REPUBLIC OF BULGARIA

COMMISSION FOR PERSONAL DATA

A N N U A L R E P O R T

of the Commission for Personal Data Protection

for 2013

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

TABLE OF CONTENTS

I. Introduction

The Annual Report of the Commission for Personal Data Protection (CPDP) is prepared pursuant Art. 7 (6) of the Law for Protection of Personal Data (LPPD) and covers the period from 01.01.2013 to 31.12.2013.

The Report contains an analysis of the achievement of CPDP priorities for 2013. It consecutively analyses the powers of the institution, data controllers' registration and data registers kept by them; statistics on the complaints filed under LPPD and the Commission's supervisory activity, as well as an analysis on the issued opinions and statistics on the requests for personal data transfers authorization, and the access provided to public information.

The Commission's administrative capacity and financial status during 2013 are also reported.

The report also addresses the information activities and public relations activities of CPDP; the implemented information and communication technology; training conducted and implementation of projects funded by European programs.

II. Analysis and report on the fulfilment of the Commission for Personal Data Protection priorities, set out in the 2012 Annual Report

An extremely important focus of the Commission for Personal Data Protection for 2013 is the increased participation in specialized working groups of the European Union and the Council of Europe, involved in the preparation of amendments to the existing privacy and personal data protection legal framework. The coordination of the new legislative proposal continues at this moment due to the principal nature of the reform and the importance of the planned amendments to the legislation.

Beeing part of the debate, CPDP expresses its principal position that the priority areas are the following: introduction of the "one stop shop" principle; extension of the scope of the international personal data transfers; the coordination and cooperation mechanism between the national supervisory authorities; enhancing the role of the national data protection supervisory authorities and the European Data Protection Board. Despite the ambitions of the Vice-President of the European Commission Viviane Reding for the successful finalization of the ongoing reform in late 2012 or 2013, the debate on the proposal for a new legislative package is expected to continue in the first half of 2014.

The introduction of the position of the data protection officer is an essential element of the reform proposed by EC in the data protection field. In order to prepare for its successful implementation in Bulgaria, when carrying out training on personal data protection, CPDP focuses on the forthcoming introduction of this position and its binding nature. The Commission's experience in conducting training of data controllers guarantees the Commission's preparedness for training data protection officers after the entry into force of the regulation that would impose their compulsory institutionalization.

The analysis of the practice and legislation of related data protection supervisory authorities shows that the CPDP powers to enter into agreements in the

field of personal data protection has no analogue in other countries. This uniqueness, however, is a legal impediment to legally bind the bilateral relations of the Commission with other EU supervisory authorities. The fact that the European supervisory authorities are not legally allowed to enter into international agreements regarding matters within their competence is an objective obstacle for CPDP to effectively exercise in practice these particular powers of the Commission. In this regard, during the reporting period, CPDP has not received requests for entering into agreements sent by similar European institutions, despite the Commission's stated willingness and readiness to establish formal legal relationship with them.

The process of moving the Commission for Personal Data Protection to a new building is to be finalized. This is the main technical reason preventing the expansion of European Union internal electronic network via setting up a contact point in CPDP.

III. Powers of the Commission for Personal Data Protection:

1. Pursuant to the Law for Protection of Personal Data

As the only public authority whose main task is to ensure privacy and personal data protection, the Commission for Personal Data Protection has diverse tools for impact. The main activities of the Commission can be grouped into two areas: adequate prevention and effective control.

Preventive activities are carried out through coordinating and expressing opinions on draft laws and regulations concering the personal data processing; issuing regulations on the personal data protection; direct involvement in the preparation of European and international data protection policies via participation in various international forums; conducting training of data controllers in the field of personal data protection and expression of opinions on various issues in accordance with the Commission's competence; keeping a register of data controllers.

The Commission exercises effective control by carrying out inspections of data controllers processing personal data; application of an authorization regime for third countries data transfers; issuance of compulsory instructions to data controllers; imposing a temporary ban on the personal data processing and administrative sanctions.

2. Pursuant to the Law on Electronic Communications

Processing of personal data in the electronic communications sector is considered risky by experts in the personal data protection field. As such, it is subject to further regulation. The national, respectively the European legislator periodically introduces specific duties and additional requirements to all entities that process personal data in the electronic communications sector.

Pursuant to Art. 261a of the Law on Electronic Communications, the Commission is designated by the Bulgarian legislator as the monitoring authority

on the security of traffic data stored by enterprises that provide public electronic communication networks and/or services. For this purpose, it supervises the operation of these providers in order to ensure the compliance with certain data retention rules to ensure data protection and security.

After analysing and summarizing the statistics of the liable enterprises, the Commission annually submits a summary to the attention of the National Assembly and the European Commission on: the total number of liable enterprises which have provided statistical information, the authorities which have requested access to traffic data, the service nature, and the data retention period.

During the reporting period there is a significant growth in the number of enterprises that have submitted information to the Commission in 2013, compared to the previous two years. It is noteworthy that in 2013 no enterprises have failed to comply with the instructions of the Commission regarding data submission form which allows for more efficient data analysis and summary. Significantly reduced is the number of unlawful access requests by the competent authorities, which is a result, achieved with the 2012 Commission's guidelines on the standardization of the procedures for request of information,

In its 2012 report, presented to the National Assembly, deposited on 30 May 2013, the Commission presented a detailed analysis of the on-going development of the process of requesting and providing access to traffic data and has identified the relevant trends.

IV. Exercise of the rights of individuals

In 2013, the Commission was approached with different types of inquiries by individuals. Not all inquiries from individuals can be united under a common indicator. Some of the inquiries, however, refer to a wide range of third parties; therefore in this analysis we focus on them.

1. Pursuant to the Law for Protection of Personal Data

1.1. New technology

With the advance of technology in all spheres of public and private life more and more individuals and data controllers raise issues relating to the permissible and lawful use of biometric data. In this regard, the Commission was asked about the possibility the employer to dismiss any employee if he/she refuses to provide fingerprints. The Commission has clarified that in the absence of any of the conditions set out under Art. 4 (1) of LPPD regarding the lawfulness of the processing of personal data of individuals, including biometric, the only legal option for an employer to lawfully processed personal data remains the consent of the affected person. Regarding challenging the legality of the terminated employment, the employee is entitled to challenge the legality of the dismissal before the employer or the court.

More often CPDP is approached with issued regarding the use of biometric data for access control in mass events or to public buildings (music concerts, school buildings, enterprises). Commission ruled that when it comes to processing personal data of students, and especially students aged below 18, the explicit consent of their parents is mandatory.

Given the expansion of video surveillance as a means of controlling access to residential buildings, in its practice, the Commission provides specific guidance on the legal implementation. The Commission accepts that under certain conditions video surveillance constitutes a "personal data processing" for the purpose of storing them in a "personal data register" within the meaning of §1 (1)

and (2) of the Additional Provisions of LPPD; however, according to Art. 1 (9) of LPPD it shall not apply to personal data processing carried out by individuals for their personal or domestic activities, such as video surveillance in common areas of the property – residential buildings in a condominium. In general, the regulation of the use of the common areas and the adjacent areas in a condominium is within the powers of the General Meeting of the respective condominium. The rules of its convening, decision-making and decision-implementation are governed by the Law on Condominium Management. Any owner may request annulment of unlawful decisions of the General Meeting before the district court at the location of the condominium.

In general, when carrying out video surveillance, data controllers are bound to comply with the regulatory requirements governing their operation and to declare a separate CCTV Register in the Register of Data Controllers and Registers Kept by Them with CPDP. It is imperative that visitors in a building subject to video surveillance be informed by means of information boards placed prominently on the use of technical means for monitoring and control of the site, without specifying their location, as well as the respective data controller's contact data. In case the visitors have not objected to the data controller for the processing of their personal data, it is assumed that they have given their consent within the meaning of LPPD for the processing of their personal data using technical means of video control.

Another important duty of data controllers concerning the rights of individuals is to provide public access of individuals to their personal data which have been processed (including videos surveillance records). In cases when the exercise of the individual's right of access results in the disclosure of a third party personal data, the data controller should provide the individuals with this data which refers only to them. For this purpose the data controller should take appropriate technical measures for deletion/masking images of other persons subject to video surveillance. In the absence of such technical capacity, the access

to video surveillance records can only be provided with the consent of all persons subject to that video surveillance.

CPDP clearly states its position that at work the installation of video surveillance equipment in the staff's rest rooms and sanitary facilities is inadmissible.

The privacy and protection of the employees' dignity are fundamental values that the employer should respect during the performance of tasks under contract.

The rapid development of technology largely allows the exchange of information between individuals in the web. This leads to problems in personal data processing in such environment. Many of the issues raised by individuals before CPDP in the past year were related to social networks, including participation in forums and the profiles created for that person containing personal data, access to specific forums, and deletion of profiles. The number of complaints of individuals for theft of e-mail accounts and password-cracking is increasing. Theft of email accounts is one of the most common Internet frauds today. It is dangerous because the stolen e-mail account can be used to comit a number of crimes related to identity theft, lottery fraud, etc. By stealing the e-mail account the perpetrator gets full access to the address book with data for close friends and important personal correspondence, data providing access to other registrations, personal information, bank accounts, etc. As far as it concerns computer crime, in such cases the Commission recommends that the affected persons should approach the Directorate for Combating Organized Crime at the Ministry of Interior.

1.2. Personal data processing in the context of employment

A lot of issues in the past year were related to the relationship between employers and their employees, involving personal data processing, such as: keeping a copy of the employee's identity card for the purposes of the company's financial accounting activities and the presentation of a copy of the identity card during job interviews.

Although the law on employment still fails to adequately reflect the personal data protection issues, the position of CPDP is based on the analysis of the existing regulations. The employers (at the same time acting as data controllers) are required to keep records of the employee's personal employment file for 50 years for the pension insurance purpose, but these should not include an employee's identitiy card copy. The employers, however, are not allowed to copy the employee's identity card, but only to record the data contained thereon and then to return it to the its holder.

It is common nowadays for the individuals when searching job to make registration on job search websites. The Commission was approached by a Bulgarian citizen who has received an offer from a foreign website offering work. The person claims that he has never filled his personal information to that website. In this regard, the Commission for Personal Data Protection has approached with a request for assistance and verification with the data protection supervisory authority in the relevant country.

CPDP frequently receives inquiries in connection with the requiring of cusomer's Personal Number by courier companies when sending/receiving goods with payment in cash on delivery. The Commission's position in this case was based on the accounting of that service as a basis for the eligibility of that personal data processing under the provisions of the Accounting Act, which define the mandatory requisites of each primary accounting document containing personal data. The identification of individuals who are not registered with the Commercial Register or the BULSTAT Register is generally made by the respective personal identification number or the personal number of foreigners.

1.3. Processing of personal data for artistic and literary purposes

A very interesting issue, presented to CPDP in the past year, concerns the study of the system of personal names in the region of the town of Ruse for the period 1830-1970. Although the publication of personal data in literary materials in

the form of birth certificates would be considered personal data processing for literary and artistic purposes, the Commission ruled that the publication of a birth certificate can be done only at the presence of one of the conditions stipulated under Art. 4 of LPPD and in compliance with the provisions of the Civil Registration Act. This effectively limits the range of persons who may have access to data from the birth certificates. Regarding the publication of the birth certificates, it should be done after obtaining the explicit and unambiguous consent of the persons or their heirs.

1.4. Other important issues raised by individuals

During the reporting period the Commission received inquiries regarding the lawful processing of personal data in connection with the transfer of outstanding and overdue payments from the creditor to a third party. The Commission explained the legal possibility for the lawfulness of the processing of data in connection with the conclusion of cession agreements. It also explained the option allowing for transfer of data to a data processor and the conditions and circumstances under which it could be implemented legally.

Offen in the commercial practice commercial dicounts are provided by major commercial chains after “customer card” or “loyalty card” or “discount card” has been issued under certain conditions. In order to issue such cards some shops or individual traders collect and process various personal data – names, address, e-mail address, telephone, etc. CPDP received a number of inquiries on the admissibility of such processing and how it complies with the LPPD’s provisions. The lawful personal data processing requires the compliance with at least one of the conditions referred to under Art. 4 (1) of LPPD on the eligibility of data processing and applicable in this case is the condition under item 2 – the natural person to whom the data relate should have given their explicit consent. The Commission considered that when making a purchase and using preferences related to the that purchase from a particular retailer /trade chain/, the individual

enters into informal contractual relationship with the retailer, which in turn implies the existence of a condition of eligibility of data processing under Art. 4 (1) (3) of LPPD, namely: the processing is necessary for the performance of duties under a contract, in which the individual to whom the data relate is a party, and for the performance of actions prior to the conclusion of the contract, undertaken upon the request of the person. Trader retailer needs data to be able to uniquely identify their counterparties.

2. Under the Access to the Public Information Act (APIA):

The procedure of examination of application for access to public information is carried out under the Access to Public Information Act. CPDP provides information as a liable subject under this law and gives individuals a possibility to aknowledge themselves with its activities.

The Chairperson of CPDP informs the public about the Commission's work by publishing information on the Commission's website or announcing information in another form (brochures, information boards, publications in mass media, etc.).

The Chairperson of CPDP decides on the received application for access to public information.

For the specified period the Commission received 5 applications for access to public information. In most applications for access to information the applicant has requested information on more than one sphere of activity of the Commission, and therefore the Chairperson of CPDP ruled on any of the requests by issuing a separate decision within the statutory period (total of 60 decisions). The requested access to public information concerned the following issues: number of complaints received in the Commission, number of administrative penalties imposed; total amount of penalties imposed by the Commission; number of acts repealed before the court; documents on administrative proceedings brought before CPDP; amount of remuneration of the Chairperson of CPDP and the administrative officials; etc.

In the majority of the decisions the access to public information was refused, because the applicant has requested access to documents without considering the fact that the procedure to access them is regulated under the provisions of the Administrative Procedure Code (APC), not under LAPI. At this point there are no repeals of the decisions refusing access to public information.

V. Registration of data controllers and data registers kept by them. State of deployed information and communication systems. Volume of incoming and outgoing correspondence.

1. Registration of data controllers and data registers kept by them

Following its legal obligation the Commission for Personal Data Protection maintains a register of data controllers (DC) and data registers kept by them (Register). The Register is public and is kept electronically.

The overall activity involved in maintaining the Register at CPDP is in accordance with the concept of e-Government aiming to provide individuals with highly effective and easy to use electronic service, built on the "one stop shop" technology. It was implemented based on the data controllers' electronic registration system (eRALD).

eRALD is a web-based application which covers all activities related to the data controllers' registration and tracks out the technological process until approval or denial of their entry in the public register. The system enables the maintenance of public registers for: registered data controllers, data controllers exempted from the registration obligation and data controllers with refused entry in the CPDP's Register. All three registers and the information contained therein are public and available on the web through the CPDP's website.

There is a trend for wider use of the electronic registration service by data controllers. The Commission associates this with the convenient and accessible working interface of the system and the training held with key data controllers.

In 2013, the processes of registration of data controllers (DCs), exemption from the registration obligation, update of the information on a controller already existing in the register, as well as DC deletion from the register continued.

As of 31 December 2012 the total number of eRALD users reached 316,993, with 287,025 submitting applications for registration as data controllers, and

29,968 submitting applications for exemption from the registration obligation (Fig. 1).

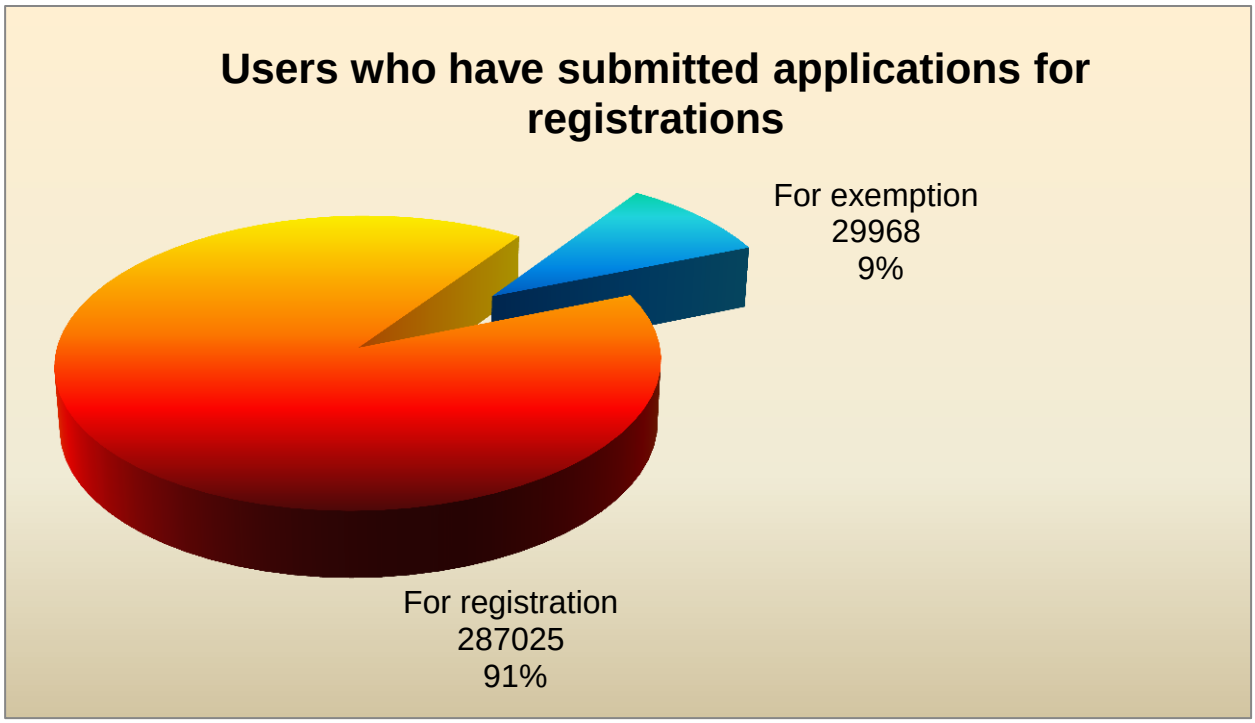

Fig. 1.

In 2013 the Commission took decisions to register 42,308 data controllers. Thus the total number of data controllers in the register reached 246,382 (Fig. 2).

The number of data controllers exempted from the registration obligation in the accounting period was 498. Thus, the total number of data controllers exempted from registration was 27,351 (Fig. 3). Compared to 2012, there is a decreasing trend in the number of submitted applications for registration exemption and an increasing trend in the number of applications for data controllers' registration.

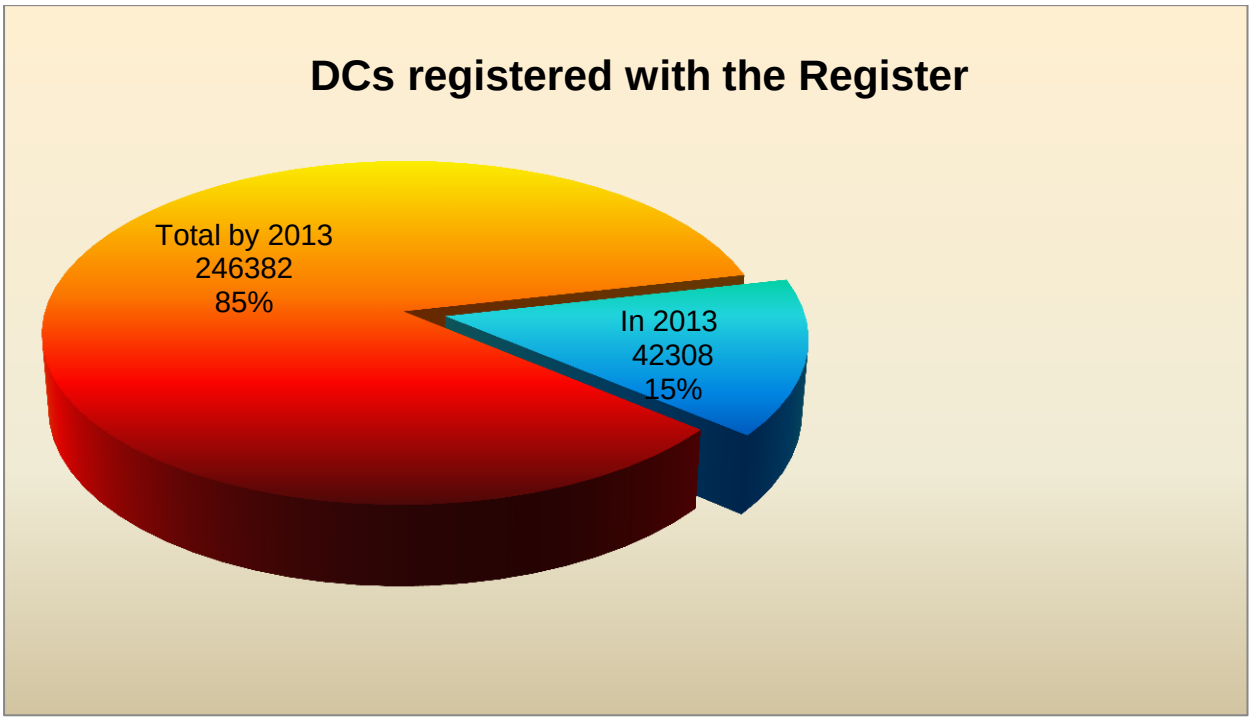

Fig. 2.

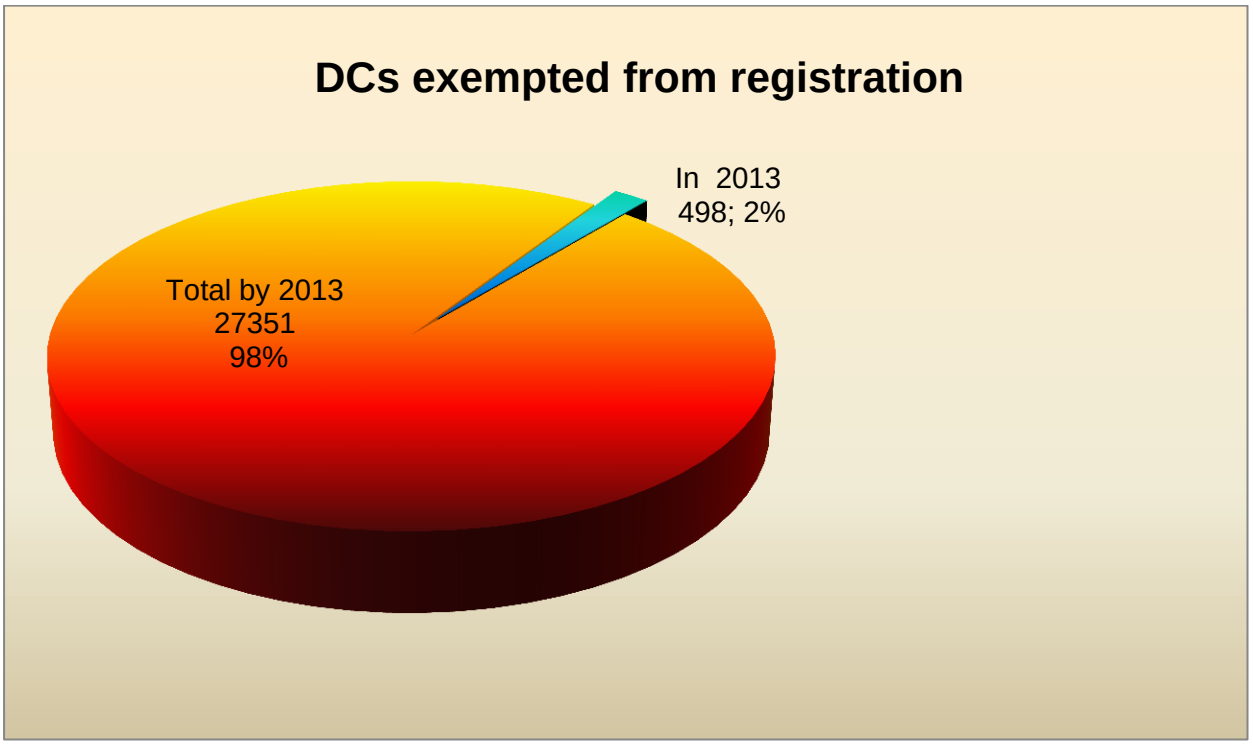

Fig. 3.

During the reporting period the Commission received 93 applications for data controllers' deletion on which CPDP decides to delete the data controllers from the register.

When a data controller applies for data processing under Art. 5 (1) of LPPD or for data, the processing of which by decision of the Commission poses a threat to the rights and the lawful interests of individuals, the Commission is required to carry out ex-ante inspection, pursuant to Art. 17b of LPPD before the registration.

In 2013, 2,748 data controllers were subject of ex-ante inspection before the registration in the register under Art. 10 (1) (2).

In 2013, pursuant to Art. 17b (3) (3) of LPPD, the Commission decided to refuse the entry of 829 controllers in the register.

In the reported period, in connection with data controllers' registration were processed 45,147 documents, submitted on hard copies. 91,170 electronic messages were sent to data controllers via eRALD, and 372 e-mails were received in the electronic system inbox, which resulted in appropriate actions been undertaken.

2. State of the deployed information and communication systems

During the reporting period the information and communication infrastructure of CPDP was further refined and therefore currently the Commission for Personal Data Protection employs modern means of data communication and exchange.

The Commission's Center Information and Contact with Individuals has so far been successfully working for three years.

The effectiveness of the activities of CPDP is assisted by the automated system for conducting paperless meetings implemented in the administration.

The Commission's website is actively maintained and regularly updated for the wider public. News and valuable information for citizens and data controller are posted on it, CPDP practice is promoted and also the views and opinions expressed on personal data protection issues.

The most important information is synthesized and posted in the electronic newsletter of the Commission issued every two months.

During the reporting period the Commission continued its cooperation with the Executive Agency "Electronic Communications Networks and Information Systems", which is responsible for GovCERT Bulgaria (National Center for Action by Information Security Incidents).

In 2013, the Commission continued its participation in the work of the 31 Working Group "Digital Bulgaria 2015" of the Ministry of Transport, Information Technology and Communications.

3. Volume of incoming and outgoing correspondence within the period from 1 January 2013 to 31 December 2013:

Incoming correspondence - 6,974;

Outgoing correspondence - 4,367;

Internal correspondence - 2,433;

Re-qualified – 19;

Complaints received - 550.

VI. Analysis and statistics of complaints and requests submitted under Art. 38 (1) of LPPD. Case law and practice of the Commission. Analysis of judicial practice.

1. Comparative analysis of complaints by type of data controllers, received at CPDP in previous years and the reporting year; key areas of public life to which refer the most common violences in the field of data protection.

Following the Commission for Personal Data Protection power to consider complaints against acts and actions of data controllers which violate the individuals' rights under the Law for Protection of Personal Data, as well as complaints of third parties in connection with their rights under the same law, in the reporting period the Commission received 550 complaints, signals and inquiries concerning personal data processing and the possibilities for exercising the rights of protection in case of unlawful personal data processing or concerning the rights of access, information, correction or personal data blocking.

For comparison, in 2012 the Commission received 548 complaints, signals and inquiries, in 2011 they were 458, and in 2010 they were 221 respectively.

For 288 requests for information about the procedures for protecting the individuals' rights, detailed answers to the asked questions were prepared and sent.

During year the Commission has issued 252 decisions on proceedings following complaints with alleged violations of individuals' rights, as follows:

1. on complaints' lawfulness - 80 decisions;

2. for terminating administrative proceedings due to the presence of another proceeding initiated before the authorities of the Ministry of Interior or the Prosecution Office - 20 decisions;

3. on complaints' inadmissibility - 32 decisions;

4. on irregularity of complaints and requests - 31 decisions;

5. on renewed administrative proceedings - 2 decisions.

6. for approving agreements reached by and between parties in administrative proceedings - 2 decisions.

The Commission considered 85 complaints as ungrounded due to a lack of violation of the personal data processing rules and of the claimants' rights.

From the administrative proceedings ended due to inadmissibility of the complaints, 16 have been withdrawn by the claimants, thus, the Commission was actually required to decline jurisdiction.

On 80 of the concluded in 2013 administrative proceedings, the Commission has considered the complaints as admissible and as result of its decisions were issued 7 compulsory instructions to personal data controllers with which was instructed personal data protection measures and actions and has established a total of 83 administrative violations of the Law for Protection of Personal Data and imposed sanctions and fines in the amount of BGN 503 300.

The violations committed by data controllers may be classified in the following groups:

- personal data processing in violation of the principles of lawfulness, proportionality of the personal data processed, the principle of processing personal data for specific, precise and legitimate purposes (Art. 2 (2) of LPPD) - 15 violences.

- personal data processing without a statutory requirement for admissibility of the personal data processing being present (Art. 4 of LPPD) - 20 violations, for which property sanctions were imposed.

- personal data processing, without data controllers having taken technical and organizational measures to protect data against accidental or unlawful destruction or accidental loss and against unauthorized access, rectification or dissemination, and against other illegal forms of processing (Art. 23 of LPPD) - 19 violences, for which property sanctions were imposed.

- personal data processing, before the controller has submitted an application for registration with the Register of Data Controllers and Registers kept by them maintained by the Commission (Art. 17 of LPPD) - 3 violences for which property sanctions and fines were imposed.

- personal data processing for marketing purposes without providing the individual with the possibility to object to the processing of their personal data for the specified purposes (Art. 34a of LPPD) - 5 violences for which a property sanctions were imposed.

- for data controller's refusal to assist the Commission in the exercise of its supervisory powers (Art. 22 (5) of LPPD) - 4 violences for which property sanctions were imposed.

- for failure of the obligation of the data controller to decide on applications for access to personal data, the Commission has ascertained two violations.

- for violence of Art. 18 (3) of LPPD, namely for not declaring CCTV Register, the Commission has ascertained that in 2013 there were 4 violations.

Legal advisor's remuneration in the amount of BGN 3,375 was adjudicated for CPDP benefit with BGN 1,500 paid voluntarily.

In 2013, the Commission reported income from administrative penalties under enforced decisions of the Commission for Personal Data Protection in the amount of BGN 185,875, of which BGN 99,775 paid voluntarily by the offenders and BGN 86,100 were forwarded to the NRA after their compulsory collection.

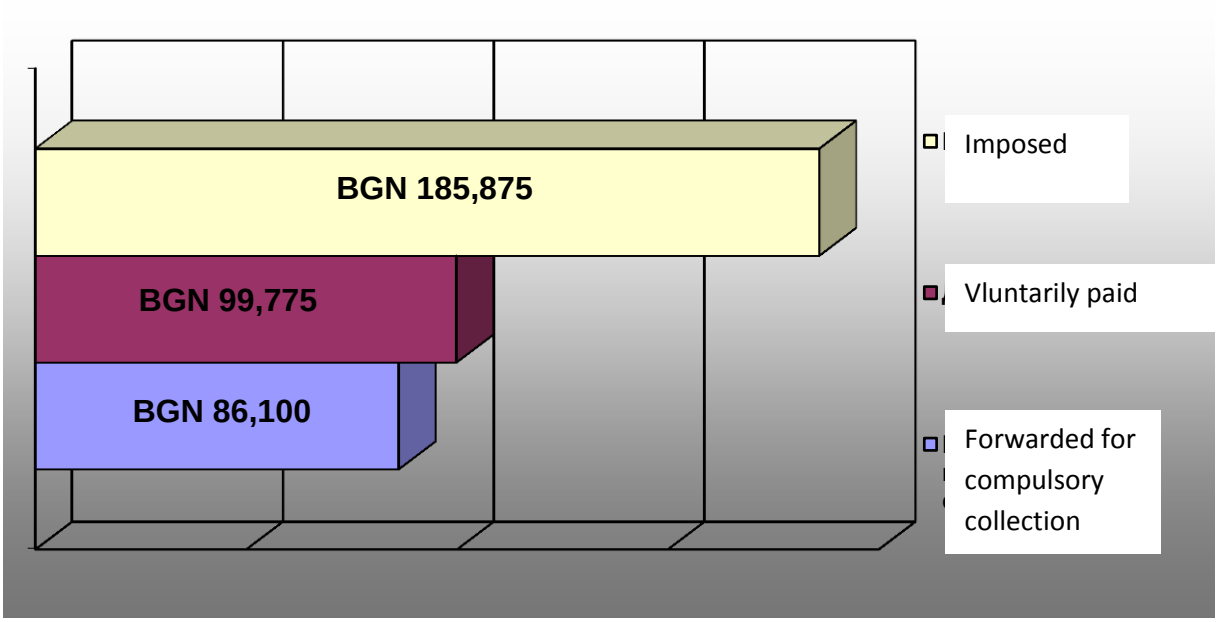

Fig. 4.

The sectors of the data controllers' activities against which most of the complaints have been submitted by individuals in 2013 are as follows:

Telecommunications	333 complaints
Labour and Social Insurance Services	42 complaints
Banks and Banking Institutions	33 complaints
Health Care and Education	13 complaints
Condominium Management	11 complaints
Judicial and Executive System	10 complaints
Media	8 complaints

Case law and practice of the Commission

The Commission for Personal Data Protection has been approached for unlawful actions regarding personal data disclosure by Natsionalna Elektricheska Kompania EAD. The complaint indicated that the individual in his capacity as manager of a company has entered into a contract for the purchase of electricity with Natsionalna Elektricheska Kompania EAD (NEK). NEK notified the

company of its intention to launch a procedure for public disclosure by publishing all existing contracts for power purchase entered into by and between NEK and its counterparties, providing a 7-day period to express consent or disagreement for such public disclosure of contracts. The claimant raised the issue on the necessity and purpose of the public disclosure of existing contracts, and principle approval was given for public disclosure of the contract between the company and NEK for the purpose of achieving transparent and mutually balanced approach to conduct business. NEK confirmed that the only reason for public disclosure of contracts for purchase, sale and transmission of electricity is to achieve transparency in the operation of the state-owned company. As a result of the actions of NEK, the Ministry of Economy and Energy published on its website the claimant's personal data in his capacity as the manager of the company.

The opinion of the Commission is that this action violates the provisions of Art. 23 (1) of LPPD, according to which: "the data controller should take appropriate technical and organizational measures to protect the data against accidental or unlawful destruction or accidental loss, unauthorized access, modification or disclosure and against other unlawful forms of processing". Regarding the publication of the contract on the website of the Ministry of Economy and Energy with undeleted personal data (name and surnames, Personal Number, ID card) of the claimant in his capacity of the manager of the company which is a party under the specified contract concluded with NEK, the data controller failed to take appropriate technical and organizational measures to protect data from illegal distribution. In the case the DC was imposed a property sanction of BGN 1,000.

In another case, the Commission was approached for violations made by a consumer cooperative. The complaint stated that each year the cooperative sends invitations for its annual meeting to its members with indicated address and personal number without enclosing them in envelopes and thus disclosing their personal data. In support of the above, the complaint enclosed an invitation for the

annual general meeting of the cooperative as evidence, which demonstrated that the claimant is identified by full name, address and personal number.

In comparison, based on the relevant provisions of the legally required amount of information for the members and prospective members of the cooperative and the content of the information included in the invitation by its management body, the Commission rules on the existence of excessiveness of data processing in the invitation, taking into account the entering of individuals' personal numbers. Relevant here is the provision of Art. 2 (3) of LPPD, under which personal data must be relevant, related and not excessive for the purposes for which they are processed.

In connection with the subject of the complaint – sending the invitation by the management body of the cooperative to cooperative members with designated personal number and address without placing them in envelopes and thus disclosing personal data – this act violates he provisions of Art. 23 of LPPD.

In this case, the Commission imposed an administrative penalty in the amount of BGN 600 for the violation of Art. 23 (1) of LPPD and issued a compulsory instruction for compliance with the provisions of LPPD in conjunction with Art. 8 (5) of the Law on Cooperatives, namely: deletion of the personal number of the cooperative members entered in the Book of Cooperative Members and sending invitations to the general meeting in a sealed envelope without designating the personal number of the receivers.

In late 2012 and early 2013, the Commission received a number of complaints from various individuals against a data controller with a specific subject of the complaints.

The complaint stated that in relation to cases brought in the Regional Department of the Ministry of Interior /RD of MoI/ the claimants were duly summoned for reference. They were informed that they were summoned because of a complaint filed against them by a company manager. The complaints filed against these individuals stated that after making various statements the head of the

respective RD of MoI has requested that some persons, including the claimants, should be notified about the complaint and they were identified by their full names and personal number following the procedure set in Art. 56 of the Ministry of Interior Act.

They also claimed that the respective complaints enclosed their photographs "taken a few days earlier on a lane in protected areas – public municipal property" without their knowledge and consent.

The claimants informed that they "had never entered into any relationship with the manager of the company, nor had provided or given permission for the processing of their personal data".

In turn, the data controller clarified that the claimants' personal data were collected from the Commercial Register, legal informational databases and Internet. In its opinion, the company stated that although the complaint claimed that its authors had never entered into contractual relations and had not provided their personal data to the company, "the specified circumstances alone, as specified by the claimants, does not constitute a violation". Basis for this argument is the opinion that since "the claimants have provided their personal data on the web completely voluntary and thus made them accessible to a wide range of individuals – in fact to everyone with access to the global network", then "the provision and receipt of such data is made with the explicit knowledge of the claimants".

The representative of the company informed that exactly in this way, through the web, he found these personal data (full name, personal number) of the claimants. He also specified that "the claimants are members of the governing bodies of various capital companies registered with the Commercial Register, respectively with the Apis Register+" and attached evidence to confirm this fact.

After clarifying the facts and circumstances of the case, the Commission ruled that there is a violation in the processing of personal data of the claimants for the purposes of initiating proceedings before the Ministry of Interior.

It also stated that the purposes for which the data are processed in the Commercial Register are different from the purpose for which the company processed the personal data of the claimants. In this respect the Commission does not share the view that the claimants have initially given their consent for processing of their personal data regarding further processing with a different purpose.

The Commission received a complaint alleging that the Regional Inspectorate of Environment and Water (RIEW) without requesting the prior consent of the individual published the individual's personal data – full name, personal number and full address – on the Internet. The claimant stated that the publication was made by disclosing on the website an individual administrative act involving the claimant. In the course of the administrative proceedings it was found that the decision of the Director of RIEW issued pursuant to Art. 2a of the Ordinance on the conditions and procedures for assessing the environmental impact in conjunction with Art. 38 (1) of the Law on Waste Management (LWM) terminated the procedure under Chapter Six of the Law on Environmental Protection (LEP) involving the contractor – the claimant in this case. The decision contained the full name, address and personal number of the claimant. Evidenced by a printout from the website of RIEW and the one officially made, the decision was posted on the website of the Regional Inspectorate. The Commission ruled that the claimant's personal data were processed by the data controller in violation of the principle of proportionality of data processed, resulting in their disclosure by posting them on the website of RIEW. This act disclosed the claimant's full name and personal number and this information constitutes personal data within the meaning of Art. 2 (1) of LPPD. The volume of the posted information is sufficient for the direct identification of the individual. Moreover, the posted decision also contained information that in itself does not constitute personal data, but linked to the names and the personal number of the individual, allows for the individual's unambiguous identification. In fact, LEP provides for the obligation of public

announcement of the decision on the environmental assessment, but the law does not require the disclosure of the personal number of the assignor. Art. 99 (3) exhaustively specifies the requisites which should be included in the Environmental Impact Assessment (EIA) Decision, and the personal number of the assignor is not among them. In this case the publication of the claimant's personal number and its disclosure on the website of RIEW was carried out in violation of the principle of proportionality in data processing.

2. Statistic data on judgements and analysis of the most common conditions for revocation of administrative acts of CPDP; problems encountered in the judicial practice when monitoring the legality of the decisions of CPDP; initiatives to address these problems.

In 2013, 64 lawsuits were brought before the Administrative Court - Sofia City /ACSC/ litigating administrative acts issued by the Commission for Personal Data Protection. Six of them were brought on litigated administrative acts issued in 2012. For comparison, the lawsuits brought in 2012 were 38.

45 lawsuits completed at first instance. Of these 20 decisions of the Commission were confirmed as correct and lawful, 15 decisions were annulled as irregular and 10 decisions amended the CPDP’s decree regarding the amount of the penalty imposed.

For the specified period ACSC has announced one decision of CPDP to be void. The reasoning of the court for the announcement of the administrative act as void refers to the fact that there is an application filed by the claimant in the administrative proceeding for withdrawal of the complaint. At the time of issuance of the administrative act, CPDP was not informed about the intention of the claimant to withdraw his complaint. The request for withdrawal of complaint was filed after the issuance of the administrative act and within the deadline for its appeal before the court through the CPDP.

In an analysis of the case law of ACSC it can be concluded that the grounds for annulment in the majority of the Commission's decisions refer to violations of administrative rules and inconsistency with material provisions. According to the practice, a violation of administrative rules is considered the failure to collect sufficient evidence to enable the administrative body to clarify all the facts and circumstances relevant to the case. The violations of CPDP identified by ACSC regarding inconsistency with material provisions refer to whether the administrative body has properly determined the infringed norm of the law. The reasoning of the court to amend the acts of the CPDP in the part of the amount of the penalty imposed is that there are not sufficient grounds to justify the sanction imposed above the minimum statutory set amount. It is assumed that the penalty should be aimed at achieving the objective of penalty that has educational, deterrent and warning function, rather than creating economic difficulties for data controllers that committed the violation.

It should be pointed out that the judicial acts which repeal the administrative acts of CPDP do not rule whether the administrative file is returned to CPDP for reconsideration. This practice creates uncertainty and inability of CPDP to exercise its powers under LPPD and iniquity of the judicial act. In the Republic of Bulgaria, the only body that can decide whether or not there is a violation of the Law for the Protection of Personal Data is the Commission. The court has no jurisdiction to decide the case on its merits. The repeal and the lack of instructions about the return of administrative file to CPDP for reconsideration, makes it impossible to resolved the particular case, which leads to instability in the relationship between the data controller and the individuals to whom the data relate and thus to inability for the protection of their rights. The lack of instructions given, respectively order to return the file for reconsideration makes it impossible for CPDP to rule on the case.

The proceedings on 31 appeals of rulings of the Administrative Court - Sofia City ended at the second instance of the Supreme Administrative Court. The final

judgements of the Supreme Administrative Court (SAC) eventually confirmed 17 decisions of the Commission. 11 judgements confirm the judgements of ACSC repealing the decisions of CPDP and 3 judgements amend the decisions of CPDP regarding the amount of the imposed sanction.

VII. Control and administrative-penal activities of the Commission

1. Control activity

The procedure and methods for carrying out the overall control activity is governed by the provisions of the Law for Protection of Personal Data (LPPD), the Rules on the activity of CPDP and its administration (RACPDPA), Ordinance 1 dated 30 January 2013 on the minimal level of technical and organizational measures and the admissible type of personal data protection (the Ordinance), the Instruction on the control activities and the Law on Administrative Violations and Penalties (LAVP).

The Commission exercised control activities in the following areas:

- analysing the current data controllers activities with regard to the compliance with the personal data protection regulations;

- assisting data controllers with consultations and guidance on the compliance with the regulations, and on measures taken for the processed personal data protection;

- exercising direct control on the personal data controllers in the public and private sector;

- imposing sanctions under the LAVP for violation of LPPD.

This control is exercised directly by the Chairperson and by the members of the Commission who are assisted by the specialized administration. According to Art. 26 of RACPDPA, the Legal Procedures and Supervision Directorate (LPSD) through its structural unit – Control and Administrative-Penal Proceedings Department supports the Commission's control activity. This activity includes inspections of data controllers to clarify the facts and circumstances and collect evidence.

The inspections comprise of a set of actions and measures designed to ensure legitimate and effective treatment and personal data protection.

The purpose of inspections is to establish:

- the personal data processing grounds;
- the procedures for keeping the personal data register;
- the purposes for which the personal data is processed;
- the proportionality, accuracy and update of the data;
- the conformity of the processed data protection level with the Ordinance.

On 30 January 2013, the Commission for Personal Data Protection adopted a new Ordinance on the minimal level of technical and organizational measures and the admissible type of personal data protection. The Ordinance was promulgated in State Gazette on 12 February 2013 and repeals Ordinance 1 dated 7 February 2007 (SG No. 25 dated 23 March 2007).

The Ordinance aims to ensure an adequate level of protection of personal data in the maintained personal data registers, depending on the nature of data and the number of affected persons in case of violation of their protection. It defines the main objectives of data protection – confidentiality, integrity and availability, and determines the personal data protection types. In order to define the adequate level of technical and organizational measures and the admissible type of protection, data controllers are required to perform a periodic impact assessment of the personal data processed. The impact assessment results in the determination of the impact level and the appropriate protection level. The basic principle for data access is the "need to know" basis. The necessary technical and organizational measures that should be undertaken by data controllers for each level of protection are defined.

Within 6 months of the entry into force of this Ordinance, data controllers are required to determine the level of impact for the registers processed by them.

For registers of personal data, kept at the time of entry into force of the new ordinance, are established the following terms for the implementation of protection measures when the impact level is determined:

– low level – within six months;

– middle level – within nine months;

– high and extremely high level – within one year.

The control activity of CPDP is consistent with the compliance and enforcement of protection measures within the terms stipulated in the Ordinance.

The control is exercised by carrying out ex-ante, on-going and ex-post inspections. Each inspection ends in the preparation of a statement of findings and in the event that an administrative violation of the provisions of LPPD is ascertained, the Commission initiates administrative penal proceedings pursuant to LAVP.

Total number of inspections carried out in 2013 – 2696, of which:

– ex-ante – 2613;

– on-going – 39; and

– ex-post – 44.

These data show that most ex-ante inspections were carried out pursuant to Art. 12 (2) of LPPD. 2696 inspections were carried out in 2013, resulting in 2684 statements of findings and 12 inspections ended only in drafting statements for ascertaining administrative violations.

For comparison: in 2012 total 1718 inspections were completed. (Fig. 5)

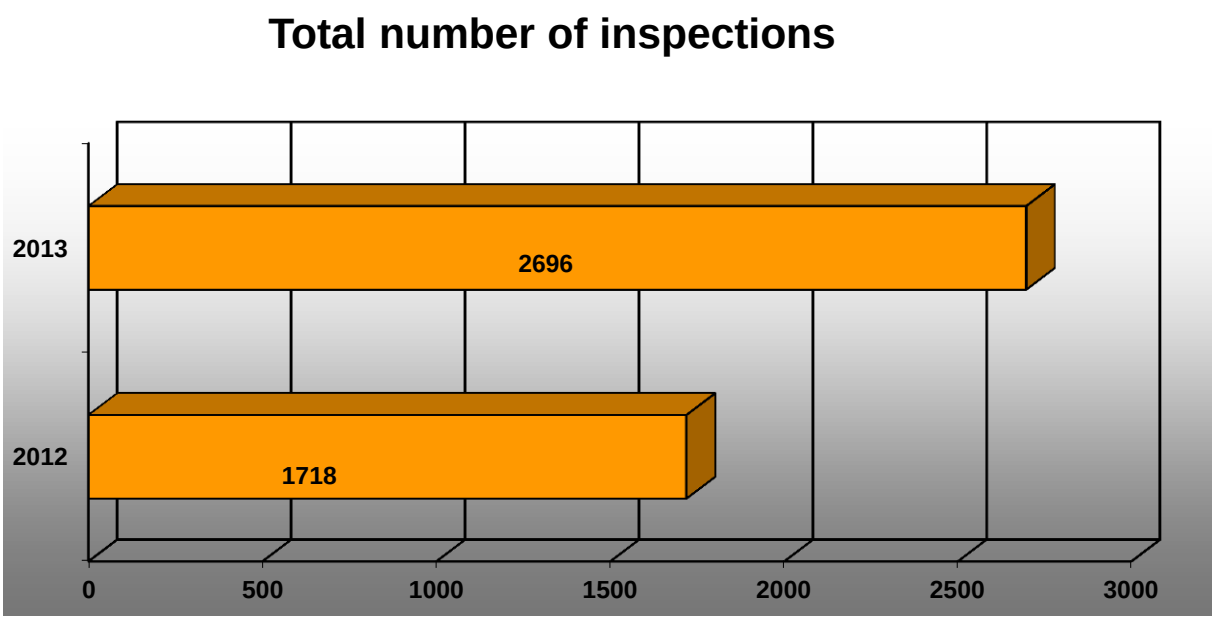

Fig. 5.

1.1. Ex-ante inspections

According to Art.17b of LPPD, these inspections are required prior to the data controller (DC) entry in the register under Art. 10 (1) (2) of LPPD in the cases where the data controller has declared processing of specially protected data under Art. 5 (1) of LPPD or according to a Commission decision, data the processing of which endangers the individuals' rights and lawful interests.

The ex-ante inspections aim to establish the technical and organizational measures undertaken by the personal data processing and the admissible type of protection provided by data controllers and their compliance with the Ordinance's requirements.

In 2013, the focus was placed on this type of inspections, resulting in a total of 2,613 ex-ante inspections compared to 1,616 in 2012 (Fig. 6).

Of all ex-ante inspections carried out in 2013, 2,588 ended with registration of the registers under Art. 10 (1) (2) of LPPD, 24 ended with termination of the registration procedure and deletion from the register under Art. 10 (1) (2) of LPPD, due to termination of the respective data controllers' operation and other reasons, and 1 inspection ended with a refusal of registration, due to the failure of the applicant to submit the necessary documents for the implementation of the inspection. The main problem in carrying out this type of inspections remains the communications with DCs in order to request the necessary documents to complete the inspection. The most common reasons include unclaimed mail, changed addresses, errors in the filed applications and failure to send the required documents after the proper notification receipt. Due to the impossibility of completion of these inspections, in 2013, CPDP issued a decision and pursuant to Article 17b (3) (3) of the LPPD rejected the registration of 828 data controllers in the Register of Data Controllers and the Registers Kept by Them. After the publication of CPDP's decision, 26 of them sent the required documents for ex-ante inspections and were entered in the register under Art. 10 (1) (2) of LPPD.

1.2. On-going inspections

Although considerably fewer in number, the on-going inspections carried out pursuant to Art. 12 (3) of LPPD are more complex in legal aspect. In 2013 a total of 39 such inspections were carried out compared to 71 in 2012 (Fig. 6).

According to the law these inspections are carried out at the request of the interested persons and at the initiative of the Commission on the basis of a monthly plan for execution of control activity adopted by the Commission.

As a result of these inspections, 20 compulsory instructions were issued, 6 statements for ascertaining administrative violations were drafted and 16 inspections did not establish any violations of LPPD.

At the end of 2012, CPDP adopted a "Plan for carrying out on-going inspections at the initiative of CPDP for 2013" (the Plan). The Plan aims at enhancing the efficiency of the Commission's control activity through its further administrative strengthening, improving the supervision organization, elaborating the methods for consulting personal data controllers and individuals.

According to the Plan the criteria for selecting DCs to be inspected are as follows:

1. DCs of structures and areas with prior significance/ of priory areas and structures in the CPDP activity:

- DCs, which activity is of public and social significance;

- DCs, which underwent significant structural changes resulting from a change in the law and the internal regulations.

2. DCs depending on the categories and the volume of personal data processed:

- DCs processing personal data pursuant to Art. 5 (1) of LPPD;

- DCs which activity endangers the individuals' rights and lawful interests;

3. DCs which have not been subject to inspection.

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

5. Administrative region where no scheduled inspections of DCs have been carried out.

The main tasks of the scheduled inspections are related to the fulfilment of DC's obligations in connection with the provisions of LPPD regarding the registration and update of DCs in the register under Art. 10 (1) (2) of LPPD and the obligations under Art. 19 (1), Art. 23, Art. 25 of LPPD, and the establishment of technical and organizational measures to protect personal data. The inspections mainly involve registers containing personal data of individuals, customers (contractors) of data controllers, according to their main business in the following areas: government, judicial, education, banking and credit activity, trade and services, etc., mostly with national scope of operations.

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

The following inspections of DCs, distributed by field of activity, were carried out:

– public administration (7 inspections) – Executive Forestry Agency, Ministry of Interior (Schengen Information System), Ministry of Foreign Affairs (Visa Information System), Ministry of Labour and Social Policy, Ministry of Interior (National Unit Europol), National Institute of Forensic Science and Criminology at the Ministry of Interior and the State Agency for Refugees at the Council of Ministers (National Eurodac System);

– healthcare (3 inspections) – Alexandrovska University Hospital for Active Treatment EAD, National Center of Addiction and Multiprofile Hospital for Active Treatment Tokuda Hospital Sofia AD;

– justice (3 inspections) – Veliko Tarnovo Court of Appeal, Smolyan Administrative Court and Smolyan District Court;

– regional and municipal administration (2 inspections) – Regional Administration – Haskovo Region and Municipal Administration – Haskovo;

– education (2 inspections) – European Polytechnic University, Pernik and Regional Inspectorate of Education – Pernik;

– financial sector (2 inspections) – DSK Bank EAD and TBI Leasing EAD;

– trade and services (2 inspections) – Moto-Pfohe EOOD and K&K Electronics EAD;

– insurance (1 inspection) – Insurance Company Euro Ins AD and

– pension insurance (1 inspection) – ING Pension Insurance Company EAD.

As a result of the completed scheduled inspection 20 statements of findings were drawn up and 13 compulsory instructions issued. 3 inspections of DCs are in the process of completion.

At the beginning of 2013, 4 inspections schedules in 2012 were completed, involving Rila Tours 2001 OOD, Metro Cash&Carry Bulgaria EOOD, Easy Asset Management AD and State Fund Agriculture. Compulsory instructions were issued on 3 of the inspections.

1.3. Ex-post inspections

The third type of inspections refers to the inspections under Art. 12 (4) of LPPD, namely ex-post inspections carried out on the application of CPDP's decisions or compulsory instructions and at the Commission's initiative after receiving a signal.

In 2013 a total of 44 ex-post inspections were carried out compared to 32 in 2012 (Fig. 6).

As a result of these inspections, 3 compulsory instructions were issued, 14 statements for ascertaining administrative violations were drafted and 27 inspections did not establish any violations of LPPD.

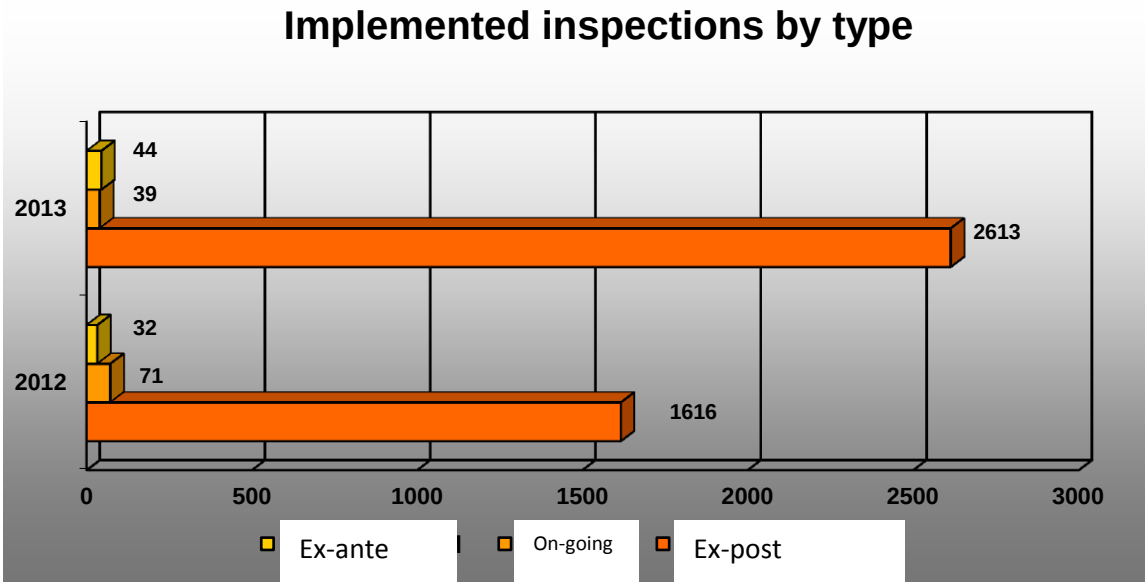

Fig. 6.

A differentiation by sectors was made in connection with the specific conditions in which personal data are processed. When performing its activity in 2013, the Commission carried out the following inspections by sectors:

No.	SECTOR	NUMBER
1.	Healthcare	1,510
2	Trade and services	310
3	Education and training	225
4	Legal and consultancy services	136
5	Construction and architecture	62
6	Tourism	51
7	Social activities	45
8	Production	39
9	Non-profit organizations	29
9	Transport	29
10	Insurance and social security	25
11	Financial and accounting services	21

11	Real estates	21
12	Telecommunication and information technology and services	20
13	Finance	19
14	Agriculture and forestry	15
15	State administration	13
16	Regional and municipal administration	12
16	Advertising and marketing research	12
16	Security services	12
17	Political parties and organizations	8
18	Other	82

The attention was drawn on the inspections of DCs processing personal data relating to health, sexual life or human genome, revealing racial or ethnic origin; political, religious, philosophical, political opinion and membership in such organizations.

1.4. Handling of requests

Pursuant to Art. 36 (2) of RACPDPA when a request does not contain data of violated rights of the applicant, action can be taken under Art. 10 (1), (3), (5), and (6) and Art. 43 of LPPD. In 2013, the specialized control department considered 123 requests from individuals, including various inquiries on personal data protection issues, and on requests for access to public information under the Law on Access to Public Information (LAPI), resulting in the issuance of the respective draft decisions.

There is a steady trend towards an increase of this type of applications, which in 2012 were 74.

Most of the requests received by the CPDP concern rights violated under the LPPD in the following sectors: Internet (56), CCTV (16), public administration (12), trade and services (6), financial sector (5), etc. Significantly lower is the

number of requests in the sectors of district and municipal administration, education and training, healthcare, gambling, telecommunications, etc.

In 2013, there is an increase in the signals sent by individuals for disclosure of their personal information without their consent, including their use for direct marketing, intrusion into their personal profiles in the social networks and/or e-mail addresses, as well as, when using video surveillance.

As a result of the consideration of the requests, 10 statements on ascertainment of administrative violations were drawn up and 7 requests were forwarded to other competent authorities. The relevant answers were sent to the senders.

2. Administrative penal activity

2.1. Compulsory instructions

Pursuant to Art. 10 (1) (5) of LPPD and in connection with the implementation of the control activity under Art. 12 (1) of LPPD, the Commission issues compulsory instructions (CI) to DCs regarding the personal data protection when processing data in accordance with the relevant activity.

These instructions aim at ensuring the adequate personal data protection level in the kept personal data registers by providing the required minimal technical and organizational means and protection measures pursuant to the LPPD and the Ordinance.

In 2013, CIs were issued to 26 DCs, compared to 16 for 2012. The most instructions were issued in the field of public administration, followed by the regional and municipal administration sector, the financial sector, and the sector of healthcare. The least instructions were issued in the following sectors: justice, education and training, information technology and services, and trade and services.

The percentage of the CIs issued depending on the violation type is specified in the chart below (Fig. 10) 7).

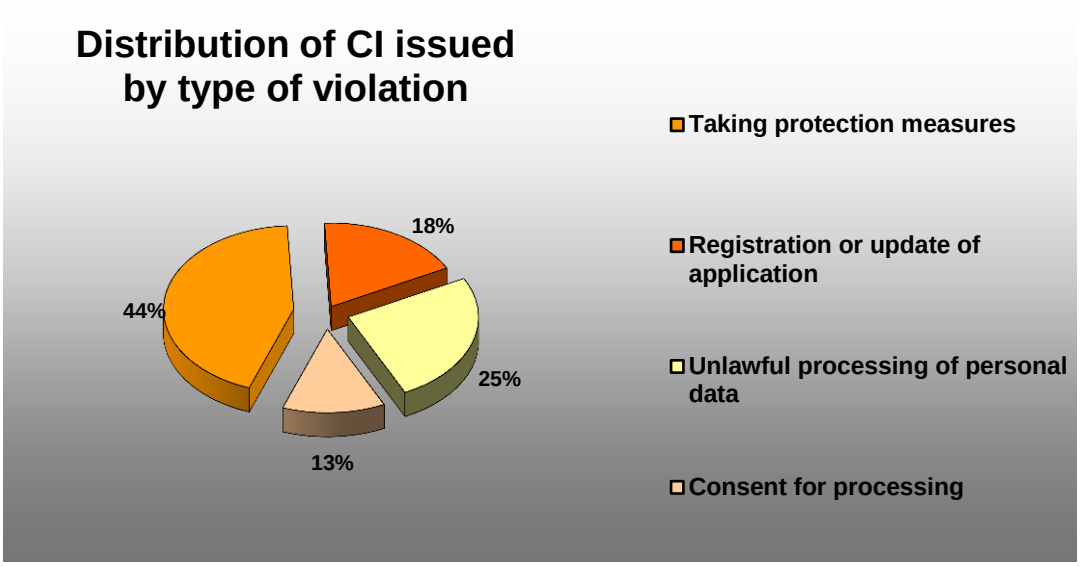

Fig. 7

Most often instructions are issued in relation to ascertainments concerning the processing of copies of the identity documents of individuals when entering into employment contract or upon holding public office. When concluding an employment contract, each employment is required to comply with the requirements of Art. 66 (1) of the Labour Code and Ordinance 4 dated 1993 on the documents required for the conclusion of employment contracts. Art. 1 of this Ordinance does not provide for the submission of an identity document copy by the conclusion of the employment contract and therefore the requirement for the provision of such copies is without legal basis. Furthermore, such a requirement is not included in the provisions of Art. 2 of the Ordinance on the documents required to hold public office. Therefore, the processing of personal data by storing a copy of the individual's identity document in the individual's labour and official records when concluding the employment contract, respectively when the employment relations are established, is unlawful and in breach of the principle, set out under Art. 2 (2) (1) of LPPD.

The instructions were issued in connection with the determination of specific measures to ensure the necessary personal data protection level. An important

point in the technical and organizational measures that should be undertaken by the DC is the obligation to determine time limits for data retaining.

Other common violations were related to the violation of the provisions of Chapter Three of LPPD relating to the DC's obligations under Art. 17, Art. 17b and Art. 18 (3) to register and/or update the register under Art. 10 (1) (2) of LPPD, and to the violation of the provisions of Art. 19 of LPPD requiring the DC to inform the individuals on any processing of their personal data.

Of the total number of 26 CIs issued – 13 were implemented within the deadlines specified by the Commission, 2 are subject to appeal and the rest are in the process of implementation.

2.2. Administrative penal proceedings

According to the provisions of Art. 43 of LPPD, the ascertainment of violations, the issuance, appealing and execution of the penal decrees (PD) is applied following the procedure established under the Law on Administrative Violations and Penalties (LAVP).

Statements for ascertaining administrative violations (SAAV) of LPPD's instructions are drawn up by a Commission's member or by officials authorized by the institution according to the requirements of Art. 43 (1) of LPPD. PDs are issued by the Chairperson of the Commission (Art. 43 (2) of LPPD).

In 2013, in accordance with the Commission's powers under Art. 12 (1) and (8) of LPPD to exercise control on the compliance of the regulations in the field of personal data protection, 40 violations of different provisions of LPPD were ascertained resulting in drafting 30 SAAVs on the basis of which the Chairperson of CPDP issued 29 PDs. Compared to 2012, there is a decrease in the number of SAAV, but there is an increase of the issued compulsory instructions.

The most common violation of LPPD concerned the failure to update the information submitted on the personal data registers kept by DCs. The violation involves processing of personal data by the data controller for the purposes of a

new register, not declared before CPDP and not entered in the register under Art. 10 (1) of LPPD.

The second most common violation concerned the failure of the data controller to take the appropriate technical and organizational measures to protect the data against accidental or unlawful destruction or accidental loss, unauthorized access, modification or disclosure and against other unlawful forms of processing, which is a violation under Art. 23 (1) of LPPD.

Next was the failure of the data controller to carry out registration following the provisions of Art. 17 and Art. 17b of LPPD.

Common violations were the violation of Art. 19 (1) of LPPD and Art. 2 (2) (2) of LPPD, and respectively in the first case, DC failed to provide the individual whose data will be processed with the necessary information on the purposes of processing and the recipients of the processed data, and in the second case, the processed data were not relevant to, related with and exceeded the purposes for which they are processed. 29 PD were issued, and 11 of them are based on statements issued at the end of 2012.

Along with the PD issued in 2013, fines and property sanctions were imposed in the total amount of BGN 76,800, of which BGN 29,800 were paid.

By a motivated resolutions of the Chairperson of CPDP pursuant to Art. 34 (3) and Art. 54 of LAVP, one administrative penal proceeding for two violations was partially terminated. As a reason for termination, the administrative penal authority considered that there was not sufficient evidence that the DC to which SAAV was issued had committed that violation. PD was issued for the other violation. In 2013, similarly to 2012, the officials experienced difficulties to deliver the prepared SAAVs through the municipalities in the country according to the provisions of Art. 43 (4) of LAVP. In some cases SAAVs were delivered to persons without representative power, in other cases no receipt was signed with which the DC certifies that it is informed of its right to submit objections to the statement within 3-day period, which led to their return for a new duly delivery.

Although not established in practice, but in order to find and deliver the SAAVs and PDs, CPDP asked for and received assistance from the authorities of the Ministry of Interior.

Of all PDs issued in 2013, no decree was revoked by the court, 1 was confirmed and the court ruled for reduction of the penalty amount.

Of all PDs issued in 2011 and 2012, which in 2013 were in the process of lawsuits, 3 were fully repealed, 12 were confirmed and on 6 of them the court ruled for reduction of the penalty amount. Currently, 25 appealed PDs are subject to judicial review.

5 PDs have entered into force in 2013 without being appealed.

From the analysis of judicial practice on the amended PDs, it can be concluded that there is a trend showing that the courts in the country reduce to the minimum the amount of the imposed penalties for the respective violation, foreseen in LPPD. Most often, the reasons of the court when making the decisions to reduce the imposed property sanctions include “lack of aggravating circumstances”, such as first violation of the data controller, relevant evidences submitted after violation ascertainment, and “lack of harmful consequences of the act”.

Repealing the decrees, the Court stated its reasons that the punitive body has violated material procedural rules, in particular it incorrectly stated the date of the offence, and therefore the Court considers this a violation of the right of defence. (PD 15/2012, against Start 10 OOD, Plovdiv). In the other case, the court found that there is no corpus delicti for the issuance of PD (PD 40/2012, against Yovkov&Yovkov OOD).

In the Commission's case law in 2013, the most significant was the case under PD 30/2011 against the political party "The Other Bulgaria", confirmed by Sofia District Court (SDC) by ruling for a penalty reduction. The Administrative Court - Sofia upheld the judgement of SDC. The decree imposed property sanctions on the political party for two violations – under Art. 17 (1) of LPPD and

Art. 18 (3) of LPPD. The violations concerned personal data processing – full name, personal number, e-mail address and location – of 702 individuals before the DC has submitted an application for registration in CPDP, and by processing personal data of 2233 counted individuals for the purposes of a new registry without informing CPDP about the change in the data of the original registration application. The aim of the political party "The Other Bulgaria " was to carry out a survey to count the Bulgarian citizens living outside the territory of Bulgaria.

There is also a positive trend in the case law with the confirmation of PDs issued against legal entities engaged in the hotel business, regarding their registration as controllers in he register under Art. 10 (1) (2) of LPPD prior to the processing of personal data of an unlimited number of individuals, updating information before making changes in the data of already registered data controllers (Art. 18 (3) of LPPD) or failure to take the required minimal technical and organizational measures to protect personal data with the rules implemented by personal data controllers (Art. 23 (4) in conjunction with (1) of LPPD).

The statistical data mentioned indicates increase in the performance of the administrative penal activity with regard to its efficiency and legality. All judgements and particularly their grounds were analysed in depth, in order to be legitimately implemented in the control activity and most of all for removal of weaknesses and gaps admitted in the activity on ascertainment of violations of LPPD and their recording in accordance with the provisions of LAVP. As a result, there is a persistent tendency to maintain a relatively low percentage of PD repealed by the court.

VIII. Proceedings on expressing opinions and authorization to transfer data to third countries

In 2013, CPDP ruled on 79 requests for opinions filed by individuals and legal entities.

In summary, the issues on which the Commission has expressed opinions can be grouped in several directions:

1. Access to the National Population Database (NPD)

In 2013, CPDP was again approached with requests for authorization of access to the National Population Database, maintained by Directorate General "Civil Registration and Administrative Services" (DG CRAS) at the Ministry of Regional Development and Public Works (MRDPW), on the grounds of Art. 106 (1) (3) of the Law on Civil Registration (LCR). The opinions stated by the Commission on the requests in question confirmed the constant practice according to which MRDPW - DG CRAS can provide information, i.e. personal data (not direct access) on the ground of the legitimate interest of applicants and after such legitimate interest is proven by appropriate legal means.

For example, such requests were filed by private companies with subject of business "credit activity" in accordance with the provisions of the Law on Consumer Loans. The requests by the above companies for direct access to NPD are reasoned with the credit activity performed by them and the related obligations for customers' identification under the Law on Measures against Money Laundering. The opinion of CPDP on the individual requests was that the data should be provided by MRDPW - DG CRAS in the form of specific information rather than direct access to the National Population Database.

Some of the requests indicated that the companies acquire for valuable consideration the receivable of bank and non-bank financial institutions by entering into contracts for the sale and transfer of receivables under which they obtain the rights of creditors for the liable persons (cession agreements). In

connection with collection of receivables, subject of the cession agreements, the companies needed to make inquiries about the civil status of the debtors who are natural persons, in particular inquiries about their permanent and current address. The representatives of the aforementioned companies approached the Commission in accordance with the provisions of Art. 106 (1) (3) of LCR with the request to be authorized to have access to the data kept in National Population Database, maintained by DG CRAS at the Ministry of Regional Development and Public Works.

In these particular cases the Commission expressed opinion, that there was no legal obstacle such information to be provided upon the request by the companies for debt collection and after justifying their right by the MRDPW and the DG CRAS to submit information, i.e. personal data (not direct access) for the exercise of their legitimate interest. The LCR text suggests that the data controller (MRDPW - DG CRAS) should assess the statutory requirements, on the basis of which it may provide personal data such as: cession agreement (for cases where the transfer of debts is carried out by cession), confirmation for concluded cessions pursuant to Art. 99 (3) of the Law on Obligations and Contracts, contracts with individuals, which include the consent of the individual that the cedant as a data controller may require and receive personal data from information databases of other data controllers, etc.

2. Third party access to personal data

As in previous years, in 2013, the proceedings carried out in the Commission handled issues related to the operation of companies with business activity involving extrajudicial actions to collect valid and due receivables (excluding enforcement by governmental or private bailiffs), the so called "collectors companies".

Furthermore, the issue related to companies with business activity involving collection of receivables should be supplemented with the request of a company

with the aforementioned business activity, filed in 2013, informing that the company enters into contracts to provide services on collection of receivables as a Contractor and undertakes contractual obligations to the Contracting Authorities (banks and non-bank financial institutions, businesses, service providers, etc.) to conduct extrajudicial activities on collecting valid and due receivable of the Contracting Authorities to third parties – their debtors. In this case there are no actions of transfer of receivables – cession. The Contractor – collection company – acts as a "data processor" on behalf of data controllers (the individual Contracting Authorities), whereas in accordance with Art. 24 (4) of LPPD the relations between the data collectors and the collection company, as data processor, are governed by a written contract for provision of services for collection of receivables.

When processing personal data of debtors of the Contracting Authorities provided by the Contracting Authorities – customers to the Contractor – collection company, the latter contacts the debtors (by written correspondence or telephone calls). In some cases, the debtors voluntarily provide the data processor with additional data, including contact telephone numbers, current addresses for correspondence. In connection with the foregoing, the collection company approached the Commission for an opinion concerning the following issue: Is it admissible that the voluntary provided personal data (current telephone numbers and addresses for correspondence) by debtors of the Contracting Authorities-customers of the Data Processor-collection company, which have become known to that the Data Processor in connection with the implementation of Contracts for provision of services for the collection of receivables, may be provided to the relevant Contracting Authority-customer of the company.

The opinion of CPDP on this issue is that the collection company, as personal data processor, is allowed to provide the customers of the company in their capacity of data controllers with personal data of debtors - individuals (current telephone numbers and addresses for access) only if the Contracts for

provision of services for the collection of receivables include an obligation of the Data Processor for the purposes of carring out the contract, to perform actions regarding the update of the processed personal data. This will be done following the obligation of the data controllers-customers of the collection company under Art. 2 (2) (4) of LPPD to maintain accurate and updated data. In case that the Contracts for provision of services for the collection of receivables do not include the obligation for the Data Processor to update the data, then the Data Processor may provide the collected additional personal data only after obtaining the express and informed consent of the affected individuals. In this case the collection company is an independent data controller with the ensuing obligations for lawful, proportionate, conscientious and accurate personal data processing.

Another interesting issue about the provision of loans to individuals, on which CPDP delivered an opinion in 2013, was the request filed by the manager of the National Social Security Institute (NSSI), which reported that NSSI received inquiries on the lawful application of Art. 25 of LPPD in assumption of destruction of data after achieving the purpose of processing. The inquires are related with the conclusion of contracts by NSSI pursuant to article 33 (5) (11) of the Code of Social Security (CSS) on the provision of information to financial institutions in connection with the financial services provided by those institutions (loans, leasing, etc.).

The contracts included specific clauses requiring that the data controller receiving the data under Art. 4 (1) (2) of LPPD should receive the consent of the inspected person before receiving the respective data. The Manager of NSSI informed that the institute carried out periodic inspections aimed to verify and ensure that the counterparties observe their contractual obligations. The right of inspection is stipulated in the contracts.

In connection with the above, the counterparties of NSSI, in order to meet their contractual obligations and upon the inspections of the NSSI to ensure the availability of the required consent sent an inquiry regarding the application of Art.

25 of LPPD and in particular the obligation that the processed data should be destroyed after achieving the purpose of processing. The specific problem was related mostly to cases where there was a refusal to the applicant to be provided with the requested financial service and respectively the difference in time from the refusal to the possible inspection of the case by NSSI.

In connection with the foregoing, the Manager of NSSI approached CPDP for an opinion on the proper application of Art. 25 of LPPD in the context of the above assumptions, while taking into account the interest of NSSI as a data controller which provides data and wants to be allowed to verify the compliance with the contractual texts which ensure the lawful processing of the data provided by third parties.

The opinion of CPDP on this issue was that banks and non-banking financial institutions, providing loan services, acting as data controllers, are required to coordinate their activities involving personal data processing in compliance with the requirements of Art. 25 of LPPD, namely: after achieving the purpose of data processing, the data should be destroyed.

In order to ensure the powers of NSSI in connection with the control on the compliance with the obligation to obtain the prior consent of the persons inspected before providing information from the NSSI database, the contracts executed between the financial institutions providing loan services and NSSI should stipulate that the personal data will be destroyed after notifying NSSI within a reasonable period agreed between the parties. The financial institutions should at any time have valid evidence concerning the destruction of data – for example, a protocol for destruction of statements of consent or other written document specifying the destruction of the personal data after achieving the purpose of their processing.

It is imperative that the financial institutions providing loan services, after the destruction of data should inform the respective individuals that the purposes

for which their data are collected have been achieved and therefore pursuant to Art. 25 (1) (1) of LPPD these data are destroyed.

3. Provision of personal data in accordance with the Law on Access to Public Information (LAPI).

In 2013 CPDP delivered an opinion concerning the application of LPPD in cases of applications filed to individual data controllers, public representatives, relating to the provision of information under the Law on Access to Public Information. CPDP expressed opinions in relation to cases where the access to the information should be refused pursuant to Art. 37 (1) (2) of LPPD or such information could be provided but with deleted data relating to third parties who have not given their consent or have explicitly refused to provide their personal data in the specific cases under Art. 31 (4) of LPPD. In such cases, the right to decide whether to refuse access to the requested information or to give access in volume and in a manner that does not prejudice the rights of third parties belongs entirely to the data controller. The aim of this approach is in each particular case to ensure the lawful personal data processing and privacy of the individuals.

An example can be mentioned the request for opinion filed by the Council of Ministers about two applications for access to public information filed by print media requiring information about the persons employed under official contracts and under civil contracts in the administration of the Council of Ministers, including the employees' name and surname, position and remuneration under the contract. CPDP expressed an opinion that the provision of information containing the name and surname, position and remuneration under the contract of individuals employed under labour and official contracts, as well as copies of civil contracts with individuals, could result in personalizing these particular individuals and as such it falls within the definition of "personal data" of the category of economic identity, as they directly identify the individuals and their remuneration. The processing of this information in the form of "disclosure" and its provision is

permissible and lawful only in cases where at least one of the conditions for admissible processing is available. In the cases of provision of public information under LAPI which contains personal data, a condition for admissible processing in the form of data disclosure is the the consent of the respective individual (Art. 31 of LAPI in conjunction with Art. 4 (1) (2) of LPPD). In its opinion, CPDP also pointed out that with regard to the processing of personal data contained in labour and service records, the provision of Art. 17 (4) of the Law on Civil Servants should apply, namely that the disclosure of information from the service records of the civil servant is not permitted without the express written consent of the data subject. By analogy, the same rule should apply in respect of persons (employees) employed under the Labour Code.

4. Requests for provision of information containing personal data

Other rulings of CPDP with opinions related to requests for provision of information containing personal data can be summarized into several groups.

At the request of Members of Parliament pursuant to Art. 90 of the Constitution of the Republic of Bulgaria filed to public data controllers. For example, the Executive Forestry Agency subordinate to the Ministry of Agriculture and Forestry filed a request for opinion on issues concerning the application of LPPD in relation to the provision of information to a Member of Parliament containing personal data on files related to the change of use and sale of land plots in forest areas. Upon the provision of the requested information, consideration should be made for the legal requirements, the public interest both in relation to the question raised by the Member of Parliament, but also for the right to privacy, and the availability of the consent of the individuals that are the subjects of the personal data should also be taken into account.

CPDP expressed an opinion that the provision of the requested information is admissible only in cases where there is at least one of the conditions specified in the provision of Art. 4 (1) (1-7) of LPPD.

A possible admissibility condition for processing in the form of the provision of data in this particular case is the availability of the consent of the affected individuals (Art. 4 (1) (2) of LPPD). In the absence of consent, possible admissibility conditions are the provisions of Art. 4 (1) (1), (5) and (6) of LPPD. In order to ensure fair processing of data in the specified legal assumptions and to achieve the objective of LPPD - ensuring privacy, the data controller can provide the files on the number of purchase and sale transactions and changes of the intended use of the land plots but only after the personal data contained therein are brought in a form that does not allow for the identification of the individuals, such as deletion or anonymisation by initials.

Request for an opinion filed by the Council of Ministers as a liable subject under Art. 90 (1) of the Constitution of the Republic of Bulgaria regarding a question raised by the Members of Parliament through the Chairperson of the National Assembly to the Prime Minister of the Republic of Bulgaria pursuant to Art. 90 (1) of the Constitution of the Republic of Bulgaria and Art. 89 of the Rules of Organization and Procedure of the National Assembly. The request for the opinion stated that the administration of the Council of Minsters has received a request for the provision of data on the number of appointed and dismissed employees in the state administration for six months, specified by: ministries, state agencies, executive agencies, regional administrations, specialized administrations - individual legal entities. It was specified that the request includes the attachment of lists of names upon complying with LPPD, as well as information on the reasons for the emergence of relationships. It was also specified that the provision of this information identifies the particular administrative structure. In this connection, the request for an opinion was whether the lists of names linked with the other required information constitute complex personal data. The Commission expressed an opinion that information containing name, specific administrative structure and reasons for the emergence of employment or service relation of a servant at the public administration could lead to the identification of this

particular individual and as such it falls within the definition of personal data under Art. 2 (1) of LPPD. The provision of such information is allowed only in cases where there is at least one of the conditions specified in the provision of Art. 4 (1) (1-7) of the LPPD. In this particular case, the Council of Ministers as a liable subject under Art. 90 (1) of the Constitution of the Republic of Bulgaria, could provide the requested information (without the names of the persons) in pursuance of a statutory obligation of the data controller within the meaning of Art. 4 (1) (1) of LPPD.

In addition to the examples on requests for access to information containing personal data, was the request filed by the Regional Inspectorate of Education - Pazardzhik regarding a letter sent by the regional structure of the trade union Podkrepa concerning the provision of personal data by the principal of the primary school in the town Pazardzhik. The information requested by the trade unions is the work schedule and the basic gross salaries of teaching and non-teaching staff of the school. It was stated that the information is requested in connection with the expected increases in wages and amendments in the Internal Rules on the Formation of Wages. The chairpersons of the trade union sections took part in the negotiations and therefore they need to know the amount of the basic wages of the categories of employees "teacher", "senior teacher" and "chief teacher". The Commission expressed the opinion that if in this particular case the information on individual wage could lead to individualization of a particular individual, then it falls within the definition of personal data within the meaning of LPPD. Processing of that information is admissible only in cases where there is at least one of the conditions specified in the provision of Art. 4 (1) (1-7) of the LPPD. In this case, as a condition of admissible processing by the provision of the requested information may serve the provisions of Art. 4 (1) (5) of LPPD - performance of a task carried out in the public interest. The information on the waged of the teaching staff in the primary school should be provided only by categories "teacher", "senior

teacher", "chief teacher" without specifying the individuals occupying the teaching positions at the school.

5. Disclosure of personal data of public persons

Another important issue regarding the access to information containing personal data, considered by CPDP in 2013, was related to the announcement of the declarations under Art. 12 of the Law on Prevention and Disclosure of Conflict of Interests (LPDCI) on the official websites of the state institutions in search of a balance between the public interest and the protection of personal data of specific persons. The disclosure of personal data contained in the declarations under Art. 12 pursuant to Art. 17 (2) of LPDCI, excluding the names of the declarer should be done with the express written consent of the individual-declarer attached as a separate text to the same declaration. Posting on the Internet the declaration under Art. 12 of LPDCI without the express consent of the declarer would constitute a violation of LPPD. Any declaration posted on an official website without the express consent of the declarer should be removed until the consent of the data subject is obtained. The announcement should not contain the signature of the declarer. In the event that the declaration contains third persons personal data, the consent of the declarer does not reflect on them and they should be anonymised.

With regard to the recent amendments to the Law on Publicity of the Property of Persons Occupying High State Positions and Other Positions which extended the scope of the liable persons, CPDP received a request for an opinion concerning the public access to the declaration posted on the website of the Court of Auditors. CPDP expressed the opinion that the posting of data of the liable persons as a form of personal data processing under LPPD is permissible and lawful, as in this case the data are collected for specified, specific and legitimate purposes, namely: for ensuring publicity and transparency of the property of public persons from the public and private sector who considering their positions and functions have a reduced level of protection than the other citizens. In terms of the

consent included as part of the declaration form, the position of the CPDP supports the fact that the consent is required under a special law and in fact is a duty to provide relevant information for the purposes of publicity of the property of persons occupying high state, public and other positions in the public and private sectors, and therefore its absence cannot block the implementation of the mandatory provisions of the Law on Publicity of the Property of Persons Occupying High State Positions and Other Positions in the Public and Private Sectors. Even the absence of the consent of the persons liable for publishing the information contained in the declarations, due to the availability of a legal obligation for the Court of Auditors to publish such information, which is also a performance of a task of public interest, the public disclosure of such information is permissible and lawful. In its opinion, CPDP made an analysis of the purpose of the Law on Publicity of the Property of Persons Occupying High State Positions and Other Positions in the Public and Private Sectors, namely: that the property of these persons should always be known as a type of anti-corruption measure which cannot be limited under LPPD. Reasons for this may also be sought in Decision 4 dated 26 March 2012 under constitutional case 14/201, which confirms the adopted in 1996 interpretation of the balance between the two rights – for public persons the protection of personal data is "much reduced" compared to the other individulas personal data protection.

6. Sensitive data

Other opinions of CPDP in 2013 were related to the access to the so-called "sensitive data" whose processing is generally prohibited under Art. 5 (1) of LPPD.

As an example may serve a request filed by the Ministry of Health, which stated that the Director of the State Psychiatric Hospital in a Bulgarian town approached the Ministry with a request for "guidance" in connection with a letter of the Ministry of Interior Regional Directorate to provide a "updated list of the currently hospitalized mentally ill persons". In this case CPDP expressed an

opinion that the requirement for maintenance of a list of mentally ill persons by police and junior police inspectors laid down under Art. 20 (1) (7) of Instruction 1з-2295 dated 2012 on the organization of operation at the Ministry of Interior on the territorial service to citizens, is contrary to the conditions for provision of health information under Article 28 (1) of the Law on Health, which protects the patients' rights, and in this particular case – the rights of the patients with mental disorders hospitalized in the respective State Psychiatric Hospital. Furthermore, the Constitution of the Republic of Bulgaria contains several basic principles regarding mentally ill persons, namely: persons with physical and mental disorders are subject to special protection by the state and society (Art. 51 (3)), the state shall protect the health of citizens (Art. 52 (3)). In addition, the text of the instruction is in absolute conflict with the provisions of Art. 157 (1) of the Law on the Ministry of Interior, which explicitly prohibits the collection of information about citizens on their health condition only (Art. 157 (1) of the Law on the Ministry of Interior). In view of the aforementioned, the Commission expressed an opinion that the requested information (updated list of the hospitalized mentally ill persons) should not be provided. Such a provision would be contrary to the provisions of Art.4 (1) and Art. 5 (2) of LPPD, the provision of Art. 28 of the Law on Health, as well as the provision of Art. 157 (1) of the Law on the Ministry of Interior. In this case, the provision of such requested information about the persons hospitalized in this hospital would violate the principles of appropriateness and proportionality, as laid out under Art. 2 (2) of LPPD.

In 2013 the Commission expressed another opinion on processing of sensitive data on requests filed by the National Health Insurance Fund (NHIF). One of them was related to the provision of lists containing information on persons qualified by Ministry of Defence as military disabled and military suffered to pharmacies which have entered into contracts with NHIF for dispensing medicines. CPDP ruled that NHIF is allowed to provide the requested information to the pharmacies which have entered into contracts with NHIF pursuant to Art. 4 (1) (1)

and (4) of LPPD, namely: the processing of personal data of individuals is permitted if it is necessary for the data controller to perform a statutory obligation, as well as when the processing is necessary to protect the life and health of the individual to whom the data relates. The provision of personal data is admissible in connection with Art. 28 (1) (7) of the Law on Health, which stipulates that health information about individuals can be provided to third parties when it is necessary for the purposes of the Ministry of Health, the National Center for Health Information, NHIF, the regional health inspections and the National Institute of Statistics.

The national Health Insurance Fund also approached CPDP on issues concerning the transfer of personal data under Art. 5 (1) of LPPD to insurance companies, referring to the Insurance Code. The opinion of CPDP is that NHIF and RHIF are allowed to provide personal data stored in the information registers maintained by these institutions upon receiving a request by insurance companies in relation to the occurrence of insurance events under Third Party Liability Insurance and Life Insurance.

7. Opinions on matters of important public interest

In 2013 CPDP expressed an opinion on issues related to the protection of personal data in connection with the conditions and procedures for the certification of the Bulgarian origin of applicants for Bulgarian citizenship. To rule on the request for an opinion, CPDP analysed the legal framework regulating the public relations in connection with the acquisition of Bulgarian citizenship through naturalization. The legislator has determined a strict procedure under which persons who are not Bulgarian citizens by origin or place of birth may acquire Bulgarian citizenship through naturalization. Based on the legal analysis, CPDP assumed that given the complex factual composition of the procedure for acquisition of Bulgarian citizenship through naturalization under the Law on the Bulgarian Citizenship, in order to exercise the powers of the Minister of Justice

and pursuant to the provisions of Art. 4 (1) (1) and (5) in conjunction with the provision of Art. 5 (2) (2) of LPPD, the State Agency for the Bulgarians Abroad should provide the Ministry of Justice with the files on the certificates of Bulgarian origin issued by the Agency and containing personal data of applicants for Bulgarian citizenship through naturalization.

Furthermore, in 2013 CPDP expressed an opinion in connection with a request filed by the Chairperson and the Secretary of the Central Election Commission in connection with the parliamentary elections.

The first question concerned the need for registration in CPDP of the nomination committees for independent candidates for parliament members. The Commission indicated that the nomination committees for independent candidates for parliament members under Art. 96 (2) of the Election Code are data controllers and they are required to be registered with CPDP.

The second question was related to the forthcoming parliamentary elections and the amendment and supplements to the Election Code adopted in February 2013 according to which the CEC has new obligations. In relation to the new obligation to broadcast the meetings of CEC in real time on the Internet, CPDP delivered an opinion that it is lawful and permissible considering the legal obligation set with the new provisions of the Elections Code and the performance of a task which is in the public interest in order to aknowledge the public with the important issues discussed at the CEC meetings.

An important CPDP's opinion of public interest was the opinion in connection with the right of access to maps of restituted property and cadastral maps along the route of the project South Stream Gas Pipeline, as well as to the registers kept with those maps. A question was raised about the possibility of providing information on current ownership data along the gas pipeline route and the following data: full name, personal number and address of the owners and holders of other real rights over these properties. After examining the received request and after taking into account the exceptional public importance of the

project, the Commission ruled that there is a condition for admissibility of the processing – implementation of a task carried out in the public interest. The data of the individuals should be processed in strict compliance with the principles of appropriateness and proportionality of data, i.e. the data processing should involve the required minimum amount of data according to the objectives, and the nature and type of data should be consistent with them. South Stream Bulgaria AD, as a data controller, should fulfil its legal obligations to notify the individuals whose data are to be processed. The processed personal data should refer to the specific individuals only – the owners or holders of other real rights over real estates located along the route of the gas pipeline. In cases where there is a statutory time limit determined for the processing of data, they should be processed within that time limit. In cases where there is no such time limit, the data controller is required to process the data for a period no longer than the period necessary to achieve the purposes for which data were received. The data controller should set the time limits for carrying out periodic reviews on the need to process data and on the deletion of personal data, whereas the measures and time limits for this purpose are determined by the instruction of the data controller.

A question of substantial financial interest on which the Commission expressed its opinion was the implementation in Bulgaria of the Foreign Account Tax Compliance Act of U.S. taxpayers, adopted by the U.S. Congress - FATCA. The request was filed by the representatives of a bank based in Bulgaria, part of a multinational company. The main purpose of FATCA is to enable the U.S. tax authorities to combat cross-border fraud of U.S. persons with accounts and financial assets abroad. This objective will be achieved by building a global system for automatic information exchange which imposes an obligation on all foreign financial institutions to provide information to the American Internal Revenue Service (IRS) about all accounts of U.S. taxpayers or foreign companies that are owned by U.S. taxpayers. Thus FATCA creates numerous new obligations for all foreign financial institutions. After a thorough analysis, CPDP assumed that due to

the fact that at this moment for the Bulgarian bank there is no regulatory obligation to provide personal data of its customers–individuals subject to the U.S. tax law to another data controller in the United States relating to the implementation of FATCA, there is no legal basis for CPDP to allow data transfer to the United States. Data transfer based solely on the consent of the individuals would be excessive and contrary to the principle of the legality of the processing of personal data because of the lack of regulatory basis to require the consent of the individuals.

Provision of data to third countries

During the reporting period the trend for reduction in the number of requests for authorization of third countries personal data transfers under LPPD continued, which is due to the amendments made in 2012 to the Rules of Procedure of CPDP and its administration. As a result of the lighter regime for third countries personal data transfer, data controllers are only required to notify the Commission on all cases of transfer based on standard contractual clauses or adequacy decisions. In this connection, the Commission received 13 notifications and 12 requests for authorization for third countries personal data transfer. Usually the transfer of data was to third countries. Authorization for transfer of personal data was requested for the following countries: Mexico, the Philippines, India, Brazil, China, Malaysia, Australia, Canada, Chile, Colombia, Guatemala, Japan, Kenya, Korea, New Zealand, Peru, USA, Singapore, Costa Rica, Hong Kong, Switzerland, Russia, Serbia, the Republic of South Africa, Taiwan, Thailand, Turkey, Ukraine and Vietnam. This year again the reasons for the provision of data stated by data controllers include outsourcing, consolidation of activities for the purpose of human resource management, investigation of signals for corruption, etc.

For the first time in 2013, the Commission received a request for authorization of personal data transfer based on the application of the so-called binding corporate rules. Binding corporate rules constitute a global code of

practice based on the European data protection standards drawn up by multinationals companies and voluntarily complied with by them aiming at providing adequate measures for the data transfer between the companies within the corporation. They have been created as an additional tool for data transfer in addition to the standard contractual clauses, and their regulation is foreseen in the Working Documents of the Article 29 Working Party. With regard to the data transfer to companies outside the corporation, located in third counties, the standart contractual clauses, adopted European Commission decisions continue to be applied.

These rules apply to all companies included in the corporation, regardless of their location (inside or outside EU/European Economic Area (EEA)), nationality of the persons whose data are processed, or any other criteria.

The Article 29 Working Group believes that if these rules are mandatory (in legal and practical aspects) and bring in all the required data protection principles, there is no reason the national data protection authorities not to allow transfers between companies belonging to a multinational corporation in accordance with their national legislation.

Since this legal instrument is not known in the Bulgarian legislation, in this particular case the Commission authorized the transfer of data pursuant to Art. 36b of LPPD, namely on the basis of the evidences certifying undertaken contractual obligations that the data controller providing data and the data controller receiving data provide sufficient data protection guarantees.

IX. Training in the field of personal data protection

In 2013, the Commission continued its purposeful training activity, and there were three main focuses in the training plan:

- Training of large data controllers;
- Training of professional organizations;
- Training conducted jointly with partner institutions.

In this regard, during the reporting period 10 training workshops were conducted, including 3 training courses for professional organizations, 3 workshops with state institutions, 4 workshops jointly with training partners. The total number of persons trained is 372 data controllers and data processors.

1. Training of professional organizations

One of the focuses in the training activities set by the Commission for 2013 is the training of professional organizations. It is a good practice identified during the exchange of experience with foreign partners of the Commission in the implementation of the Leonardo Da Vinci Mobility project and put into practice by CPDP. The training of professional organizations allows for better unification of standards and data protection practices of all members of the organization, as well as wider dissemination of learning outcomes. The coordination and logistics of the representatives from the country are also facilitated by the conducting of professional organizations training.

In 2013 training was conducted for the Association of Banks in Bulgaria, Bulgarian Hotel and Restaurant Association, International Banking Institute and the Bulgarian branch of the European Law Students' Association (ELSA).

Association of Banks in Bulgaria

On 14 May 2013, the Commission for Personal data Protection carried out training of the employees of 23 of the leading banking institutions in the country. The event was held jointly with the Association of Banks in Bulgaria.

The event was met with great interest and attended by representatives of: Association of Banks in Bulgaria, Corporate Commercial Bank, Crédit Agricole Bulgaria, Municipal Bank, Bulgarian-American Credit Bank, Eurobank Bulgaria, Allianz Bank Bulgaria, DSK Bank, Central Corporative Bank, First Investment Bank, International Asset Bank, Societe Generale Express Bank, Citibank, ProCredit Bank Bulgaria, Cibank, TBI Bank, MKB Unionbank, D Commerce Bank, Tokuda Bank, Raiffeisenbank, United Bulgarian Bank, Unicredit Bulbank, Piraeus Bank.

The topics of the training included discussions on the current personal data protection legislation and the imminent introduction of a common EU legal framework in that area with the Council Regulation on personal data protection. The discussions were related to the data controllers' basic obligations for lawful processing of data and issues relating to the new Ordinance 1 of CPDP dated 30 January 2013.

The lecturers of CPDP acquainted the trainees with case studies of the Commission concerning the processing of personal data in the context of banking.

Bulgarian Hotel and Restaurant Association

On 21 May the officials of the Commission for Personal Data Protection carried out a training course for the Bulgarian Hotel and Restaurant Association.

The trainees showed a keen interest on the personal data protection measures, the methods of data storage and destruction, the data processing principles. They stated their gratitude for the understandable and clear presentation of the material and expressed hope for continued joint cooperation, including via conducting trainings in the country.

European Law Students' Association (ELSA)

On 26 April was organized a training, jointly, with ELSA Bulgaria - European Law Students' Association. The event was attended by 66 law students from various Bulgarian universities who demonstrated a strong interest in personal data protection and privacy issues. The trainees asked both theoretical questions on

the legal framework and case studies and inquiries about the loan borrowers and their rights, the access to personal data collected by video surveillance, authorization of employees to collect personal data, the practice of banks and mobile operators on personal data collection and processing.

ELSA Bulgaria expressed their appreciation for the training and the efforts of speakers and they declared their readiness to continue the fruitful cooperation with the Commission for Personal Data Protection. The Commission was awarded a certificate for outstanding service to the European Law Students' Association ELSA Bulgaria.

2. Training of state institutions that are large data controllers

In 2013, the Commission identified the need for training personal data controllers which maintain a substantial volume of data arrays. This is conditioned by both the need to ensure the necessary protection level of the processed personal data by the respective administrators and by changes in the legislation, in particular Ordinance 1, according to which the appropriate level of protection is directly related to the number of persons that may be affected by unlawful processing of their personal data.

Regarding this category, in 2013 training was carried out to the following data controllers: Agency for Child Protection, Bulgarian National Bank and Directorate General "Civil Registration and Administrative Services".

State Agency for Child Protection

On 25 April a training course was organized for the officers of the State Agency for Child Protection. During the training, assistance was provided to the officers of the agency and instructions were given for drafting new internal instructions of the data controller which should comply with Ordinance 1 dated 31 January 2013. The trainees asked questions about the rules for handling sensitive personal data, transfer of children's data to third countries and measures necessary for the protection of the information funds.

Bulgarian National Bank

On 21 June Commission's experts conducted a training course for the data processors at the Bulgarian National Bank, which was attended by over 40 officers from 15 administrative units of the bank, who deal with maintaining data registers.

The trainees were introduced with the main aspects of the personal data processing, focusing on a number of practical issues. For this purpose, the experts of CPDP conducted a practical exercise with representatives of the Bulgarian National Bank aimed at preparing an impact assessment on the registers maintained by the bank.

The trainees highly appreciated the training, and the practical examples, in particular, received extremely positive evaluation. A recommendation was made for the future trainings to include more information on issues related to the implementation of the new Ordinance 1 on the minimum level of technical and organizational measures and admissible type of personal data protection.

Directorate General "Civil Registration and Administrative Services"

On 4 July in the building of CPDP was conducted another training course included in the annual training plan intended for data controllers and processors. It was attended by representatives of the Directorate General "Civil Registration and Administrative Services".

The trainees raised questions related with the performance of their professional duties such as: destruction of personal data arrays, drafting internal rules, applying for different types of personal data registers, third parties data transfer. The trainees showed a particular interest in the topics related to the implementation of Ordinance 1 on the minimum level of technical and organizational measures for personal data protection and the trends for development in data protection field.

3. Training of data controllers conducted jointly with training partners

In 2013, the Commission relied on the implementation of best practices in its

training plan aiming to increase the level and effectiveness of the conducted training. These practices are identified and summarized in a catalogue of best practices thanks to a project under the Leonardo da Vinci Programme. One of them refers to conducting joint training with partners who are specialized in the field. This form of cooperation is particularly beneficial for the Commission as it reduces some of the difficulties in the learning process, namely the use of human resources for the coordination of training and of financial resource – for the provision of materials.

In 2013 the Commission established cooperation with two training organizations - the International Banking Institute and the Institute of Public Administration.

International Banking Institute

On 25 June the Commission conducted advanced training for the employees of commercial banks jointly with the International Banking Institute. It was attended by 20 trainees from the following banks: Raiffeisen Bank, Piraeus Bank, First Investment Bank, International Asset Bank, Crédit Agricole Bank, Allianz Bank, Municipal Bank, DSK Bank, United Bulgarian Bank.

The training was specialized - on matters relating to the implementation of Ordinance 1 on the minimum technical and organizational measures for personal data protection, and advanced - it was attended by the bank employees who attended the personal data protection training conducted on 14 May 2013, organized with the assistance of the Association of Banks in Bulgaria.

The trainees highly assessed the training, stating that the presented case studies and examples and the focus on topics specific for the banking sector have contributed significantly to increase their understanding and knowledge in the data protection field.

Institute of Public Administration

At the invitation of the Institute of Public Administration three training courses were organized in 2013 jointly with the Institute of Public Administration, 1 for managers and 2 for experts. They were attended by representatives of the central and local government of Bulgaria. For the first time this year the Institute included in its training catalogue a training module on the EU policy on personal data protection, legal regulation and practice in Bulgaria. The training intended for civil servants was highly appreciated.

4. Statistics and trends

When analysing the feedback surveys for the evaluation of the training course the following results may be summarized (Fig. 8)

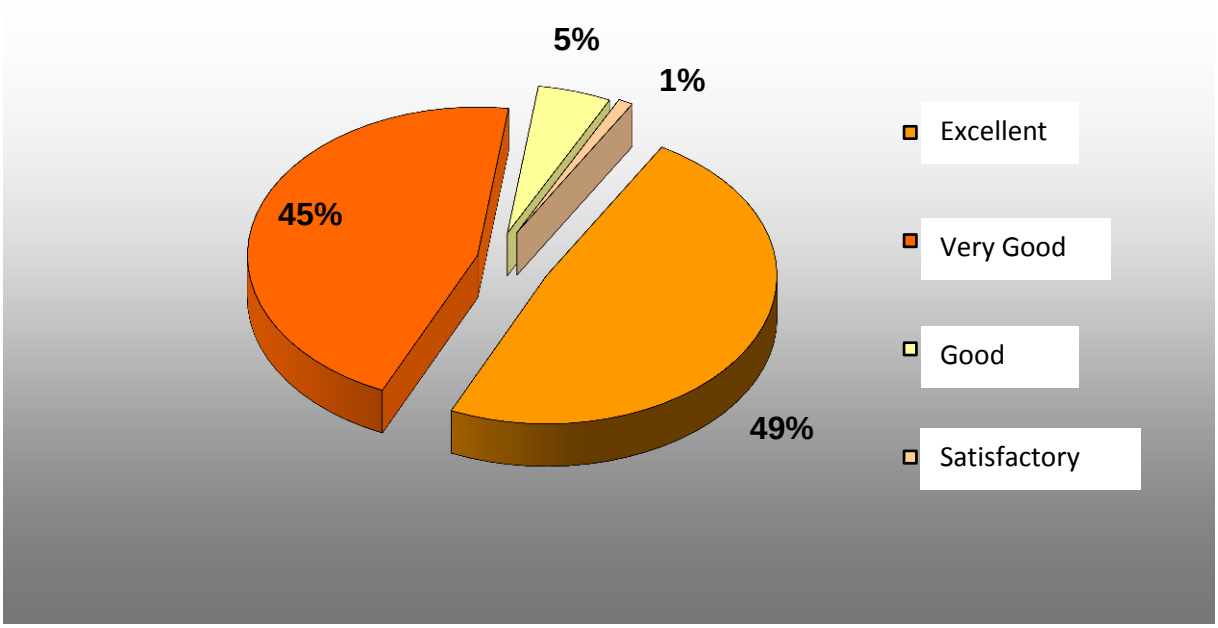

Fig. 8

When comparing the results of the training with the results of the preceding years 2011 and 2012, it may be concluded that the Commission succeeded to significantly increase the level of efficiency of its training courses. This is a result of the adaptation of training programm in accordance with the accumulated recommendations in previous years. The topics of the lectures in 2013 are optimized and updated to include the latest trends in the data protection filed. More

examples were included and case studies and role plays were developed. Specialized trainings were designed and conducted, namely: for the implementation of the new Ordinance 1.

This was highly appreciated by the participants in the training - the percentage of trainees evaluated the training as "Excellent" has almost doubled. At the same time the number of trainees who have assessed the training as "Good" decreased almost four times. 28% of the trainees who have completed the feedback questionnaires answer the question "What do you most like about the training?" by indicating "The practical examples and case studies", other 16.4% - "The accessible presentation on the matter" and "The practical orientation of the training".

5. Implementation of projects with national and international funding

The Commission for Personal Data Protection is the only supervisory authority on personal data protection in Bulgaria. Due to limited funding from the national budget, CPDP strives to improve its operation and raise the quality of services by attracting European funding. This pursuit of the institution is in line with the national policy followed by Bulgaria regarding the use of the opportunities provided by EU funds.

Regarding the development and management of projects, year 2013 was the most successful year in the history of the Commission. This year marked the successful completion of a project launched in the previous year and the conclusion of contracts for funding of another 3 projects, amounting to BGN 335,961. The total number of projects managed by the Commission's experts in 2013 is 5 under two different European programmes with a total value of contracts amounting to BGN 384,413.

5.1. Leonardo da Vinci Programme

Leonardo da Vinci Programme is a programme that supports and carries out the policy on professional education and training of the EU member states by

complying with the content and organization 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 gained experience. Two projects of the Commission were approved within the frame of 2012.

"Exchange of experience in the conduct of training in personal data protection field" Project, "Leonardo da Vinci" Programme, Activity: "Mobility"

The Commission's project started in August 2012. The amount contracted with the Managing Authority was EUR 13,720. The deadline for the implementation of the project was by the end of July 2013. The main part of the implementation of the project proposal, namely: the exchange of experience with partners from the Polish and German supervisory authorities was carried out in November 2012. In 2013, the participants in the project proceeded with analysing the exchanged experiences and with drafting a Catalogue of Best Practices in Training, which may be used in the work of the Commission. This catalogue was drafted and in June 2013 the Commission carried out an event to announce the outcomes of the project to all employees of the Commission. The announcement of the outcomes included a workshop where the employees were introduced with the training activities of the partner organizations under the project, the best practices identified were presented and a discussion was carried out with questions and answers.

In an official letter in October 2013, the Managing Authority of the programme informed the Commission that recognizes all expenses incurred by the Commission in full, and thus the project proposal was officially closed.

"Raising awareness of the persons working on 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 CPDP is EUR 11,000 and the deadline for the completion of the project is July 2014. Partners of CPDP under this project are 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. The project implementation covers 6 working meetings in the partner countries under the project, which should lead to the development of a Handbook for personal data protection for persons on the labour market. The Handbook is intended to be used by the individuals looking for work or working in the European Union and aims to increase their understanding of issues related to the protection of their personal data. The publication includes the legal framework and practical data protection issues, but also provides advice to individuals.

Three meetings were held under the project in 2013 - in Split (Croatia), Sofia (Bulgaria) and Prague (Czech Republic). The attendants of these meetings specified the format and type of the handbook, its content is almost finalized and English version of the publication is completed. The final version of the handbook is to be released in the summer of 2014.

5.2. Projects under the Operational Programme "Administrative Capacity"

"Administrative Capacity" is one of the seven operational programs for the programming period 2007-2013. It is directed to the state administration and aims to improve its operation 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 professionalism, transparency and accountability in the judicial system. In 2013 the Managing Authority of the programme approved 3 project proposals of the Commission.

Project entitled "Improving the management, organization and functions of the Commission for Personal Data Protection by conducting a functional analysis"

The funding contract for the project was signed on 6 February 2013 and amounts to BGN 213,829.91. The project aims to improve the management, organization and functioning of the Commission for Personal Data Protection. The main activity of the project is to carry out a functional analysis of the Commission in order to identify opportunities to improve its performance and optimize the structure and business processes within the organization.

In 2013 the project team was formed and 3 procedures were conducted for the selection of contractors of the project activities. The implementation of the functional analysis started in the autumn of 2013, which was outsourced to a contractor selected via an open procedure under the Law for Public Procurement.

The project is to be completed by June 2014.

Project entitled "Promoting the professional development of the employees of 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 amounts to BGN 34,647. The project aims 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 will undergo a series of training courses chosen by the employees, aimed at enhancing their professional competence. In 2013, over 20 employees of the Commission participated in over 10 training courses under the project.

The training of the employees of CPDP will also continue in 2014. The project is scheduled to be completed by 4 July 2014.

Project entitled "Strengthening the administrative capacity of the Commission for Personal Data Protection for working with databases, information systems and team work"

The contract for this project was signed on 4 July 2013 and amounts to BGN 34,647. The project also aims to improve the professional competence of the employees of the Commission for Personal Data Protection (CPDP) for more effective and efficient performance of their duties, but unlike the previous one, this project is aimed specifically at employees of the Informational Funds and Systems Directorate. Under the project the Directorate's employees will participate in various training courses to improve their team work, increase their skills to work with Windows 2008 web-based systems and Oracle.

The procedure for the outsourcing the project activities was initiated in 2013. The project is scheduled to be completed by July 2014.

Project entitled "Improving and expanding electronic services to businesses and individuals by the Commission for Personal Data Protection, and integrating them with a single point of access to e-services"

At the end of 2013 the Commission was awarded the implementation of a project entitled "Improving and expanding electronic services to businesses and individuals by the Commission for Personal Data Protection, and integrating them with a single point of access to e-services". The project implementation is scheduled to start in 2014, and the outcome of its application is expected to improve the quality of services provided by the Bulgarian data protection supervisory authority and enhancing the efficiency of its work. The project is worth BGN 391,089.38.

X. Personal data protection reform

The large-scale legislative package, proposed by the European Commission in early 2012 was subject to extensive debates in the European Parliament and the Council which also maintained their intensity in 2013. There are high expectations to the reform package that includes a general Regulation[1] on data protection and a separate Directive[2] in the police and justice field. These expectations to fill the gaps in the existing EU legislation relating to data protection in the Internet, and to send a strong signal to the international community that Europe wants and is capable to overcome the national differences and administrative obstacles and to impose unified directly applicable protection standards, which subsequently will cause a domino effect worldwide. The European legislation can play a crucial role in the future determination of the international data protection rules, which when linking the largest possible number of participating countries will impose a coordinated and effective regulation on the movement of the primary commodity of the digital economy - the information.

This European legislative reform includes changes both in the current Directive 95/46/EC[3] of the European Union and in the Convention 108[4] of the Council of Europe, which, in turn, has the potential to become the first international data protection instrument interned to invole third countries in the modernization process.

[1] Regulation on the protection of individuals with regard to the processing of their personal data and the free movement of such data (General Regulation on Data Protection)

[2] Directive on the protection of individuals with regard to the processing of their personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data

[4] Convention 108 of the Council of Europe of 28 January 1981 for the protection of Individuals with regard to automatic processing of personal data

The Consultative Committee on Modernisation of Convention 108, set up to supplement and amend the current text of the Convention completed its work in 2013. The newly proposed provisions are to be voted by the dedicated Ad hoc Committee, where the leading Bulgarian institution is the Commission for Personal Data Protection. The position of the Commission for Personal Data Protection in the preceding consultations and in the current voting process is to achieve a high protection level and maximum consistency and compatibility of the legislative reforms at the Council of Europe and the European Union level. At the same time, the neutral character of Convention 108 should be preserved without creating a detailed legal framework, which is the purpose of this international instrument. An important issue that requires further discussion are the requirements for the third countries data transfer.

The proposal for a General Data Protection Regulation in the European Union continues to be a serious legislative challenge. The draft regulation is considered both in the European Parliament (EP) and the Council. In 2013, the relevant EP Committee of "Civil Liberties, Justice and Home Affairs" (LIBE) presented its report /link to LIBE/, which includes a significant number of revisions to the original proposal of the European Commission. The Member States are also actively working on the text proposed by the European Commission, and in 2013 the draft regulation underwent a number of amendments – currently only in the draft form.

There are several principal issues that can be taken from the general discussion plan. First, the central point in the debate remains the finding of a balance between the different national practices – administrative and judicial, the individuals' rights and business needs. It should be highlighted that there is a need for higher flexibility in the public sector through the introduction of exceptions in certain provisions of the proposed Regulation in order to ensure the consistency of the state policy in many areas.

The debate covers the practical application of the data protection rules in the Internet and the need for a more complete description of modern communication technology, respectively opportunities to respond to them. Last but not least, a key aspect that has an effect on a number of mechanisms of the Regulation proposal is the so-called principle of "one stop shop" of data controllers, respectively the determination of the competent data protection supervisory authority and the role of the future European Data Protection Board.

The Bulgarian positions on these and other aspects of the draft Regulation are prepared by the Commission for Personal Data Protection. On a technical level, the discussion of the draft is carried out in the Working Group on Information Exchange and Data Protection (DAPIX) to the Council, where the Bulgarian participants are the representatives of the Commission for Personal Data Protection. Due to the fact that at political level the main guidelines, on the principles and mechanisms set in the Regulation proposal, are adopted by the Ministers of Justice in the Justice and Home Affairs Council, in the format of Ministers of Justice, the official position of Bulgaria is coordinated with the Ministry Justice, as far as this legislative dossier is always subject to consideration by the Justice and Home Affairs Council.

The general position of Bulgaria is that the in future Regulation must be maintained high standards for the protection of individuals. The "size" of personal data controllers should be taken into account using various incentives and exemptions, but not at the expense of the exercise of the fundamental protection right. The independence and powers of the national supervisory authorities should be preserved and strengthened, including within the framework of the coordination mechanism between the supervisory authorities and the determination of the leading authority. Provisions should be included for the maximum preservation of the intended amount of the penalties which should have a deterrent effect by extending the other provided preventive measures - recommendations and written warnings.

XI. National and international cooperation

At the national level, in 2013, the Commission for Personal Data Protection carried out coordinated actions with a number of government agencies on international issues.

Extremely active is the interaction of CPDP with the Ministry of Justice. Due to the current nature of the European data protection reform, this legislative dossier is on the agenda of the Justice and Home Affairs Council in the format of Ministers of Justice. The position of Bulgaria developed by the Commission for Personal Data Protection as the competent body in this filed, is approved by the Council on European Affairs and the Council of Ministers and is submitted to the Minister of Justice. Very good contacts are established between the two institutions at expert and political level, which ensure the necessary timeliness and quality of the Bulgarian positions.

Interaction in various directions is exercised with the Ministry of the Interior. This year, the Commission for Personal Data Protection noted the rise of the inquiries concerning the processing of personal data in the second generation Schengen Information System (SIS II). The inquiries are generally related to the refusal of deletion of personal data in SIS II and requests for advice on the exercise of rights towards SIS II. While considering the inquiries, the Commission for Personal Data Protection requires the inspection of the respective cases by the SIRENE National Bureau. We are pleased to note out the timely operation of the Bulgarian SIRENE Bureau for provision of information on the received signals.

In response to an inquiry of the Schengen Joint Supervisory Authority, the Ministry of Interior provided a report reflecting the executed transition from SIS I to SIS II and the compliance with the data processing requirements in SIS II.

The cooperation takes place on a regular basis also under the operation of Article 23 Working Group (home affairs). It should be noted the contribution of the Commission for Personal Data Protection in the analysis of objectives and legislation listed in No. 2013/0218 (COD) "Proposal for a Regulation of the

European Parliament and of the Council adapting to Article 290 of TFEU a number of legal acts providing for the use of the regulatory procedure with scrutiny". The overall assessment of the Commission was that the automatic adaptation of the regulatory procedure with scrutiny to Art. 290 of TFEU is not appropriate.

The Commission periodically performs an exchange of views with the State Agency "Archives" in relation to the concerns of the Agency about the negative effect of the implementation of the future Data Protection Regulation on the archives. The considerations of the Agency are adopted by CPDP and expressed in the appropriate formats at EU level.

Given the general view of the Member States that the proposal for Data Protection Regulation would have adverse effects on the process of processing and storing data for historical and research purposes, an approach has been adopted at European level for the introduction of appropriate exemptions from the application of the Regulation in this area.

In 2013, the Commission for Personal Data Protection continued its active participation in the process of preparation, revision, co-ordination and implementation of European data protection and privacy legislation, as well as, in the information and experience exchange bilaterally and at European and global level on existing and newly emerged issues.

Furthermore, CPDP provided advice and answers to a number of individual inquiries and investigations of Bulgarian and foreign individuals and organizations in connection with the application of the Bulgarian and European personal data protection legislation, and in particular, on the use of video surveillance, raising the awareness of citizens about the protection of children personal data, strengthening the cooperation between data and privacy protection authorities, data processing in the banking sector, etc.

Active cooperation at national level is also carried out in connection with the introduction of Regulation 611[5] of the European Commission, effective as from 25 August 2013 and the need to provide secure communication channels for announcing data breaches. In this context, at the initiative of CPDP a number of meetings with representatives of the State Agency "National Security" were carried out. As a result of the meetings, the parties agreed on a comprehensive technological solution which was presented at a meeting organized by the European Commission on 18 September on the implementation of the Regulation. The current technological solution, involves the creation of a protected website for secure communications with providers of electronic and communications networks and/or services. The meeting organized by DG "Internal Affairs" was attended by Prof. Veselin Tselkov, member of CPDP.

The Commission for Personal Data Protection is a partner and co-beneficiary, and the State Agency "National Security" - the leading structure of the project "Establishment of a national unit for collection and processing of PNR data in the Republic of Bulgaria" funded by the European Commission. The project activities start in early 2014.

A representative of the Commission for Personal Data Protection participated in a meeting organized by DG "Internal Affairs" of the European Commission, which aimed to find a common EU approach to the transfer of passenger name records (PNR) data at the request of third countries. At present, the transfer of this data type is implemented on the basis of bilateral agreements. With the increasing number of third countries which introduce PNR systems, it is necessary to look for new solutions to this issue, given the cumbersome and lengthy procedure of negotiating bilateral agreements. The general view of the Member States is that a unified legal instrument should be developed which should be legally binding on its adherent parties.

[5] Regulation 611/2013 of the European Commission on measures applicable to the notification of security breaches of personal data under Directive 2002/58/ for the right to privacy and electronic communications

In pursuance of the decision of the Article 29 Working Group under Directive 95/46/EC, the Commission for Personal Data Protection posted on its website a set of documents relating to the right of individuals to access their personal data relating to the Terrorist Finance Tracking Programme (TFTP). The documents are prepared under the TFTP Agreement and described in detail the access procedure.

Other priorities of the Article 29 WP in which various documents have been prepared and submitted for voting by the Member-States include: data protection by undertaken police actions and criminal justice; software applications for smart devices, principle of puropose limitation of personal data processing; drafting and implementation of binding corporate rules for data processors; protection of personal data and smart metering systems; collection and processing of personal data by electronic devices installed at the border points (smart borders); use of public sector information and consent when installing cookies.

Other important issues discussed within the Article 29 Working Party in 2013 are: achievement of higher flexibility about the data protection in the public sector, using pseudonymised data, expressing consent, the new mechanisms proposed for coordination and cooperation, international transfers and assessing the impact on the personal data protection, the transfer of PNR data, etc.

During this reporting period CPDP continued to participate in the Joint Supervisory Authorities of Europol, Schengen and Customs. The main directions of their activities in 2013 related to: checks of various specialized systems used in the framework of police and judicial cooperation and the fight against terrorism; state of national units – the introduction of new devices and systems; review and analysis of the current legislation and future amendments thereto; preparation and distribution of information materials in connection with their work; creating a single point of access to the systems.

It should be noted that in 2013 the Joint Supervisory Authority of Schengen ceased its activity, and a new structure was set up in its place that will exercise

control on SIS and in which Bulgaria is a full member even though the process of accession to the Schengen at national level has not yet been completed.

The Commission for Personal Data Protection takes active part in the work of the specialized Supervision Coordination Groups of the special information systems – Schengen, Customs, Visa and Eurodac, created at the European Data Protection Supervisor, and in the context of the information exchange, discussions conducted and requests for opinions sent, the following issues have been discussed: information management in large-scale information systems and ensuring their security, quality of the data that is submitted into them; access of law enforcement authorities at national and European level – taking into account that access and work with the systems; inspections carried out, including joint inspections by the supervisory data protection authorities; recent developments in systems following the ongoing changes worldwide.

In 2013, the Management Body of the Commission for Personal Data Protection participated in numerous international forums, outlining key data protection trends.

In March, the Chairperson of the Commission, Ms. Veneta Shopova took part in an academic conference, the subject of which was the principle of providing informed consent via the Internet.

Main priorities of the European data protection authorities in the preparation for the International Conference on Privacy were discussed during the so-called Spring Conference. This year's conference was held on 16 and 17 May in Lisbon and it was attended by Ms. Veneta Shopova and Mr. Valentin Enev, a member of CPDP.

Representatives of the Commission for Personal Data Protection in the International Conference of Data Protection and Privacy Commissioners (Warsaw, 23 to 26 September) were Ms. Mariya Mateva and Mr. Veselin Tselkov, members of CPDP.

On the two annual meetings of the International Working Group on Data Protection in Telecommunications (15 to 16 April in Prague and 2 to 3 September in Berlin), and on the IV International Conference on Data Protection, organized in November by the Russian Federation (6 to 7 November, Moscow), the Commission for Personal Data Protection presented the new rules introduced in Ordinance 1 on the minimum measures and the admissible level of protection.

Representatives of the Commission participated in the workshops, addressing the problems to "accountability", which was held in Warsaw and Toronto. The representative of CPDP in this project is Prof. Veselin Tselkov, member of CPDP.

Following the priorities to strengthen the cooperation at regional level, in May, the Commission for Personal Data Protection hosted a meeting with a delegation of the National Data Protection Authority of Kosovo, held in pursuance of the Memorandum of Cooperation signed in 2012.

The management body of CPDP participated in the annual Conference of the Central and Eastern European Data Protection Authorities, which this year was held in Belgrade from 10 to 12 April.

XII. Institutional interaction and cooperation with higher education institutions and NGOs. Public relations and publicity and transparency policy Partnership with media representatives and information activity.

In 2013 the Commission for Personal Data Protection continued to develop effective cooperation with both international and national institutions, and representatives of higher education institutions and non-governmental organizations in the country.

CPDP, represented by its Chairperson - Ms. Veneta Shopova, took part in the discussion organized by the Council for Electronic Media on the subject matter of "Protecting Individual Privacy in the Business of Media Service Providers", which was held on 21 February 2013 in Matty Hall, National Palace of Culture.

In her speech Ms. Shopova emphasized the demand and the establishment of the desired balance between the right to privacy and the constitutionally protected right to freedom of speech and the public interest. She discussed a number of case studies of the Commission for Personal Data Protection. At the discussion the Chairperson of CPDP explained that the complaints of individuals against media are significantly less in number than the other complaints that are received and reviewed by the Commission.

The event was attended by relevant specialists from different fields - psychologists, social researchers, media experts, human rights defenders, civil associations, electronic and other media. The discussion initiated by the Bulgarian media regulator addressed the following issues: when the two constitutional rights intersect; where is the boundary between the in depth disclosure of data and the editorial responsibility for respecting the privacy; when the intrusion in the privacy is justified and how much is the weight of the public interest; how to show children and mentally ill and whether the consent of their relatives actually ensures protection of their interests.

CPDP was a co-organizer of the conference "Protection of Personal Data in the Context of Information Security" together with the National Military University "Vasil Levski" - Faculty of Artillery, Anti-Aircraft Defence and Communications and Information Systems, Department of Information Security, and the State Commission on Information Security. The event was held on 6 and 7 June 2013 in the town of Shumen.

The Chairperson of the Commission for Personal Data Protection - Ms. Veneta Shopova, presented a paper entitled "State policy in the sphere of personal data protection".

"The implementation of the state policy in the personal data protection field is a continuous process that involves effective functioning of the supervisory authority at the national level, assessment of public attitudes, application of adequate prevention and exercising enhanced control. An important element of the policy is the undertaken actrions aiming at awakening the self-responsibility of all parties involved: individual - data controller - supervisory authority." said the Chairperson of CPDP.

She briefly introduced the participants in the forum with the status, the general and specific powers of the institution and the components constituting the state policy in the data protection field. Special attention was paid to the thematic and sectoral approach in the analysis of problems and the adequate prevention in this area. Different methods and initiatives were discussed, which are used by the Commission in the exercising of its preventive activities – educational and information campaigns, coordination policy with other government institutions, imposition of uniform data protection standards.

"The third major component of state policy is the increased control. It runs independently and in parallel to the preventive activities. It may be planned, to be implemented according to the particular case, or to carry out follow-up monitoring. The aim is strict compliance with the mandatory provisions of the law, in order to prevent the repetition of certain malpractices and irregularities", revealed Ms.

Shopova and presented a number of mechanisms used by the supervisory authority to exercise its control functions.

In her report, the Chairperson of CPDP covered the current European legislative reform in the personal data protection area, the main purpose of which is to ensure the protection and security of data without hampering their freedom of movement. "Europe is on the verge of introducing the first high, uniform personal data protection standard, applicable to all international companies offering goods and services in the European internal market and which will find its projection in both national policy and the practice, and in privacy taking into account the emerging global networks", concluded Ms. Shopova.

The report of Prof. DScC Veselin Tselkov - Member of the CPDP, entitled "Minimum technical and organizational requirements for the protection of personal data" addressed some of the major problems associated with the new information technology and the protection of personal data, and the new fundamental definitions are based on NIST SP 800-145, dated September 2011.

In the context of new challenges, taking into account the modern European and international trends in the personal data protection field (complying with the term "big data", the right to be forgotten and conducting impact assessment), the Commission adopted a new Ordinance 1 on the minimum level of technical and organizational measures. It defines a new terminology, such as: objectives and data protection type, assessment and impact level, and objectives of data protection – ensuring their confidentiality, integrity and availability. To relieve the businesses and citizens, the impact analysis is limited to the comparison of potential adverse effects with standard situations, already recognized as threats and described as levels of impact.

Data protection in the context of information security is the main focus of the revision of the existing legislative framework. It is expected that in the final version of the draft general Personal Data Protection Regulation the principles for data processing will be extended with a new principle: data processing should be

done in a manner that ensures adequate security of data and their privacy, revealed the report of Prof. Tselkov.

The event in the town of Shumen was opened by Prof. Manol Mlechenkov, DScMil, and the greeting of Assoc. Prof. Nelko Nenov, PhD – Dean of the Faculty of Artillery, Anti-Aircraft Defence and Communications and Information Systems – Shumen. Reports and presentations were also given by representatives of Protection of Classified Information Directorate at the State Commission on Information Security, the Commission for Communications Regulation and the Law and Internet Foundation.

The conference was attended by the interim governor of Shumen Region – Ivailo Iliev, the local public mediator at Shumen Municipality – Ivan Kapralov, representatives of Information Security Directorate at the Ministry of Defence, State Agency for National Security, Executive Agency for Electronic Communications Networks and Information Systems at the Ministry of Transport and Communications, the Ministry of Interior, the Administrative Court - Shumen.

The program of the event also included work by scientific sections – State and Security, Information Security, and Student-PhD, which were attended by managers, teachers, students and doctoral students at the National Military University "Vasil Levski", Shumen University, Veliko Turnovo University and Bourgas Free University.

Year 2013 was full of working visits with foreign delegations in order to intensify the co-operation between the Commission and the similar European authorities. The overall preparation and organization of the international visits, as well as the provision of favourable conditions for work and recreation of guests, testify for the successful selection of strategies of the institution for building and maintaining effective public relations and the protocol activities.

Following the policy of openness and transparency established over the years, the Chairperson and the Members of the Commission for Personal Data Protection "opened doors" for all interested citizens, data controllers and media

representatives on the Personal Data Protection Day - 28 January. On this date in 1981 the Member States of the Council of Europe signed Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data.

Every year CPDP celebrates the Personal Data Protection Day by conducting events and various initiatives on different scale with the active public participation.

Many citizens, data controllers and media representatives took advantage of the opportunity to ask specific questions, to get expert answers and relevant information on personal data protection issues.

In the open reception of CPDP they were met by representatives of all specialized departments of the institution, who carried out consultations and provided legal assistance on cases related to the Law for Protection of Personal Data, as well as information on the European and international personal data protection legislation, Schengen information System and clarifications on the procedure for registration of data controllers and the register maintained by CPDP - eRALD.

For the first time this year, in order to celebrate the event, CPDP created a Skype account to directly connect with citizens and media representatives. This is part of the Commission's policy for development and enhancement of the online communication forms. As part of activities organized on the occasion of 28 January, the Commission for Personal Data Protection also presented a summary of the Annual Report on its activities for 2012.

In 2013, the initiatives on the privacy protection were also supported by maintaining sustainable and fruitful relations with national media representatives. Electronic, print, and internet information channels were providing the CPDP messages to the public, allowing the maximum number of people to raise their awareness on the issues affecting their personal data.

In 2013, thanks to the already existing facilitated and more personalized contact between the Commission and the media representatives, over 150

interviews and materials with the participation of the Chairperson, members and experts of CPDP became possible. The continuous cooperation of the institution with the reporters led to the publication of a significant number of information materials and journalistic investigations, which affect various personal data protection aspects. Successfully built and maintained media relations provided a reliable channel for distribution of useful news and initiatives that will mark the work of the Commission in the future.

Raising public awareness is assessed by the Commission as the main prevention measure for maintaining security in today's society. Therefore, during the reporting period the institution continued its successful and effective measure fot preparation, printing and distribution of thematic information brochures in Bulgarian and English, containing useful information. They reach the interested parties through the reception of CPDP, the events and meetings organized, as well as the participation in international forums and visits by the representatives of the institution abroad.

In order to continue the information campaign launch in early 2012, CPDP prepared, updated and additionally printed 2,000 copies of brochures in Bulgarian on the topic: "Video Surveillance" and "Who Can Copy Your Identity Card", 2,000 copies of brochures in English on the topic: "Personal Data in Schengen", "Video Surveillance – Your Rights" and "Internet and Children".

XIII. Administrative capacity and financial status

1. Administrative capacity.

During the reporting period, the Commission for Personal Data Protection used its best efforts to implement the Commission's priorities for the protection of personal data set out in the annual plan for 2013.

During the reporting period CPDP made business contacts and cooperated with representatives of the Institute of Public Administration at the administration of the Council of Ministers, with representatives of the State Commission on Information Security, Ministry of Finance, National Audit Office, Ministry of Defence, National Revenue Agency and National Insurance Institute.

The total staff numbers in 2013 is 87.

Employees employed under full-time contracts for the period from January to December 2013:

Under official contracts - 52;

Under labour contracts - 18.

Vacant positions:

Under official contracts - 15;

Under labour contracts - 2.

Employees employed within the period from January to December 2013 - total 4:

Under official contracts - 2;

Under labour contracts - 2.

Terminated labour relations as follows:

Under official contracts - 7;

Under labour contracts - 4.

Reappointed employees:

- Under official contracts 2 (replacing absent employees);

Change of service:

- promoted in rank – 1;

- promoted in position – 2;

1.1. <u>Training of employees in accordance with the plan, approved by CPDP</u>

For the Commission for Personal Data Protection, the administration staff traning is an important element of the human resources management.

As in previous years, in 2013, the basic principles foreseen by the CPDP for the training and qualification of the administration of the Commission were as follows:

- **Adequacy –** planning and conducting training corresponding to the need in the respective units, leading to increased quality at work;
- **Timeliness –** training should correspond to the changes in legislation relating to the CPDP activities and the best national and international practices;

During the reported period priority was given to those training courses that would increase the work efficiency and contribute for the achievement of the CPDP's objectives.

In March 2013, Annual Training Plan was drafted and approved with two main activities:

- Mandatory training – for staff appointed for the first time as civil servants – 5 newly recruited civil servants at expert position were trained;
- Specialized training – for professional development and qualification rising. The Annual Plan provides for the training of 23 employees.

For the reported period, the main institution to execute the Commission's scheduled staff training was the Institute of Public Administration (IPA) to the Council of Ministers.

In April 2013, the Commission for Personal Data Protection was awarded a project under OPAC, Priority Axis: Human Resources Management, Sub-priority: Competent and Efficient Public Administration – "Promoting the professional development of the employees of CPDP by applying a system of training according to their professional duties", No. CA 12 22 56 dated 9 April 2013.

The project provides for 33 training courses, which will be attended by 43 employees of the administration for the total of 166 trainings.

The selection of employees to be trained under the project was made after an analysis of the current practice and the training scheduled in the CPDP's 2013 Annual Training Plan. This was done to avoid double funding using the following criteria:

- The employee should have not received training on the same topic;
- The training should be related to the duties arising from the employee's position;
- The training should contribute to the professional, career and personal development of the employee concerned.

Employees of CPDP administration also took part in trainings organized by other institutions on specific topics related to the activities of the Commission, namely:

- "Management of occupational health and safety" - 1;
- "Closing of accounts and taxation of budget entities for 2012. Changes in tax laws for 2013. Financial audit." – 1;
- "Appeal of administrative acts under APC" - 5;
- "Law on Financial Management and Control in the Public Sector" - 1;
- "Training of beneficiaries on the practical aspects of project management under OPAC" - 6;
- "Training in providing comprehensive administrative services" - 2;
- "Law on Financial Management and Control in the Public Sector and its current practical application" - 1.

The total of **63** employees of the CPDP's administration participated in trainings for enhancing their qualification and professional development under the Annual Training Plan and the project under OPAC.

In order to enhance the administrative capacity of the CPDP's employees in the reporting period, workshops were organized for the employees on the following topics:

- The boom in information technology and the new privacy and personal data protection challenges; Methods for evaluation of information security, lecturer Prof. DScC. Tselkov, member of CPDP; and Ordinance on the minimum level of technical and organizational measures and admissible type of personal data protection, presented by the working group assigned for its preparation;
- Presentation of the outcomes of project "Exchange of experience in the conduct of training in personal data protection field" under the "Leonardo da Vinci" Programme, Mobility Module 2012-1-BG1 – LEO03-06870, to the employees of the Commission for Personal Data Protection;
- Trends and developments in data protection (35th International Conference of Data Protection and Privacy Commissioners) and Technological Solution of CPDP for the implementation of the obligations under Regulation 611/2013, lecturer Prof. DScC Tselkov, member of CPDP, and the Law on Electronic Communications and Regulation 611/2013 EC, lecturer D. Toshkova, Director of Legal Affairs, Training and International Cooperation Directorate at CPDP.

1.2. Analysis and evaluation of the effectiveness of the conducted training.

All the employees of the Commission's administration, after completing various training courses, prepared reports and completed questionnaires that served as a basis of analysis and adequate reporting of the training results.

The analysis of the employees' participation in training workshops showed that the separation from the work process has not affected the performance of the employees' duties. In general, the effectiveness evaluation of the trainings conducted indicated a connection between the training process and the performance of CPDP's tesks, objectives and priorities.

Reporting on the training efficiency under the OPAC project is provided as part of the activities under the project, which is scheduled to be completed in 2014.

1.3. Training funding

The training courses for CPDP's employees scheduled under the Annual Training Plan are financed by the funds provided from the state budget.

The training on the project "Promoting the professional development of the CPDP's employees by applying a system of training in accordance with their professional duties" is financed by OPAC.

1.4. Evaluation of the performance of the employees of the CPDP's administration

The evaluating of the performance of the CPDP employees takes place annually following the rules set in the Ordinance on the conditions and procedures for evaluating the performance of the employees in public administration (OCPEPEPA).

The process of evaluation of employees (under official and employment contracts) of the CPDP's administration provides objective information to the evaluating manager on:

- the level of professional qualification of the staff in the manager's unit, and the conformity of the professional qualification with the requirements stipulated in the job descriptions;
- improving relationships in the work process, including between superiors and subordinates, and improving teamwork;
- creating conditions for the implementation of fair and transparent procedures for professional and career development of the CPDP's employees.

During the reporting period, evaluations on the performance of 61 employees were prepared in 2012. Such evaluation was not carried out for 13 employees, because 6-month absence during the evaluation period.

The individual work plans of 70 employees were prepared and coordinated, and no plan was prepared for 4 employees, because of their prolonged absence (maternity leave - 3, extended unpaid leave - 1).

During the period from 1 July to 15 August 2013 an interim meeting was held between the evaluation managers and the evaluated employees (total 68 employees). Upon completion of the interim meeting, the completed evaluation forms were stored in the files of the employees.

1.5. Conducting competitions for vacant positions in CPDP's administration

During the reporting period, no new completions were announced for filling vacancies in the administration of CPDP.

1.6. Job descriptions

In accordance with the Ordinance on the job descriptions of civil servants and the Ordinance implementing the unified classification of administrative positions, all administrative job positions in CPDP have job descriptions. Their last update was as of August 2012, reflected changes in the public administration regulatory requirements. During the reporting period, 1 job description had to be amended or supplemented.

1.7. Development of internal regulation documents

During the reporting period significant amendments were made to the Public Procurement Act. In this regard, a draft of new rules governing the procedures of public procurements was developed and approved by the Chairperson of CPDP.

The lawful and proper implementation of the amendments to the regulations also required appropriate amendments to the CPDP's internal regulation documents. In this regard, a draft of internal rules for human resources management and development was prepared in CPDP.

1.8. Public Procurement

During the year the Commission carried out 9 procedures of public procurements in compliance with the requirements of the Law on Public

Procurement. Of these, 4 are related to the execution of approved projects under the Operational Programme "Administrative Capacity".

After the successful implementation of these procedures, contracts were executed with the selected contractors. The files of the completed public procurements are completed and archived in accordance with the requirements of LPP and the Internal Rules of CPDP.

2. Budget

With the Law for the State Budget of the Republic of Bulgaria (LSBRB) for 2013 and the Council of Ministers Decree No 1 dated 9 January 2013 on the implementation of the state budget of the Republic of Bulgaria for 2013, the operating budget of the CPDP was approved to the amount of BGN 2,700,000.

During the year the budget of the Commission was increased by BGN 18,430 as it was adjusted by the Ministry of Finance in connection with concluded contracts for granting financial support for the projects Mobility and Partnership under sectoral programme "Leonardo ad Vinci", Lifelong Learning Programme of the European Union.

Pursuant to the Council of Ministers Decree No. 75 dated 29 March 2013 on the restructuring of non-interest expenditures in the national budget for 2013, the budget of the CPDP was reduced by the amount of BGN 24,900.

After these adjustments the budget of the CPDP amounts to BGN 2,693,530.

The costs incurred for ensuring the activity of the Commission for Personal Data Protection and its administration amount to BGN 2,514,960, or 93.37 % of the approved estimated for the year. The types of costs distributed by sections of the Unified Budget Classification (UBC) are presented in the following table:

Section	Name of expenses	Amount (BGN)
01-00	Salaries and wages for staff employed under labour and official contracts	1,040,847
02-00	Other remunerations and staff payments	72,037
05-00	Compulsory social securities paid by employers	268,028
10-00	Allowance	1,117,178
52-00	Acquisition of tangible fixed assets	16,870
	Total budget expenditures	2,514,960

XIV. Conclusion

In the context of the activities carried out by the Commission for Personal Data Protection in 2013, the focus of future work shall be to finalize the European data protection reform at international level and to ensure its implementation - nationwide.

This involves the implementation of targeted information and training activities for raising awareness of the public about the expected trends in the European data protection policy: introduction of the position of "data protection officer", providing services to individuals and businesses on the "one stop shop" principle; self-reporting of data controllers.

As before, for the implementation of this preventive policy, the Commission for Personal Data Protection will rely on good cooperation with partner institutions and stakeholders.

The annual report for the activity of the Commission for Personal Data Protection in 2013 was adopted by a decision of the Commission at a meeting held on 15 January 2014 (Minutes of meeting No.1).

CHAIRPERSON:

Veneta Shopova /Signed/

MEMBERS:

Krasimir Dimitrov /Signed/

Valentin Enev /Signed/

Mariya Mateva /Signed/

Veselin Tsekov /Signed/