data controller, namely the Ministry of Interior, has undertaken the required technical and organisational measures in order to protect the data against accidental or illegal destruction, or against accidental loss, unauthorised access, modification or dissemination, or against other illegal processing, in accordance with CPDP's *Ordinance No 1 dated 30 January 2013 on the minimum level of technical and organisational measures and the admissible type of personal data protection*.

The opinion of the CPDP in response to this particular inquiry was that the Minister of Interior, in the capacity of DC, can process personal data in the form of video information from the automated information system "Videotaping of roadside checks". In the case at hand the processing is appropriate and lawful on the grounds of Article 4(1)(6) LPPD, namely exercising of powers provided to the data controller by special laws (Articles 25, 26 and 91 MoIA as well as Article 165(2)(7) RTA).

2. Data transfers

During the reporting period the CPDP received 11 requests for permission of data transfers to third countries in the meaning of the LPPD.

In summary, the Commission's position on data transfers to third countries is the following: where personal data is transferred on the grounds of Article 36a(5)(2) LPPD, the DC need not request a permission for such transfer. In these cases the DC should notify the forthcoming transfer to the CPDP and provide evidence of concluded standard contractual clauses.

If the data transfer is pursuant to Article 36a(5)(1) LPPD, no permission is required if the European Commission has by its decision confirmed that the third country, to which the personal data is transferred, provides an adequate level of protection. The DC should notify the data transfer in a register kept by the CPDP according to Article 42(1) of the Rules on the activity of the CPDP and its administration (RACPDPA), including the country of the data recipient.

If the data transfer agreement is concluded with a recipient company established and based in the United States of America, which is included in the Safe Harbour List[1] and has confirmed to the US Department of Commerce that it will adhere to what is known as the

[1] List of US-based companies that agree to respect and apply Commission Decision No 2000/520/EC of 26 July 2000 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 list is published on the website of the US Department of Commerce and is regularly updated.

Safe Harbour Framework, the data controller should request from the CPDP permission for data transfer to a third country. Articles 36a(7) and 36b(1) LPPD apply in these cases.

In respect to all data transfer requests based on Article 36a(7) LPPD, including point 1 thereof, in each individual case the CPDP makes an assessment as to whether an adequate data protection level is ensured and also assesses the data protection measures undertaken. Any processing for purposes other than the original purposes for which the personal data is collected will amount to reprocessing and will need a valid reason of its own in order to the permissible (Article 4(1) LPPD). The individual's consent is one of the alternative conditions for the admissibility of personal data processing, set out in Article 4(1) LPPD, and is one of the preconditions for the transfer of such data to a third country (Article 36a(7)(1) LPPD). The consent is mandatory whenever the DC transfers personal data to a company based in a third country and relies on the said Article 36a(7)(1) LPPD.

As in previous years, in 2014 the CPDP also 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. These rules are developed and complied with on voluntary basis by multinational corporations in order to ensure adequate data transfer environments between companies within the corporation. This data transfer tool is complimentary to the standard contractual clauses and is regulated by the Working Papers of the Article 29 Working Party. The standard contractual clauses approved by the European Commission's Adequacy Decisions continue to govern data transfers to companies outside the corporation based in third countries. 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 in fulfillment of Article 36b LPPD and on the basis of the provided evidence that the DCs which provide and receive the data have undertaken contractual commitments to ensure sufficient protection.

VII. Training in the area of personal data protection

In 2014, the Commission continued its systematic, purposeful training activity. There were four main focuses in the training plan in the reporting period.

- Training of professional associations;
- Training of large data controllers;
- Training of central and judicial authorities;
- Training conducted jointly with partner institutions.

19 training workshops were carried out in 2014, including 2 workshops for professional associations, 7 training courses with central and judicial authorities and 3 workshops with large data controllers from the telecommunication sector. This includes also 7 workshops conducted jointly with training partners (the Institute of Public Administration (IPA), the International Banking Institute).

1. Training of professional associations

One of the focuses in the training activities set by the Commission for 2014 was the training of professional associations. This tradition is a good practice introduced in 2013 and found its natural continuation in 2014. The training of professional associations allows for better alignment of standards and data protection practices of all members of the associations, as well as wider dissemination of learning outcomes. One of the purposes of these trainings is to find answers to common problem areas and to create uniform practices in addressing these areas.

In 2014, training was delivered for two professional associations: the Association of the Professional Accounting Companies and the Bulgarian Medical Association.

2. Training of large data controllers

In 2014, the Commission identified the need for training data controllers which maintain large-scale data bases. The focus was on telecommunication operators providing electronic communications services. The level of penetration of mobile services in the Bulgarian market is high (123% against 112% EU-average), which makes telecommunications a priority sector for preventive work of the CPDP. Telecommunication operators process significant volumes of personal data, and in 2013 over 60% of all

complaints submitted to the CPDP from citizens were against a company in the telecommunications sector.

In this regard, in 2014 trainings were delivered to employees of MTel, Bulgarian Telecommunication Company and Telenor (formerly Globul).

3. Training of central and judicial authorities

As part of its activity, the CPDP aims to achieve better interaction with state authorities in order to facilitate workflows and customer services. In its previous training campaigns, the CPDP always placed a particular emphasis on the training of state institutions as the latter are expected to serve as a model for compliance with the legal norms and rules. For comparison, in 2011 the CPDP trained the employees of all institutions that had access to the National Schengen Information System. In 2012, the focus of the training was placed on local authorities, wherein a series of trainings took place in several regional cities in Bulgaria. In 2013, the state authorities that participated in the trainings were selected based on the volume of personal data collected and processed. The application of this working principle continued in 2014. The trainings of large data controllers in the reporting period covered DCs working with large-scale data bases. The trainings in 2014 consisted of workshops for judges and court staff from the administrative courts in Haskovo, Pazardzhik and Smolyan, the National Insurance Institute, the Ministry of Labour and Social Policy and the National Revenue Agency.

In 2014, at the invitation of the National Institute of Justice, a representative of the CPDP was included for the first time as a lecturer in the distant learning series of the Institute. The specific training on "Protection of personal data in the judicial system", intended for court staff from the courts in the country was conducted as a distant learning combined with attendance meeting using the specialized web-based system of the Institute.

4. Training conducted jointly with partner institutions

In 2014, the Commission implemented successfully the best practices in conducting trainings jointly with partner institutions, wherein the CPDP provided lecturers and training materials, while the partner institution was responsible for the organisation of the training itself and for dissemination of the materials. Trainings conducted jointly with partner organisations are particularly beneficial for the CPDP, as they help the institution with the logistics of the training process. In 2014, the Commission continued its cooperation with the

International Banking Institute and the Institute of Public Administration by conducting seven training workshops in total with more than 270 trainees.

5. Statistics and trends

In 2014, the trainings conducted by the CPDP included 515 controllers and processors of personal data, an increase of over 38% compared to the previous year.

In the course of the trainings, the CPDP offered a feedback survey, through which the trainees evaluated the conducted training. Statistics show that in the reporting period, 199 attendees completed the survey. The combines rating across all trainings is presented on Figure 11:

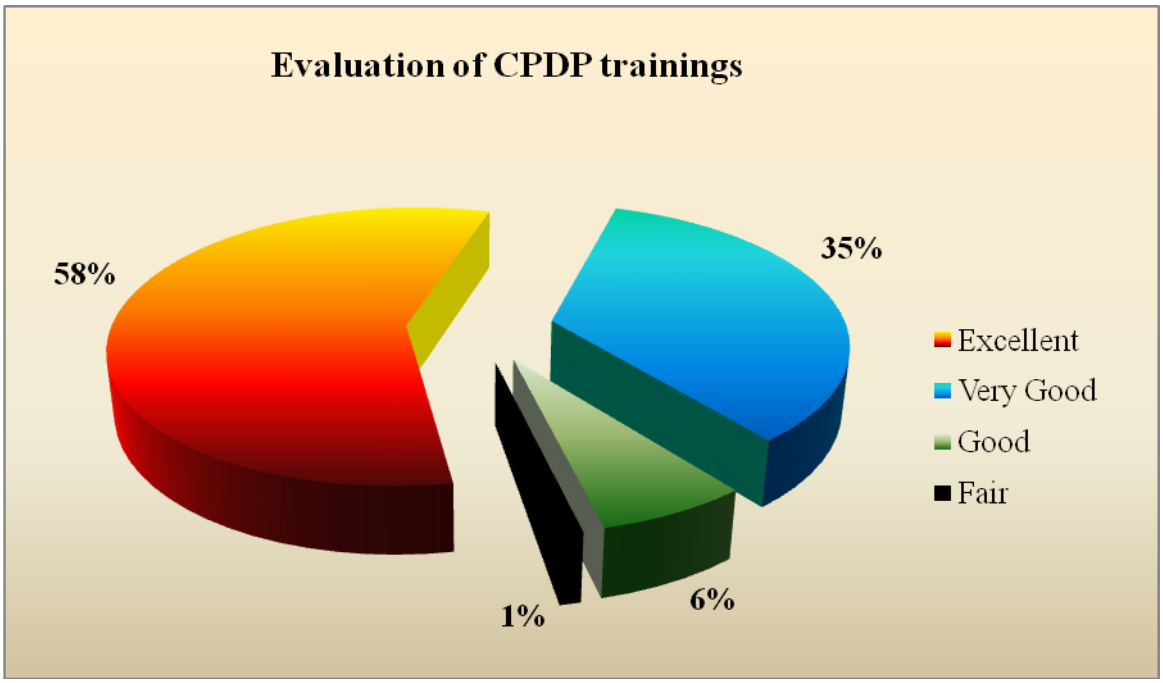

Fig. 11

When benchmarking the results of the training with the results of the preceding years 2011, 2012 and 2013, a grounded conclusion can be made that the Commission has significantly raised the level of its training courses. This is a result of the adaptation of the training programme in line with the accumulated recommendations and lessons learned in previous years. The topics of the lectures in 2014 were optimised and updated to include the latest trends in the development of public relations in the field of personal data protection. The emphasis was on the practical orientation of the training by developing case studies and

role plays. This was highly appreciated by the trainees as almost two-thirds of the respondents evaluated the training as „excellent“. The highest marks „excellent“ or „very good“ were given by 9 out of every 10 respondents. At the same time, those that rated the training only as „satisfactory“ were only 1%. The practical orientation of training was pointed out as its greatest advantage – one-fourth of the respondents said that this was the most positive feature of the learning process. Another 10% were impressed by the competence and the professionalism of the lecturers.

The main recommendations of the trainees related to the need to ensure stability and continuity in the learning process by conducting subsequent trainings and dissemination of information materials.

6. DC training needs analysis

An important supporting activity of the training process carried out by the CPDP is the analysis of training and awareness needs of DCs and the public at large. This activity is important with a view of fully meeting the needs of citizens and businesses and effectively spending the limited financial and human resources available to the CPDP for the trainings. The study of training needs allows identification of trends and tendencies for adjusting in the curriculum, contributes to improving the quality of learning materials, and dedicates efforts and resources to sectors that have the greatest need for training. A significant advantage of this supporting activity of the CPDP is its broad scope. The study includes data controllers who have obligations under LPPD as well as the citizens who are entitled to protection. The interaction between rights and obligations in the data protection and privacy system is essential for its normal functioning.

In 2014, the CPDP continued the tradition of studying DCs training needs in order to adapt the learning process to their requirements and expectations. This is accomplished by carrying out surveys among DCs, and their number for 2014 was 130.

In the completed surveys half of the controllers said that they had a thorough knowledge of the LPPD and 90% of the respondents believed they are aware of their obligations as data controllers (DC). Over 75% have never encountered difficulties relating to the protection of personal data, but two-thirds said they would like their employees to be trained by the CPDP. On the question how much of their staff should be trained, 41% of the DCs believed that training should be extended to all employees in the company or organisation, half of the respondents believe that training should be delivered only to the employees that actually process personal data. As regards the most adequate form of training,

the controllers expressed their preference for lectures and workshops (73%) and only 14% rely on distant learning by using self-study materials. Online training is the least preferred option as only 8% of all respondents support it.

As regards the content of the training courses, the controllers believe that it should be carried out in 2 consecutive days with a total length of 8 hours covering mainly topics related to the legal framework on data protection, the technical and organisational measures for protection and the obligations of controllers. 90% of all the respondents wish to receive informational materials, almost all prefer to receive them electronically rather than on paper. The controllers hope to find in the materials mainly specific case studies and case-law of the CPDP, as well as more details on the measures to protect personal data. Indicative of the need for training in the protection of personal data is the fact that over 90% of respondents believe that such training would be of practical use in their work. However they suggest that more training workshops for data controllers is needed to improve the training effectiveness.

Due to the undeniable usefulness of training needs analysis as a tool for active and focused policy to increase public awareness on the protection of personal data, the CPDP will maintain this practice in its future activities.

7. Public awareness needs analysis

CPDP's analysis of training and awareness needs in the field of personal data protection covers also the citizens, whose data is subject to processing. They have the right of protection of their personal data and privacy. The most effective way to protect their data is by achieving greater awareness and knowledge of the legal framework and the rights of individuals, which contributes to the prevention of possible violations. In this regard it is important to explore the citizens' awareness and needs for training and information campaigns.

191 respondents completed the 2014 CPDP surveys intended for individuals. Over half of them indicated that they are vaguely acquainted with LPPD, but another 40% believe they have profound knowledge of this issue. Anyway, over 80% of the respondents believe that they know what personal data is and another two-thirds respond that they know their rights as individuals. One-third of the respondents have a need to exercise their rights relating to the protection of personal data, and only 10% have difficulties in this regard.

The majority of respondents, more than 80%, are of the opinion that the personal data of Bulgarian citizens is not adequately protected, but only 30% say they have been victims of abuse of personal data. Among the most common abuses are direct marketing campaigns,

collecting disproportionate amounts of personal data and failure by controllers to take adequate protection measures.

A significant majority of the respondents would like to receive information materials or participate in information campaigns relating to the protection of personal data – as much as 85%. Over 80% of the respondents to this question prefer to receive materials electronically. Citizens firmly believe that the CPDP should have an even greater presence in mass media. 90% of respondents replied positively to this question.

VIII. Implementation of nationally and internationally funded projects

Given the fact that the Commission for Personal Data Protection is the only state authority in the field of personal data protection and privacy and due to the limited funding from the national budget available for it to exercise its powers, the CPDP strives to improve its operation and raises the quality of the services rendered by attracting European funding This pursuit of the institution is in line with the national policy followed by the Republic of Bulgaria regarding the use of the opportunities provided by EU funds.

In terms of development and management of projects, 2014 was the most successful year in the history of the Commission. This year marked the successful completion of 4 projects and the conclusion of contracts for funding of another 2 projects, amounting to BGN 335,961. The total number of projects managed by the CPDP in 2014 was 7 under 3 different European programmes.

1. Leonardo da Vinci Programme

Leonardo da Vinci Programme is a programme that supports and carries out the policy on vocational education and training of the EU Member States by taking into account the content and organisation of the relevant national policy. The programme is aimed at enhancing the quality of vocational education and training, encouraging innovation, and disseminating good professional practices and systems in Europe through transnational cooperation and on the basis of the experience gained. Two projects of the CPDP were approved within the programme in 2012 and the first one was successfully completed and reported in 2013. The implementation of the second project within the programme finished in 2014.

„Raising awareness of the persons working in the EU labour market on personal data protection issues“ Project - „Leonardo da Vinci“ Programme, Activity: „Partnerships“

The project started in September 2012. The total amount of funding allocated to the CPDP was EUR 11,000. The funding was verified by the Managing Authority and reimbursed in full after completion of the project in July 2014. Partners of the CPDP in this project were the Bureau of the Inspector General for Personal Data Protection in the Republic of Poland,

the Office for Personal Data Protection in the Czech Republic and the Agency for Personal Data Protection in the Republic of Croatia.

Six working meetings in the partner countries were carried out in the course of the project. The working meetings were part of the preparation of the outcome of the project – development of a Guide titled „Privacy protection at the workplace. Employee guide". The Guide is intended to be used by the individuals looking for jobs or working in the European Union and aims to increase their understanding of issues related to the protection of their personal data. The handbook includes practical data protection issues and provides advice to individuals. The publication itself is divided into 5 parts – job search, recruitment procedure, employment period, data protection and termination of the employment relationship, employee rights and supervisory authorities as a helping hand. The supervising authorities, partners under the project, are presented in the Guide and the key definitions in the field of personal data protection are summarised in the glossary of terms.

In 2014, two project meetings were held in Zagreb (Croatia) and in Gdansk (Poland) respectively, the second one being the official presentation of the publication to the public. The Guide was presented in Bulgaria at a dedicated round table on 28 July in the CPDP premises. Representatives of the Ministry of Labour and Social Policy, the General Inspectorate of Labour and the Employment Agency took part in the event by an invitation of the CPDP.

The Guide for individuals in the labour market can be found on the respective website of the institutions that participated in the project. It can be found in the Get Informed section of the CPDP website. The Guide is also disseminated through the websites of partner institutions – the Ministry of Labour and Social Policy, the General Inspectorate of Labour, the Bulgarian Chamber of Commerce and Industry and the Employment Agency. In September, a request was received by the CPDP from the Romanian data protection supervisory authority to permit the translation and distribution of the Guide on the territory of Romania with view to its topical importance and excellent practical relevance. The CPDP answered positively to the request.

2. Projects in the Operational Programme „Administrative Capacity" (OPAC)

OPAC was one of the seven operational programs in the programming period 2007-2013. It is designed for the state administration and aims to improve its functioning in order to implement effective policies, to provide quality services to citizens and businesses, and to create conditions for sustainable economic growth and employment, as well as to enhance the

professionalism, transparency and accountability in the judicial system. In 2014, the CPDP completed and reported three OPAC projects. Furthermore, the OPAC Managing Authority approved two new project proposals of the CPDP to be completed in 2015.

2.1. Project entitled „Improving the management, organisation and functions of the Commission for Personal Data Protection by conducting a functional analysis“

This was the first personal data protection project of the CPDP within the framework of OPAC. It amounted to BGN 213,829.91 and aimed to improve the management, organisation and functioning of the Commission for Personal Data Protection. The main activity of the project was functional analysis of the CPDP in order to identify opportunities to improve its performance and optimise the structure and business processes within the organisation.

The project was completed in June 2014. As a result, new internal rules of the CPDP were developed and approved and the structure and functional interaction within the institution were changed. Some of the other activities undertaken in 2014 included training in change management for CPDP staff, a round table with stakeholders and a final press conference. After the project completion, the CPDP successfully passed a detailed spot check carried out by authorised representatives of the Managing Authority, which found high quality of project management. The Managing Authority verified all project costs amounting to BGN 125,703.14.

The successful completion of the project contributed significantly to the accumulation of useful experience in project implementation by the CPDP experts and enhanced the effective functioning of the Commission.

2.2. Project entitled „Promoting the professional development of the employees of the CPDP by applying a system of training in accordance with their professional duties“

The contract for this project was signed on 4 July 2013 and amounted to BGN 34,647. The project aimed to improve the professional competence of the employees of the Commission for Personal Data Protection for more effective and efficient performance of their duties. Within the project, the Commission staff took a series of training courses chosen by themselves, aimed at enhancing their professional competence. A total of 34 training courses were conducted on a variety of topics, including legal disciplines, software training, training of trainers, courses in human resources management and improvement of communication skills.

The project was successfully reported to the Managing Authority in August 2014. The Managing Authority verified all project costs, which amounted to BGN 28,279.16.

2.3. Project entitled „Strengthening the administrative capacity of the Commission for Personal Data Protection for working with databases, information systems and teamwork“

This BGN 87,484.74 project was completed in July 2014. The project aimed to improve the professional competence of CPDP staff for more effective and efficient performance of their duties and was aimed specifically to the employees of the Informational Funds and Systems Directorate. The experts from this Directorate of the specialized administration participated in various training courses to improve their teamwork, increase their skills to work with Windows 2008, web-based systems and Oracle. Within the project, 4 training courses with 14 participants were conducted in total. The Managing Authority verified all project costs amounting to BGN 76,472.48.

The successful implementation of this project allows the CPDP to acquire greater autonomy and professional security in managing its own information resources and helps improve teamwork and interaction in the administrative units of the Information Directorate.

2.4. Project entitled „Improving and expanding the electronic services to businesses and individuals provided by the CPDP, and integrating them with the Single point of access to administrative e-services“

The contract for financing the project was signed in February 2014 and amounted to BGN 391,089.38 The aim of the project was 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. Its successful implementation should lead to the development and implementation of new and updated features of the Information system for registration of data controllers (eRALD) and its integration in the Single point of access to administrative e-services.

At the date of this report, the project inception conference has been carried out and questionnaires have been developed and approved to assess the level of impact (threat) and to identify measures for protection of processed personal data, as well as questionnaires for ex-ante, current and ex-post checks for compliance with the LPPD requirements by DCs (inspections).

The project is planned for completion in August 2015.

2.5. Project entitled „Improving the qualification and building on skills and competencies of the CPDP staff for more effective and efficient performance of their duties“

The CPDP and the OPAC Managing Authority signed a grant contract in September 2014. The contract value is BGN 158,068.40.

The main aim of the project is to improve the qualification and build on existing skills and competences of the CPDP staff for more effective and efficient performance of their duties. The project builds on the other two CPDP projects related to staff training. The need for an additional series of training stems from the changes in the European legal framework on data protection, which are currently underway, as well as from the changes in the Rules on the activity of the CPDP and especially the new functions of the administrative units of the CPDP. In view of this fact, the project includes training on strategic planning, risk management, more effective communication with EU institutions, development of communication strategies and information campaigns. There will also be trainings for the general (non-specialised) administration, to be conducted by the Institute of Public Administration.

The project is scheduled for completion in September 2015.

With regard to the election of the new managing body of the CPDP in April 2014, annexes to all contracts concluded under approved projects in 2013 and implemented in 2014 were drafted and signed, as well as to contracts concluded in early 2014 for Project Manager, Coordinator, Accountant and Technical Assistant.

3. Programme for the Prevention of and Fight against Crime of the European Commission

Project entitled „Creation of a national unit for collection and processing of Passenger Name Record (PNR) data in the Republic of Bulgaria“

The CPDP is a co-beneficiary under this project jointly with the State Agency for National Security (SANS). The objective of the project is the setting up of a SANS unit to collect and process PNR data of passengers arriving in or departing from the Republic of Bulgaria by air. This will support the efforts to combat terrorism and identify individuals who potentially endanger the national security of the EU Member States. Representatives of the CPDP participate in the project with expertise and opinions, intended to ensure compliance with the European and national legal framework on data protection and protection of the rights of individuals in the creation and operation of the PNR Unit.

The project is scheduled for completion by the end of 2015.

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

On 8 April 2014 the Court of Justice of the European Union invalidated Directive 2006/24/EC of the European Parliament and of the Council dated 15 March 2006 on the retention of data generated or processed with regard to the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Directive on retention of traffic data)[2]. The judgment holds that the provisions of the Directive infringe the right to privacy and the fundamental right to personal data protection stipulated in the Charter of Fundamental Rights of the European Union (EU). By the end of 2014, the European Commission was still carrying out a thorough evaluation of the ECJ judgment and its consequences.

Following the invalidation of Directive 2006/24/EC in 2014, the Ombudsman of the Republic of Bulgaria referred the Constitutional Court with an application to establish the unconstitutionality of the provisions of Article 250a - Article 250f, Article 251 and Article 251a of the Electronic Communications Act (ECA), which transpose the Directive, arguing that these texts are inconsistent with Article 5(4), Article 32(1) and Article 34 of the Constitution of the Republic of Bulgaria. Regardless of the initiated constitutional case and the ECJ judgment, the CPDP considers that its status of security supervisory authority requires the CPDP to fulfill its legal obligation regarding the provision of summary statistics on the retention of and access to traffic data. In this regard and in compliance with Article 261a(5) ECA, the CPDP prepared and submitted its annual analysis to the National Assembly and to the European Commission within the statutory time-limit (31 May).

In its analysis, the CPDP concludes that although it managed to introduce some tendencies for compliance with its instructions, including to some of the recommendations made, additional explanatory outreach activities are necessary among all companies aiming at alignment of the interpretation and application of ECA.

In the analysis, and subsequently in its opinion to the Constitutional Court, the CPDP maintained in terms of data protection the present version of the ECA creates prerequisites for violation of the principle of proportionality in two aspects:

1. The fact that the authorised bodies under Article 250b(1) and Article 250c(4) ECA do not make any requests for access to data relating to Internet telephony, Internet access and Internet email or rather do this as an exception, calls into question the necessity and desirability of preserving this kind of traffic data concerning unlimited circle of Bulgarian

[2] Judgment of the Court (Grand Chamber) in Joined Cases C-293/12 and C-594/12 of 8 April 2014.

citizens using the Internet as a communication tool or a means of information.

2. The period for storage of traffic data in accordance with the current ECA (one year) is too long. It has been found that the optimal data age is generally three (3) months. It is appropriate that future legislative changes (including at EU level) reduce the maximum time allowed for data retention (for example, up to three months) with a possible extension to a maximum of one year for data, which has already been requested and granted access to.

At national level, with regard to the ECJ judgment and the application of the Ombudsman of the Republic of Bulgaria to the Constitutional Court, the CPDP, as a supervisory authority on data security (Article 261a of ECA), initiated in April 2014 the creation of an interdepartmental working group for regulation of communications with a wide range of stakeholders, namely the Supreme Administrative Court, the Supreme Court of Cassation, the Prosecution of the Republic of Bulgaria, the Ministry of Justice, the Ministry of Interior, the Ministry of Defence, the National Intelligence Service, the State Agency for National Security, the Ministry of Transport, Information Technology and Communications, the CPDP. The task of the working group is to formulate a reasoned proposal for legislative changes that reflect the considerations of the European Court of Justice. Given the importance and the principal nature of the ECJ judgment, the CPDP relies on maximum commitment from the competent Bulgarian authorities to develop a joint position. While the CPDP shares the reasoning of ECJ judgment for invalidation of Directive 2006/24/EC, the Commission is of the opinion that the interdepartmental working group, set up at its own initiative, in its work should find a reasonable balance between the protection of individual rights and all other constitutionally recognised values.

Reaching a coherent approach within the European Union is essential for the drafting of changes to the national laws. The logical pathway is to strengthen the coordination between Member States and the European Commission in view of the situation created by the invalidation of a European Directive which at the time of invalidation was validly in force.

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

In 2014, the CPDP continued its cooperation with the State Agency for Child Protection (SACP), which started in 2013 by training SACP staff in the field of the protection of personal data. As a result of the initial inter-institutional contacts with SACP, the two state institutions make joint efforts to address issues related to the privacy and protection of personal data of one of the most vulnerable categories of personal data subjects – children. In the reporting period, the SACP Chairperson referred to the CPDP the issue on the lawful provision of child data in cases involving an international element. SACP reported that applicants request social reports, which contain a lot of personal data, including sensitive data as well as third persons' data of the parents and the relatives of the children. A question is raised concerning the lawful performance of these actions and the compliance with the rules stipulated in the LPPD.

In order to objectively and comprehensively rule on the matter, in 2014 the CPDP set up on its own initiative an expert working group tasked to jointly analyse the challenges facing the international protection of the child based on the inter-institutional approach and within the competence of the individual departments. Invitations were sent for nomination of experts by the competent institutions – the Ministry of Justice, the Ministry of Interior, the Ministry of Labour and Social Policy, the Agency for Social Assistance and the State Agency for Child Protection. The experts are expected, on the basis of the existing legal framework, to draft a proposal for the approval of uniform rules regarding the procedure and the exchange of information under cases with an international element where children are involved.

In 2014, the cooperation of the CPDP and the State Agency for National Security (SANS) continued within the framework of the project „Establishing a National Passenger Information Unit (PIU) for gathering and processing of PNR data in the Republic of Bulgaria". The CPDP participates on a regular basis in the working meetings under the project. Representatives of the CPDP are included in a separate working group with SANS for drafting the legal amendments in order to create the necessary legal prerequisites for establishing a National Passenger Information Unit (PIU) for gathering and processing of PNR data. The CPDP was invited to a seminar organised by the State Agency for National Security, which included ground-handling operators and airlines operating in the territory of

Bulgaria. A representative of the CPDP was invited by the organisers to deliver a lecture on „Measures to protect personal data of passengers when processed by the PNR unit".

In pursuance of its powers to maintain a register of the data controllers and of all the registers kept by them, the CPDP interacts with the Directorate General „Civil Registration and Administrative Services" (GD GRAO) with the Ministry of Regional Development in terms of access to personal data of the National Database „Population" for a particular individual, as well as with the Registry Agency with the Ministry of Justice concerning the BULSTAT Register and Commercial Register. The CPDP receives data from the two institutions about natural and legal persons as well as central and local authorities in their capacity of data controllers. This information is required for maintaining the register under Article 10(1)(2) of LPPD.

The CPDP provides on-demand information to the structures of the Ministry of Interior and those of the judiciary concerning the registration status of particular DCs.

In 2014, the CPDP continued its consistent policy of transparency and openness in the implementation of its activities, of beneficial partnership and interaction with other state bodies, with representatives of the civil society and the media.

Following the established tradition, the CPDP celebrates every year the Data Protection Day 28 January, by organising and implementing events and initiatives of various types and scale. The organised events on this day aim not only to promote the important date, but also raise public awareness on the issue of protection of personal data as a fundamental element of security in modern society.

On the occasion of the Data Protection Day in 2014, the CPDP organised and conducted for the first time a combined training of DCs (institutions and professional associations) in the health sector. Representatives of the Ministry of Health, National Health Insurance Fund, „Fund for Treatment of Children" Center, National Addiction Center, Bulgarian Medical Association, Bulgarian Pharmaceutical Union, „Fund for Assisted Reproduction" Center, Association „Health Protection Confederation" and the non-profit organisation „Bulgarian Association for the Protection of Patients" were invited to participate in the training. Representatives of the national media attended and covered the event.

The training programme covered topics related to the obligations of DCs, personal data processing, the rights of individuals and the processing of sensitive personal data in the health sector. Special attention was paid to the protection measures and development trends in the field of health. Particular examples were presented as well as CPDP case studies related to DC duties and LPPD violations.

On the same day, in an open reception room, the CPDP provided an opportunity to interested citizens, DCs and media representatives to receive advice and assistance on specific issues relating to the implementation of the LPPD. Representatives of all specialised departments of the institution responded to questions on the European and international legislation in the field of the protection of personal data, the Schengen Information System and more. Last but not least, the procedure for registration of DCs and the aRALD register maintained by the CPDP were explained.

In the reporting period, the CPDP continued its communication with other state bodies, NGOs and media in Bulgaria. This fruitful cooperation and coordination with the institutions is regarded by the CPDP as a guarantee for achieving the objectives in the field of protection of personal data at a higher level.

During the reporting period the CPDP continued to develop effective cooperation with representatives of higher education institutions. For yet another year, the CPDP is a co-organiser of a scientific conference „The new paradigm in cybersecurity" jointly with Vassil Levski National Military University (Artillery, Air Defence and CIS Faculty - Information Security Department), State Agency for National Security, State Commission on Information Security, CIS Directorate and Information Security Directorate with the Ministry of Defence and the Defence Institute „Professor Tsvetan Lazarov" with the MoD. The event was held on 5 and 6 June in the city of Shumen. The CPDP experts presented a paper entitled „Personal data protection in cyberspace", stating the major problems related to privacy in the context of collection, generation and processing of large databases in the provision of cloud services, and offered generalised solutions and recommendations for more effective management and regulation of the existing processes. The paper offered response mechanisms based on the national and international practice of data protection authorities. It also provided guidance for the improvement and development of data protection through training at all levels, conducting discussions, strengthening the interaction between experts – lawyers and IT specialists, as well as by good cooperation between all stakeholders at national and supranational level.

Public relations and providing information to the media

Whether in its daily activities or in the implementation of long-term projects, the CPDP always strives to deliver the highest possible level of information and transparency.

On 16 April 2014, at a special press conference and amid serious interest by printed and electronic media, the new composition of the Commission for Personal Data Protection was presented. At his first press conference, the Chairperson of the CPDP, Ventsislav

Karadjov, presented the members of the supervisory body and outlined the priorities in the work of the new management of the institution. The event was attended by the former CPDP Chairperson Veneta Shopova and by the former member Krassimir Dimitrov and Valentin Enev.

In July 2014, at a special press conference in the Ceremonial Hall of the Central Military Club, the results of the checks of the political parties, coalitions of parties and initiative committees that submitted documents for registration to participate in the elections for Members of the European Parliament were officially presented. Hundreds of citizens were affected by misuse of their personal data during the registration of political entities in the MEP elections held on 25 May 2014. The CPDP announced, at the meeting, the official findings of the checks on the political parties, coalitions of parties and initiative committees that submitted documents for registration to participate in the MEP elections, as well as the recommendations made for data protection in their capacity as DCs. Recommendations were made to citizens as well to act more responsibly in the provision of personal data.

The event was attended by representatives of the Office of the Vice President Margarita Popova, the Central Electoral Commission (CEC), non-governmental organisations that participated as observers during the checks carried out by the CPDP, as well as representatives of 45 political entities – political parties, coalitions of parties and initiative committees that were checked by the CPDP. Representatives of over 30 electronic and printed media, including national and local TV channels, covered the event with multiple publications in the press and interviews with the CPDP Chairperson and members.

The CPDP website is an essential tool for information and public outreach. Materials are regularly published in the individual sections reflecting the activity of the CPDP and the monthly media monitoring. The information on the website is constantly updated, making it a valuable tool for citizens in matters relating to the protection of personal data in various life situations. The aim is to achieve comprehensive awareness of the broad public with the CPDP activity and full operational transparency.

In the reporting period, due to the already established and facilitated personalised contacts between the CPDP and media representatives, over 150 interviews and materials were realised with the CPDP Chairperson and members and with experts from its administration. Electronic newswires and electronic media regularly cover the activity of the CPDP. During the year, the CPDP responded to topical public issues and participated in interviews on various topics shown on the Bulgarian National TV, bTV, Nova TV, TV7,

Horizont Radio, Hristo Botev Radio, Darik Radio, 24 Hours Daily, Trud Daily, Capital Weekly, Banker Weekly, Monitor Daily and others.

The CPDP provides timely information to journalists in response to their written or verbal questions. The continuous cooperation of the institution with the line reporters led to the publication of a significant number of information materials and journalistic investigations that affect 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 CPDP to achieve publicity, transparency and open dialogue with the Bulgarian society.

XI. International activity. Reform in the area of personal data protection

In 2014 the CPDP continued its active participation in the implementation of the European legislation on data protection and privacy, as well as in the discussions of the legislative reform package on data protection proposed by the European Commission.

CPDP stands ready for stronger involvement in the work of data protection authorities in the European Union with taking leadership positions in the Working Party under Article 29 of Directive 95/46/EC and the Customs Joint Supervisory Body. The Chairperson of the CPDP Ventsislav Karadjov was elected a Vice-Chairperson of the Article 29 Working Party and Tsvetelin Sofroniev, CPDP Member, a Vice-Chairperson of the Customs Joint Supervisory Body.

The protection of personal data is one of the priorities of the Bulgarian Rotating Presidency of the Police Cooperation Convention for Southeast Europe (July-December 2014) with the CPDP having a key role in the presidency. The provided opportunity allows the CPDP to address a key stage in the protection of personal data under the Convention. In 2014, the process of evaluating the level of data protection in the Contracting States was successfully completed. According to the requirements of the Convention, the positive assessment in the field of protection of personal data is one of the conditions for exchange of information, including personal data. The cross-evaluation process was launched in 2009 with the creation of a specialised Ad-hoc Working Group on Data Protection and completed in 2014. This was the occasion, during the two-day meeting on data protection held on 2-3 December in Slovenia, part of the calendar of the Bulgarian Rotating Presidency of the Convention, on which the CPDP proposed rethinking the mission of the Ad-hoc Working Group on Data Protection so as to provide a timely response to successful evaluations in the field of protection of personal data in all 11 Contracting States and to ensure consistent application of the provisions set out in the Convention for the protection of personal data.

In preparing the documents that form the basis of discussion during the meeting held in Slovenia, the CPDP recognised the importance of the Ad-hoc Working Group as a key tool to monitor the exchange of personal data for the purposes of the Convention and the need to achieve higher consistency among the Contracting States. Closer co-operation should be sought not only with regard to compliance with the provisions of the Convention, but also towards enhancing the public visibility of the Ad-hoc Working Group on Data Protection and improvement of communication in the event of specific national issues relating to the

protection of personal data, including the exchange of good practices in handling complaints from individuals.

As a result of the meeting held and the objectives that the CPDP had set, an agreement was reached on the need to change the mandate of the Ad-hoc Working Group on Data Protection. The highlights in the proposed new functions are the advisory powers of the Working Group and the right to give recommendations and opinions on issues related to the protection of personal data within the framework of the Convention, the requirement for exchange of information on inspections carried out by the national data protection supervisory authorities on the operating units under the Convention and the creation of uniform practices for inspections, exchange of case-law on complaints from individuals, the creation of a catalogue of good practices and the launch of activities for raising public awareness.

In view of the continuing nature of the tasks proposed in the new mandate, it was agreed to change the status of the Working Group on Data Protection by removing its *ad-hoc* feature. A draft Decision of the Committee of Ministers of the Convention is being prepared to amend the Rules of Procedure for evaluations in the field of protection of personal data, which should be discussed during the Hungarian Presidency of the Police Cooperation Convention for Southeast Europe in 2015.

The year 2014 was a preparatory stage for the implementation of the obligations arising from Commission Regulation No 611/2013 on measures applicable to the notification of security breaches of personal data.

During the reporting year, the CPDP fulfilled its obligations for cooperation and interaction with the national supervisory authorities of the Member States and the bodies of the European Union through the exchange of information and experience on inquiries relating to the powers of the CPDP and their implementation. 75 international inquiries were considered, and most of them came from peer authorities for data protection. Answers were given to inquiries from other organisations, research institutes and consulting companies dealing with the issues of privacy and data protection. The areas of cooperation cover control activities, imposition of administrative sanctions, registration of DCs, permission of data transfers to third countries, digital education, individuals' right of access to their data, including the Schengen Information System, direct marketing, processing of personal data on the Internet (acceptance of cookies when using websites, use of malicious software), legal provisions, processing and protection of personal data of minors, the methodology for assessing the impact on privacy and others.

The CPDP participated in the preparation of the Bulgarian position in the discussion of the proposed legislative dossier on data protection at the Justice and Home Affairs Council. Along with the views expressed during the year with regard to the discussed aspects of the proposal for a general data protection regulation, the CPDP offers as a national position a call for the Member States to reach a reasonable compromise in order to achieve real progress on the dossier.

The CPDP contributes to the formation of a common approach of the EU Council on the proposal for a new Europol Regulation, which aims to create a more effective supervision mechanism. The position of the CPDP is to maintain the strong role of the national data protection authorities in the supervision of Europol.

In 2014 the CPDP also contributed to the implementation of European initiatives such as the project of Open Society Institute on the importance of personal data to promote equality and the implementation of Directive 2002/58/EC on the processing and protection of personal data in the electronic communications sector.

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

The participation of CPDP representatives in international working groups and supervisory bodies continued in 2014.

1.1. Participation in the regular meetings of the Working Party under Article 29 of Directive 95/46/EC

During the reporting period, representatives of the CPDP continued to participate in 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. Key topics discussed in the meetings held were the consequences of mass surveillance programs used by the security services and the creation of systems for the processing of PNR data, the practical cooperation between data protection authorities and the status of the reform on data protection. The adequate level of protection in third countries with emphasis on modernization of the Safe Harbour Programme was another subject of discussion. From a technological point of view, another important issue of the Article 29 Working Party is concerns the development of analysis as regards of techniques for pseudonymization and anonymization of personal data, risks and opportunities for the exercise of control (consumer

and institutional) using the Internet connected devices (Internet of Things), cloud services and unmanned aerial vehicles (drones) for civilian purposes. The activity of the Working Party regarding the privacy policies of social networks and Internet search engines continued. In relation to the processing of personal data on the Internet, the main task of the Working Party during the year was to regulate the relations with DCs that process personal data. A thorough analysis was made of the decision of the European Court of Justice in the Google case and a methodology was developed to align the practice of supervisors in handling similar cases on a national level. The WP also discussed the consequences of the ECJ judgment which invalidated Directive 2006/26/EC on the retention of traffic data.

1.2. Participation in regular meetings of the Joint Supervisory Authorities of Europol and Customs

In 2014, representatives of the CPDP continued to participate in the meetings of the Joint Supervisory Authorities (JSA) of Europol and Customs.

Within the framework of the **Europol Joint Supervisory Authority** (Europol JSA), issues were discussed related to the powers and competence of the supervisory authority and its relations with other supervisors and in particular with the European Data Protection Supervisor and the protection of personal data resulting from the provisions in the proposal for a new Europol Regulation. The basis for the exchange of operational and strategic information and intelligence data, as well as the operation of the Cyber-attack Response Centre and the implementation and operation of a new system for analysis of Europol were subjects for discussions as well. Another focus of group was the organisation of inspections on the processing of personal data in the system of Europol. The modernisation of the system for secure information exchange SIENA and the introduction of harmonised criteria for the exchange of law enforcement information between the police systems, the justice and the data protection systems and the need for standardised questionnaires/checklists for use in inspections were also among the priorities of Europol JSA in 2014.

During the meetings of the Joint Supervisory Authority of the Customs Information System (Customs JSA) issues were discussed relating to practical application of the working framework on data protection and the Customs Information System and the right of access of individuals to the system. The inspection conducted by the European Anti-Fraud Office (OLAF) as well as possible future actions were discussed as well. An overview was made of the developments related to the approved brochure on the rights of persons and the responsibilities of the competent authorities with regard to the Customs Information System.

1.3. Participation in regular meetings of the Coordination Groups for supervision of the Customs Information System, Eurodac, the Visa Information System and the Schengen Information System

The Commission for Personal Data Protection takes active part in the work of the specialised Supervision Coordination Groups, which are led by the European Data Protection Supervisor and consist of representatives of the national data protection authorities of the Member States of the European Union.

During the reporting period, at the meeting of the Supervision Coordination Group of the Customs Information System (CIS), the inspection reports of the Irish CIS and OLAF, the draft Manual for the exercise of the rights of persons to access data in CIS and the work program of the coordination group for the period 2014-2015 were considered. The evaluation of the usefulness of CIS, the exercise of the right of access by persons, the improvement of the interaction between the Joint Supervisory Authority and the CIS Supervision Coordination Group were outlined as the main priorities of the Group.

The meetings of the EURODAC Supervision Coordination Group discussed the current state of the system and its use, the pending preparation of leaflets with information on data processing for persons accessing the Eurodac system, as well as the upcoming review of the system in 2015.

The Visa Information System (VIS) Supervision Coordination Group discussed issues such as the latest developments of the visa information systems and the competent authorities with access rights, updates of the information provided by the system, as well as assigning part of the activities on issuing visas to subcontractors while enabling data protection authorities to carry out checks on these subcontractors. In this respect, the CPDP gives implementation guidance to the Ministry of Foreign Affairs.

The information system security, the rights of persons and the ongoing development and preparation of regulations on necessary security measures in case of outsourcing certain processing operations to external contractors were the topics discussed at the meetings of the Supervision Coordination Group of the Second-Generation Schengen Information System (SIS II). Other topics discussed were the update of the catalogue with good practices as well as the common standards for solving problems in the Schengen Information System. The developments with regard to the incident reporting procedure as well as the increasing number of complaints from individuals submitted to the SIRENE National Bureaus were also discussed.

2. Participation in international conferences on data protection

In 2014, the CPDP continued its participation in European and international events in the field of data protection and privacy.

2.1. Conference of the data protection authorities from Central and Eastern Europe

Every year, knowledge, experience and ideas are exchanged during the conference with a view to establish cooperation and develop uniform action methods of data protection authorities in the region. The main topics discussed are the modernisation of the European legal framework on data protection, the exchange of information on national regulations and practices and the processing of large data volumes.

CPDP delivered a presentation at the conference dedicated to the provision of cloud services, the main risks to privacy in terms of processing large amounts of data, the new principles of data protection – by default, at design, at redesign of the system, and the principle of accountability, „the right to be forgotten“, „openness and transparency“ and basic questions and tasks that should be solved to ensure protection of personal data in the modern information society.

2.2. Meetings of representatives of the national data protection authorities on the implementation of Regulation 611/2013/EC concerning the measures applicable to the notification of security breaches of personal data under Directive 2002/58/EC on the right of privacy and electronic communications

The meetings discussed the work of Member States in implementing the provisions of Regulation 611/2013 as well as the establishment of a common form of notification and uniform assessment of violations in order to improve interaction between the parties, the interaction between data controllers, the processors, the citizens and the data protection authorities, the preparation of a list of appropriate technological protection measures, the links with other legal instruments, recent developments of the legislation on information and network security and the need for notification in case of incomprehensible or anonymised data.

2.3. European Conference of Data Protection Authorities

The focus of the Conference was the cooperation between the data protection authorities and the improvement of their collaboration. It also considered the current state of play of the European and international cooperation in the implementation of data protection, the expectations of data protection authorities, citizens and DCs and the vision for further development of the cooperation. The Handbook on European Data Protection Law published by the Council of Europe and the European Union Agency for Fundamental Rights was presented at the Conference. Resolutions were made on revision of Convention 108/81/EC on the protection of individuals with regard to automatic processing of personal data and on the accreditation of the data protection authority of Georgia as a member of the European Conference with the status of a European National Data Protection Authority.

2.4. 36th International Conference of Data Protection and Privacy

The motto of the 2014 conference was „A world order for data protection – is our dream coming true?“ where the unifying theme was the need for a consistent and efficient international data protection system.

Presented were the prospects of interconnected systems for data protection and improved technologies to enhance privacy. The synchronization of the rules for cross-border protection and the aspects of e-health were discussed, as well as the principle of „one-stop shop service“ and effective law enforcement.

The Conference adopted a Declaration on the Internet of Things and Resolutions on Privacy in the Digital Age, Big Data, Enforcement Cooperation and on accreditation of new members and observers. The Conference adopted also a model Global Cross-Border Enforcement Cooperation Agreement, which aims at the establishment of procedural rules to facilitate data protection authorities in exercising their powers of control and expedite the exchange of information between data protection authorities.

During the conference, the CPDP made a bid to host the 40th International Conference of Data Protection and Privacy, which will be held in the autumn of 2018. This will be the year of the Bulgarian Presidency of the Council of the European Union.

3. Regional cooperation with peer data protection authorities

During the reporting period, the CPDP partnered with the Data Protection Directorate of the Republic of Macedonia within the Instrument for Technical Assistance and Information Exchange (TAIEX), whose beneficiary is the Macedonian authority. The aim of the project is the exchange of legislative and practical experience between the two authorities, while

comparing their supervisory powers and discussing the possibility of building a coordinated approach to conducting joint operations in the field of cross-border data protection and to identify and overcome potential problems. The project looked at the prevailing economic presence of multinational companies which carry out continuous exchange of information as well as the incorporation of enhanced cooperation between supervisory authorities in the current data protection legislative reform.

The training programme included a presentation of powers and methodology of inspection, simulated check on a Bulgarian data controller with a branch in the Republic of Macedonia and assessment of joint control activities. The advantages and challenges of the bilateral cooperation were identified as part of the simulated check.

A cross-border case under which the two institutions were working was discussed during the visit, namely, an alert from a Bulgarian citizen who had been registered without his knowledge on a Macedonian employment website.

At the end of the meeting the parties reported good cooperation and exchanged working documents with analyses and recommendations.

4. Analysis of the state of play of the Data Protection Reform

In 2014, intensive work at expert level continued on the European Commission's proposals for a General Data Protection Regulation and for a Data Protection Directive in the field of police and criminal justice and for modernisation of Convention 108/81/CE.

4.1. Proposal for a General Data Protection Regulation (GDPR)

The proposal for a General Data Protection Regulation continues to be a serious legislative challenge in the European Union. The draft Regulation is being considered in parallel by the European Parliament and by the Council of EU and some issues are discussed also by the Working Party under Article 29 of Directive 95/46/EC. Currently, the texts of the Regulation are still in a draft form as the discussions continue. The main issues discussed in 2014 were related to the need for greater flexibility with regard to the processing of personal data by public authorities, the instruments proposed for transfer of data to third countries, the new mechanisms for cooperation between Member States, e.g. „one-stop shop" service, the role of national data protection supervisory authorities and of the future European Committee on data protection, the exceptions when processing data for statistical, archival, scientific, historical and journalistic purposes and others. The Bulgarian position is drawn up by the CPDP and the changes are discussed at expert level by the Working Group on Information

Exchange and Data Protection at the EU Council and at political level by the ministers of justice within the Justice and Home Affairs Council.

The CPDP expressed the following principle positions in the course of the discussions:

- With regard to the „one-stop shop service", the exact balance should be found between the proposed mechanism for „one-stop shop service", including the determination of a leading data protection authority and its cooperation with national data protection supervisors concerned in a case raised at the leading authority, achieving uniform application, legal security for citizens and less administrative burden for the data controllers based on saving time and resources in implementing the mechanism;

- The transfer of data to third countries should be governed by broad legal tools for data transfers to recipients in third countries through adequate solutions (territorial and sectoral), suitable safeguards (binding corporate rules, standard contractual clauses; codes of conduct, certification mechanisms, safeguards included in the administrative tools for the public sector) and derogations in strictly defined cases;

- As regards the scope of the proposed Regulation, it should include activities related to monitoring the behaviour of individuals and DCs established in third countries, when offering goods and services or when monitoring the behaviour of EU citizens and these activities are carried out on the EU territory;

- As regards the introduction of exceptions from some of the rights of the individuals in the processing of data for statistical, archival, scientific, historical and journalistic purposes, clearly formulated and defined exceptions should be adopted. In such cases, account should be taken of the need to achieve a balance between the right to privacy and data protection and other fundamental rights, and the existence of a serious public interest;

- With regard to the delegated acts[3] it is necessary to take account of their usefulness, as they are a suitable tool to ensure that the regulation is maintained up-to-date in the face of the new data protection challenges.

- As regards the responsibility of the controller and the processor, the text of the Regulation should lay down in a definite way the distribution of obligations, wherein the leading role of the data controller should be maintained, and the relations between the parties should be governed by a contract that contains clauses on data protection. The contract should

[3] Delegated act is a legally binding act of the European Commission to supplement or amend certain non-essential elements of a given legislative act. Delegated acts may be adopted in the form of regulations, directives and decisions.

also provide for the exercise of control by the competent supervisory authority on the controller and the data processor.

4.2. Proposal for a Police and Criminal Justice Data Protection Directive

In its position on the proposal for a Directive, the CPDP supports the view that ensuring coherence between the proposals for a Regulation and a Directive should not be at the expense of automatic transfer of provisions, taking into account the specific activities of the police authorities. Nevertheless, consistency should be achieved between the texts of the two acts where necessary. In drafting the provisions of the Directive a high level of protection should be ensured and it should not lead to lowering the already established standards and powers. There should not be obstacles to the free exercise of fundamental rights of individuals. The exercise of the right of access to information should follow the logic of the proposal for a General Data Protection Regulation. The right to change, delete and restrict data processing should be respected taking into account the specificity of police authorities. The practice of ex-ante consultation with the national supervisory authorities on data protection should be maintained.

4.3. Modernisation of Convention 108/81/CE

In 2014, proposed amendments to Convention 108/81/CE were discussed and endorsed at the meetings of the Interim Committee on Convention 108, where the CPDP also participated. The CPDP in-principle position is that maximum harmonization should be achieved between the new instruments available at EU level and those of the Council of Europe, while maintaining the overarching, neutral nature of the Convention. The meetings discussed amendments to the scope of the Convention aiming to achieve wider coverage. The emphasis was on the obligations of the parties to the Convention to ensure its effective implementation. Major open issues under discussion were the processing of special categories of data and data transfers to third countries, as well as exceptions from the rights of individuals with respect to data protection as well as the conditions of accession to the Convention.

XII. Administrative capacity and financial resources

1. Administrative capacity

In 2014, a change in the structure of the CPDP was made in conjunction with the functional analysis of the institution within the project **„Improvement of management, organisation and functions of the CPDP by carrying out a functional analysis.“** The Rules on the activity of the CPDP and its administration (RACPDPA) were amended and supplemented (SG No 46 of 3 June 2014), wherein the changes in the structure of the CPDP were in line with the recommendations made in the functional analysis.

The change is realised through the merger of four departments of the General Administration Directorate and the setting up of two departments. In addition, the functions performed so far by the specialised administration, but not typical of its operations, were transferred to the General Administration Directorate.

As a result of the structural changes, the coordination between the separate administrative units was improved and the time necessary to perform tasks and implement business processes was greatly reduced. Thus, at the end of 2014 the overall business management of the financial and material resources was optimised and made more efficient.

To keep the general to specialised administration ratio, the vacated managerial positions were converted to expert positions and were redirected to the directorates of the specialised administration. This was done to strengthen the existing capacity in those areas of the CPDP in which there is a shortage of expertise and a need for the recruitment of experts in the area of development, international activities, strategic planning and performance monitoring, as well as in activities related to strengthening the Commission’s control role.

The restructuring optimised the operations of the specialised administration also by inclusion of new activities relevant to each administrative structure, such as organisation of goal setting in the various units, monitoring and reporting on the results of the implementation of strategic documents.

During the reporting period nine recruitment competitions were announced to fill vacancies in the general and specialised administration of the CPDP. Five of these competition procedures ended with the appointment of 5 new employees under civil servant contracts. The remaining recruitments should be completed in early February 2015.

For the Commission for Personal Data Protection, staff training is an important element of the human resources management function. During the reported period priority was given to those training courses that would increase the work efficiency and contribute to the achievement of the CPDP's objectives.

In March 2014, an Annual Training Plan was drafted and approved with two main activities:

- Mandatory training – for staff appointed for the first time as civil servants – 1 newly recruited civil servant at expert position and 1 newly recruited employee at a managerial position were trained;
- Specialized training **–** for professional development and skilling. The Annual Plan provides for the training of 65 employees. Actually, 7 employees were engaged in the annual training plan for the reporting period. Participation in training was suspended due to imposed budget restrictions.

During the reporting period the main training provider to the Commission was the Institute of Public Administration (IPA) to the Council of Ministers.

In 2014, the CPDP continued the implementation of the awarded OPAC Project, Priority Axis: Human Resources Management, Sub-priority: Competent and Efficient Public Administration – „Promoting the professional development of the employees of the CPDP by applying a system of training according to their professional duties", project No CA 12 22 56 dated 9 April 2013 where 40 employees were involved during the reporting period.

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

- Management of occupational health and safety: 25 employees;
- Closing of accounts and taxation of budget entities for 2013: 1 employee;
- Law amending the Public Procurement Act – Analysis and Interpretation: 1 employee.

A total of **74** employees of the CPDP's administration participated in trainings for enhancing their qualification and professional development.

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

2. Public procurement

2.1. Public procurements related to the working environment of the CPDP in 2014

The following public procurement procedures were launched and carried out in 2014:

- 24/7 physical security of the building of the Commission for Personal Data Protection at No 2, Prof. Tsvetan Lazarov Str., Sofia;
- Supply and installation of 51 air-conditioners;
- 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 CPDP and the administration staff, as well as provision of additional travel-related services;
- Supply of fuel and accessories for the motor vehicles owned by the CPDP;
- Post-warranty subscription-based maintenance of the Commission's motor vehicles and supply of spare parts.

Irrespective of the amendments to the Public Procurement Act (PPA) dated 1 July 2014, the above public procurement procedures were carried out successfully and procurement contracts were awarded for 2014 and 2015. The files of the completed public procurements were completed and archived in accordance with the PPA and with the Internal Rules on the conditions and procedures for planning, preparation and carrying out of public procurement procedures of the CPDP.

Internal Rules for maintaining the „Buyer profile" in the CPDP were adopted in accordance with the amendments and the requirements of the LPPD related to public procurement and the implementing regulations of July 2014 and a current „Buyer profile" is maintained on the website of the institution.

2.2. Completed public procurement procedures under OPAC

In 2013, the Commission carried out public procurement procedures under the PPA through an open bid and public calls for the various projects, and the awarded contracts were finalised in 2014, namely:

- „Functional analysis of the CPDP administration", implemented under project No A12-11-9/06.02.2013 „Improving the management, organisation and functions of the Commission for Personal Data Protection by conducting a functional analysis", financed under Operational Programme „Administrative Capacity";

- „Provision of logistic services for events and development and delivery of training materials“ in relation to the implementation of the project „Improving the management, organisation and functions of the Commission for Personal Data Protection by conducting a functional analysis“.

- „Audit of the project activities“, carried out under project No A12-11-9/06.02.2013;

- „Training of trainers – build-on module“ under project „Promoting the professional development of the employees of the CPDP by applying a system of training in accordance with their professional duties“, OPAC grant contract CA 12-22-56/4.07.2013, Priority Axis II: Human Resources Management, Sub-priority 2.2. Competent and Efficient Public Administration, budget line BG051PO002/12/2.2-08;

- „Training of employees of Information Funds and Systems Directorate for administrators of Oracle database“, implemented under project „Strengthening the administrative capacity of the Commission for Personal Data Protection for working with databases, information systems and team work“, OPAC grant contract CA 12-22-57/4.07.2013, Priority Axis II Human Resources Management, sub-priority 2.2. Competent and Efficient Public Administration, budget line BG051PO002/12/2.2-08;

- „Training of employees of „Register and Archive“ Department in Information Funds and Systems Directorate for work team and achievement of team goals“, implemented under project „Strengthening the administrative capacity of the Commission for Personal Data Protection for working with databases, information systems and team work“, OPAC grant contract CA 12-22-57/4.07.2013;

- „Provision of information and publicity services“ in relation to the implementation of project „Strengthening the administrative capacity of the Commission for Personal Data Protection for working with databases, information systems and team work“, OPAC grant contract No CA12-22-57/04.02.2013.

2.3. Organising and conducting procurement procedures in 2014 with regard to the new projects approved under OPAC

In relation to project entitled **„ Improving and expanding the electronic services to businesses and individuals provided by the CPDP, and integrating them with the Single point of access to administrative e-services“**, grant contract No 13-32-13/11.02.2014, 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, procurement procedures were carried out under Article 14(4)(2), under the terms and provisions of Chapter 8A of PPA with the following subject-matter:

- Develop a toolbox to assess the level of impact, to determine measures for data protection by data controllers and to conduct inspections by the CPDP;
- Information and publicity;
- Audit.

The procurement procedure was completed successfully in 2014.

In relation to the approved project **„Improving the qualification and building on skills and competencies of the CPDP staff for more effective and efficient performance of their duties“** as per grant contract concluded between the Ministry of Finance, OPAC Managing Authority – OPAC Directorate and the CPDP for implementation of this OPAC project co-financed by the European Union through the European Social Fund, Priority Axis II: Human Resources Management, sub-priority 2.2, a successful procedure was carried out under Article 14(4)(2), pursuant to the provisions of Chapter 8A of PPA for „Information and publicity“.

3. State of play of the implemented information and communication systems in the CPDP in 2014

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 implemented automated system for conducting paperless meetings, electronic document management system and task tracking system contribute to more effective operation and functioning of the CPDP.

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

The CPDP continues its participation in Working Group 31 „Digital Bulgaria 2015“ under the Ministry of Transport, Information Technology and Communications.

4. Financial resources - general information on budget spending of the CPDP for 2014

In accordance with the Law for the State Budget of the Republic of Bulgaria (LSBRB) for 2014 and Council of Ministers Decree No 3 dated 15 January 2014 on the implementation of the state budget of the Republic of Bulgaria for 2014, the initially approved operating budget of the CPDP was BGN 2,373,000.

During the year the budget of the Commission was reduced by BGN 113,000 pursuant to § 3, point 2 of the Law amending the Law on the budget of National Health Insurance Fund for 2014 (SG No 67 of 12.08.2014).

After these adjustments the budget of the CPDP amounted to BGN 2,260,000.

The operational expenditures of Commission for Personal Data Protection and its administration amount to BGN 2,239,111, or 99.08 % of the approved estimates for the year. The types of costs distributed by headings of the Unified Budget Classification (EBK) 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	1 036 618
02-00	Other remunerations and staff payments	138 336
05-00	Mandatory social insurance contributions paid by employers	269 248
10-00	Maintenance	667 357
19-00	Taxes, fees and administrative sanctions paid	9 898
52-00	Acquisition of long-term tangible assets	117 654
	Total budget expenditures	2 239 111

XIII. CPDP Goals and priorities in 2015

A strategic objective of the Bulgarian government is the introduction of comprehensive administrative services across all public administrations in 2015. The basic model of integrated administrative services complements and builds on the model for „one-stop shop“ administrative services. This process will inevitably influence the activity of the CPDP in terms of improvement and expansion of its electronic services provided to businesses and individuals, and their integration in the Single point of access to administrative e-services.

Taking account of the experience gained in the field of control activities and with the aim to establish conditions for uniform application of the data protection rules by DCs performing similar activities, the CPDP relies on changing the approach for selection of DCs for inclusion in the annual inspection plans and focuses on the conduct of sectoral inspections. A leading criterion in selecting the sectors of social and economic life, which will be subject to checks, is the processing of personal data of extremely large number of individuals (for example in the Education and/or Health sectors).

In continuation of its policy of raising public awareness on data protection issues, the vulnerable groups in society remain in the focus of the CPDP. In the coming period, the CPDP will build on the activity, already implemented in 2012, for protection of personal data of children and adolescents by directing efforts towards synergies with partner institutions and stakeholders. Early prevention among vulnerable groups is a reliable guarantee for the successful exercise of the right of protection of personal data and prevention of its misuse.

The focus of the CPDP in 2015 is the identified need for legislative changes in electoral law in order to define clearly the obligations of all actors in the electoral process and ensure adequate protection of personal data of voters.

Given the managerial positions taken up in data protection authorities at EU level in 2015, the CPDP will 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.

An essential international focus of the CPDP remains the preparation of the institution to implement the new legal framework on data protection, which, after three years of

discussion, is in its final stage. In 2015 the main efforts will be aimed at creating the necessary preconditions for the introduction of the new European requirements at national level both in respect to a wide range of DC as well as to specific sectors such as Police and Justice. An important factor for the successful preparation of the country for introduction of the new, higher data protection standards, is advanced professional training and specialised expertise of the CPDP administration. The CPDP will continue investing in this area.

Another priority related to the upcoming finalisation of the European reform, which remains high in the agenda of the CPDP, is the introduction of a new figure in the Bulgarian legislation, namely the data protection officer (DPO), respectively DPO training by the CPDP. The mandatory introduction of such a figure will significantly strengthen the right to protection of personal data and will contribute to the full functioning of the data protection system in Bulgaria.

The CPDP will also continue to contribute actively to the achievement of another major priority of the Republic of Bulgaria – full accession to the Schengen Area.

The Annual Report of the Commission for Personal Data Protection for its activities in 2014 was adopted by a Decision of the Commission at a meeting held on 22 January 2015 (Protocol No 4).

CHAIRPERSON:	MEMBERS:
Ventsislav Karadjov (signed)	**Tzanko Tzolov (signed)**
	Tsvetelin Sofroniev (signed)
	Mariya Mateva (signed)
	Veselin Tselkov (signed)