TABLE OF CONTENTS

Summary

The purpose of this report is to give an overview of the overall activity of the Commission for Personal Data Protection for the year 2011 in its major area of competence. The report has been drawn up pursuant to Art. 7, Para. 6 of the Law for Protection of Personal Data (LPPD) and covers the period from 01.01.2011 to 31.12.2011. The report starts with an analysis of the 2011 CPDP priorities. Consequently are presented the powers of the Commission, arising from the LPPD and the Law on Electronic Communications (LEC), the registration process of data controllers and the registers kept by them, as well as analysis of the practice adopted by the Commission regarding the handling of complaints and its supervision activities. An overview is given of the key opinions expressed by the Commission, the third countries' data transfers subject to authorization by the Commssion and the training carried out in the personal data protection fileld. Special attention is given to the CPDP co-operation with other government bodies at national level and the international co-operation with similar supervisory authorities, the readiness of the Commission to exercise supervision on personal data processing in the Schengen Information System with respect to the expected accession of the country to the Schengen Area. The report provides an overview of the national supervisory authority contribution to EU personal data protection policy. The Commission's administrative capacity and financial status during the year are also presented.

I. Analysis and report on the extent to which the priorities of the Commission for Personal Data Protection, as set out in the 2010 Annual Report, have been fulfilled.

During the reporting period CPDP made every efford to fulfill the Commission's priorities, set out in the 2010 Annual Report. The main focus that year was on the carrying out of training in the personal data protection field for specific target groups. The Commission continued its traditional educational activity developed in the past years, and even developed a large-scale information campaign - realized with own financial and human resources and adapted to the specific needs and requirements of data controllers. In pursuance of the annual training plan, 22 seminars and training courses were held with the participation of 481 employees from 106 institutions and organizations. A key priority with respect to the training activity was the series of seminars designed for data controllers and personal data processors having access to the National Schengen Information System. The training of personal data controllers and processors having access to the N.SIS was one of the compulsory measures included in the National Action Plan for the full application of the provisions of the Schengen acquis and for the abolition of the control at the external borders.

Another key priority for 2011 was the fulfillment of the CPDP's obligations as supervisory authority regarding data security according to the Law on Electronic Communications. In compliance with its legal obligations for the first time the Commission summarized and submitted to the European Commission and the National Assembly statistical information on cases of access to retained traffic data and launched an initiative for holding regular meetings and consultations with all parties involved in data retention process at national level and undertakings providing electronic communication networks and/or services.

Another priority of the Commission for the year 2011 was to actively participate in the work of the the European bodies and institutions with respect to the privacy and personal data protection. Special attention was paid to defining the main areas and parameters that require revision of in the European data protection legal framework.

One of the significant aspects of Commission's work at the EU level was related to the data protection

in the telecommunications, which was realized with the participation in a specialized public consultation of the European Commission in connection with the transposition of legal instruments on data protection in this area at national level.

A permanent task in 2011 was the constant communication of the Commission with similar supervisory data protection authorities. In order to share best practices and co-operation in solving similar cases during the year numerous inquiries and information were exchanged on issues concerning the practical application of the Schengen Convention's provisions, personal data protection with regard to video surveillance, the transportation of official documents containing personal data by mail and couriers, etc.

An aspect of the policy to raise citizens' awareness regarding their data protection rights was the carrying out of wide-ranged educational and information activities. To achieve this objective, aimed mainly at raising the awareness among young people, in 2011, the Commission approved and adopted information and educational platform dedicated to the threats on the Internet and intended for children and parents. Taken into account the importance of this objective, it will remain a priority in the future activity of CPDP as well.

In 2011 CPDP successfully continued the specialized national information campaign launched in 2010 dedicated to raising the level of awareness among the citizens of the Republic of Bulgaria regarding their data protection rights in the country and in the Schengen Area. With the co-operation of state bodies and structures, as well as of NGOs, the distribution of foreign language versions of 20 000 information leflets- in English, German, Serbian, Russian, Turkish, French and Spanish – was completed.

The official websute of CPDO is the main tool used for information and contact with citizens. During the reporting period, pursuant to the priority of the institution to carry out valuable and effective educational activities among different target groups of the society, CPDP published on the website and in its newsletter various information reflecting events and facts relating to the personal data protection in order to achieve and maintain an adequate awareness level among Bulgarian citizens as to the national and European personal data protection regime, as well as their rights and obligations under the LPPD. The Commission's website was updated with new, more detailed information about citizens' rights related to the processing of their personal data in the Schengen Information System.

II. Powers of the Commission for Personal Data Protection pursuant to the LPPD and pursuant to the Law on Electronic Communications

1. Pursuant to the LPPD

1.1. Expressing opinions

The overall activity performed by CPDP in its daily work is aimed at establishing clear rules and the application of uniform requirements for the personal data protection. An important tool for support and effective supervision with regard to data controllers is the power of the Commision to express opinions on the processing and protection of personal data. Many of the cases on which the Commission was approached in 2011 and has expressed an opinion on the application of the LPPD, refer to a large group of data controllers as these opinions are used to explain specific legal requirements and to decide on principle matters,with regard to the personal data protection. This type of opinions of the supervisory authority is crucial, especially because they are used to create clear and transparent criteria for the uniform application of law by all who have obligations under it. Despite of that, during the reporting period continued the practice of expressing opinions on specific issues related to the activity of a particular data controller, and the opinion expressed by the Commission in these cases is individualized depending on specific characteristics.

1.2. Co-ordination of the laws and regulations

Besides the official opinions on matters within its competence, in 2011, the Commission has regularly been approached with respect to the co-ordination of draft regulations pursuant to Art. 32, Para. 3 of the Rules of Organization of the Council of Ministers and its administration.

1.3. Personal data protection training

The CPDP is the only personal data protection supervisory authority in the Republic of Bulgaria and being such, it seeks to apply uniform rules in this area. The main tool for achieving uniform data protection standards is to conduct compulsory training in the personal data protection. In 2011, the Commission continued and expanded its

work on the data controllers' training, launched in previous years. In 2010 amendments to the LPPD were promulgated and these amendments legally established the Commission's competence to conduct and develop training activities. This function of the CPDP was included in Art. 10, Para. 1, Item 12 of the LPPD, stating that the Commission organizes and coordinates personal data protection training.

1.4. Exercise of the individuals' rights

It is worthy to be noted that this year the citizens are more aware of the need to protect their personal information and approach the Commission with issues of various nature not only when they believe their rights have been violated, but also to obtain competent opinion in relation to the processing of their personal data and the data of their families.

In 2011, the CPDP received the total number of 346 inquiries from data controllers and individuals on personal data protection matters. The two main forms of communication are e-mail messages and CPDP website – www.cpdp.bg.

The most important issues may be structured as follows:

• **Regarding the data controllers registration:** In order to meet the obligation for submitting registration applications in the Register of data controllers and the registers kept by them, in 2011, the CPDP received a large number of inquiries made by state institutions, the Central Election Commission, municipal and regional election commissions, businessmen, NGOs, exchange offices, real estate agencies, advertising agencies, persons engaged in electronic commerce, auditing firms, accounting firms, nomination committees under Art. 96 of the Election Code (EC), companies located in third countries through their local representatives, branches of foreign banks, etc. The Commission was also approached by data controllers - individuals such as lawyers, experts and other freelancers.

• **Regarding the hard copies of identification papers:** The Commission responded to numerous inquiries from citizens whether specific data controllers may copy their identification cards, such as: banks, notaries, mobile operators, insurance and reinsurance companies, employers in relation to workers/employees and to job candidates.

• **Regarding the personal data provision:** The Commission notes that in 2011 there is strong public interest for the personal data processing in certain cases as follows: the provision of personal data by drivers of motor vehicles, upon payment of the vignette for the use of national roads in the country; upon the purchase of goods and services by credit cards through POS terminals buyers are required from vendors to present an identification card for identification purposes; from individuals by providing personal data as a prerequisite for the participation in games/lotteries; the right of persons who carry out security activities to require the presentation of identification cards by individuals upon their entry into protected buildings; individuals by the receipt of parcels/ registered mail by "Bulgarian Posts" EAD; electing individuals, voluntarily included in subscription lists, with which they support the participation of independent candidates in the elections; the requirement to provide a photocopy of identification cards of candidate trainees applying for enrollment in institutes of higher education; the right of doctors in hospitals for primary healthcare/doctors of dental medicine to require patients' personal data; the option for employers to implement a control system for the working hours through the collection of biometric data from workers/employees with whom they are in professional relationships; processing by recording personal data with CCTV cameras monitoring a neighboring property; the practice of job employers to require from applicants to provide personal information about themselves and about their family; the requirement of some employers to job candidates to provide their "actual photo" when applying for a specific job position.

• **Regarding the personal data publication:** The Commission has repeatedly been approached whether the following is lawful: publication in the media of information representing "personal data" in notices of public sale of property, as well as whether personal data of the owner of the property, subject of sale, may be included - such as owner's full name, personal identification number, passport data, address; free access to personal data of persons entered in the Commercial Register, the publication of personal identification numbers in invoices issued to subscribers/clients.

• **Regarding the personal data provision to third parties:** In 2011, the Commission found that more and more citizens inquire about whether the following is lawful: provision of personal data of users/subscribers to third parties in order to collect irredeemable debts; provision of personal data to third parties used for direct marketing purposes, and what are the rights of individuals in these cases.

• **Regarding the submission of a request for data transfer:** Due to the globalization of world economy, many Bulgarian and foreign companies approached the Commission with respect to: what are the requirements that requests for data transfer to third countries must meet; how can requests be made; what information and evidence should be presented by the requesting party in connection with the initiation of administrative proceedings before the CPDP under requests for data transfer; what is necessary in connection with the authorization procedure for the personal data provision in a third country recepient.

• **Regarding the personal data erasure:** In order

to strengthen the data controller's commitment to their obligations under the LPPD, in 2011, the Commission was also appoached with inquiries concerning who has the right to erase personal data and what is the procedure for the personal data erasure.

2. Pursuant to the Law on Electronic Communications

Directive 2006/24 (Data Retention Directive) was transposed into the Bulgarian legislation through amendments to the LEC in 2010. With the enactment of these amendments all parties involved in the data retention process and traffic data access were legally determined and the CPDP was designated as supervisory authority on data security. In the fulfillment of its powers under the LEC, in 2011 for the first time the CPDP summarized and submitted to the European Commission and the National Assembly statistical information in accordance with the required legal parameters within the period specified in the LEC.

Along with the analytical and summarizing activities, performed by the CPDP at national level in the period April-May 2011, in May the same year in Brussels was presented the European Commission's (EC) the report on the evaluation of Data Retention Directive transposition process into the legislation of the Member States. The overall conclusion of the EC in this report is that data retention is a valuable tool for the juridical systems and for the implementation of the legislation in the European Union (EU). Notwithstanding this overall positive conclusion, the EC found a number of problems: the Directive has not completely harmonized the data retention approach and has not created equal conditions for operators; there are significant differences between the Member States legislation in terms of objectives, data access, retention periods, personal data protection and the provision of statistical information. Therefore, in its report the EC encourages/recommends that Member States, besides statistical data and information, should provide EC with analysis of the usefulness of the received and retained traffic data; information about specific/individual requests for the access to such data; the age of the data should be given; a breakdown of statistical data by various indicators should be provided; as well as information whether retained data is crucial to criminal investigations and the judgment of convictions/acquittals. The general purpose of this EC call is to see the role of retained traffic data for criminal investigations, and its weight and respectively the influence on the outcome of the criminal proceedings.

On the basis of the above-stated analysis and EC conclusions, and taking into account the fact that the statistical information provided by enterprises in 2011 differs in the details, the CPDP decided to initiate the holding of meetings at national level with all parties involved in the data retention and traffic data access process in order to achieve clarity on all aspects on which the EC would like to receive information and analysis by Member States. Only when such information is available, the Bulgaria will be able to participate in the discussions on EU level and express a common national position and understanding on the issue concerning the future of the Directive and its amendment and the CPDP will also be able to provide national analysis of the usefulness and effectiveness of this tool and not only statistical information.

The purpose of the meetings, initiated by the CPDP, was to share the practice and difficulties in the implementation of the LEC by all subjects involved in the process, and also to discuss the possibility of providing (in addition to quantitative data) analysis and statistical information regarding the impact of retained data on the course of the investigation. In this connection, between September and December 2011 were organized and held four meetings between the CPDP and stakeholders as follows: with the authorities competent under the LEC, with enterprises providing electronic communications networks and/or services, with the prosecution and the court.

The Commission has discussed and clarified the following issues:

- Usefulness of information on retained traffic data for the detection and investigation of criminal offences, and respectively the search of people, as well as the judgment of convictions/acquittals;
- The possibility to provide analysis and consultation on specific types of criminal offences or the predominant type of criminal offences regarding which access to retained traffic data is most commonly requested;
- The possibility to summarize data on the legal basis and the purpose for which access is usually requested;
- The fulfillment of the obligation to keep records of the requests for access, denials, authorizations by the court and the information given;
- The option to provide information on cases where the period for data retention was extended with 6 months according to Art. 250a, Para. 5 of the LEC;
- Cases where the companies have denied the data provision;
- The period for which traffic data is retained (the so called data age);
- Clarification by the companies of the reporting period for provision of statistical information to the CPDP;
- Clarification of the option to submit more detailed information to the CPDP (breakdown of the time elapsed from the data retention until it was requested

by the authorities by months within the one-year data retention period, as well as by services' types);

• Explaining the procedures for access to traffic data retained under the rules and procedures of the Criminal Procedure Code for the purposes of pre-trial and legal proceedings;

• The possibility of the prosecutor in charge to exercise supervison on the actions of investigating authorities with respect to their right to request reports on retained traffic data;

• The cases of access to retained traffic data in trial procedures.

Having gathered and analyzed the enchanegd information, the Commission for Personal Data Protection has identified the particular areas of future work in order to provide in early 2012, binding instructions in accordance with of Art. 261a, Para. 3, Item 2 of the LEC.

III. Registration of data controllers and data registers kept by them. Status of implemented information and communication systems

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

In pursuance of the Commission for Personal Data Protection legal obligation to keep a public register of data controllers and data registers kept by them (hereinafter referred to as the "Register"), in 2011, the data controllers' (DC) registration process continued, as well as the procedures for exemption from registration and updating of the information about controllers already existing in the registry.

The system for electronic data controllers' registration (eRALD) automates all activities of the CPDP's administration by the process of registration of DCs and is accepted with increasing confidence by data controllers and individuals.

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

The overall maintaining of the three public CPDP's registers is in accordance with the concept of e-government to provide citizens with highly effective and easy to use online service, built on the "one stop" technology.

As of 31.12.2011 the total number of eRALD users reached 261 355, and 235 475 of them expressed their willingness to be registered as DCs, and 28 249 submitted applications for the exemption (Fig. 1) from the registration obligation. 2 369 are registered as DCs, but due to the narrowing of their activity or changes in the data processing circumstances, they have requested for exemption of registration and retained both their profiles (for registration and exemption) in the automated system. As a result of changed circumstances there are 2 369 DC profiles archived so far.

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

In 2011, the Commission approved and registered in the CPDP's register 42 911 DCs, of which 28 127 newly registered, and 14 784 updated the details of their existing registrations. 8 715 of the newly registered DCs submitted applications for entry in the register and 19 412 – applications for exemption from registration.

With the DCs registered throughout the year, the total number of DCs entered in the public register reached 135 497 data processors **(Fig. 2)**, and 26 627 exempted from registration **(Fig. 3)**.

In 2011 citizens continued to actively use the provided online service for the DCs registration. Of totally 28 127 newly submitted documents only 1 748 were submitted in paper forms.

Digital signatures are increasingly used by the submission of documents. The service is provided by the submission of registration applications and in 2011 from 8 715 applications in total, 1 695 were digitally signed via Universal Electronic Signature (UES) **(Fig. 4)**. The analysis of the data from previous years indicates growth by 3% of the use of universal electronic signature.

During the reporting period the CPDP also completed the electronic processing of the documents received in connection with the update of DCs data and the registers kept by them. 71 515 applications for registration and 63,941 confirmation papers were submitted online and prepared for processing. These are classified in archival boxes in accordance with the archival fund's requirements.

When the data controller applied for data processing under Art. 5, Para. 1 of the LPPD or for data, the processing of which by decision of the Commission threatens the rights and the lawful interests of individuals, the Commission must carry out prior checking before the registration under Art. 10, Para. 1, Item 2 pursuant to Art. 17b of the LPPD.

In 2011, 1 634 applications were submitted for inspection under Art. 17b before entering the data controllers in the CPDP's public register, bringing the total number of DCs registered after prior check to 5 387. The tendency these DCs to exercise their activities in the fields of healthcare, brokering and intermediation for job seekers and settlement, as well as security services is preserved.

The distribution of data controllers subject to inspection pursuant to Art. 17b of the LPPD in years is graphically shown in **Fig. 5**.

In 2011, continued the modernization of the data controllers' electronic registration system (eRALD). In the autumn of 2011, the Central Election Commission, along with all 264 local election commissions were registered as DCs and were given unique identification numbers in the CPDP's public register.

The created system architecture and the use of trusted networks for servers increase the reliability of the system and its information security.

2. Status of implemented information and communication systems

The Information Center opened in early 2010 by the Commission for Personal Data Protection has become an effective communication tool for the citizens in 2011. The Center answers to inquiries received by telephone (on average 1130 calls per month), via CPDP's web site and its official mail. In the second half of 2011, a competition was organized to achieve the highest possible degree of autonimization of the "Information Center" work. "Call Center Improvement" was implemented, allowing for even more beneficial contact with citizens and providing response on issues submitted by them.

After the holding of a tender procedure, a project for the conducting of paperless meetings was also realized, with indisputable economic impact.

A "Payroll and Personnel" automated system was also implemented for the CPDP's needs.

In 2011, the CPDP continued its professional contacts with the Executive Agency "Electronic Communication Networks and Information Systems", which is responsible for GovCERT Bulgaria (Bulgarian Computer Security Incidents Response Team), which is essential for the successful and trouble-free operation of the CPDP's information system.

IV. Complaints and requests submitted. Case law and practice of the Commission. Analysis of judicial practice.

1. Analysis and statistics of complaints and requests submitted under Art. 38,Para. 1 of the Law for Protection of Personal Data. Case law and practice of the Commission.

In accordance with its powers to carry out comprehensive control on the compliance with data protection regulations, including with the requirements of the Law for Protection of Personal Data, the Commission for Personal Data Protection examines requests submitted by individuals with claims for legal violations.

Upon submitting requests, seeking protection of violated rights of the requesting party, the Commission for Personal Data Protection initiates proceedings for complaints handling under Art. 38, Para. 1 of the Law for Protection of Personal Data. In accordance with the legal requirements, complaints must be submitted by a person who seeks protection of his/her rights within one year after finding out about the claimed violation, but not later than five years of its execution.

Upon the receipt of requests that do not contain data about violated rights of the requesting party, steps are adopted for conducting inspections and giving compulsory instructions to data controllers concerning the personal data.

In 2011, the Commission was approached with 458 complaints, signals and inquiries concerning personal data processing and the possibilities for exercising the rights for protection against unlawful personal data processing or the rights of access, information, correction or personal data blocking.

A significant part of the claims are connected with contractual relations between individuals and data controllers and the personal data processing in this regard. It should be noted that in some cases the Commission was addressed to assist for the termination of these relationships or their settlement in connection with the provision of a particular

service. Individuals have complained about the calculation of amounts due under contracts, about exceeded payments for the use of telecommunication services, comparing personal data by the purchase of medical goods or goods with special sales regime, etc. In those cases individuals received information on how they should protect their rights, in so far as personal data processing by or in connection with a contractual relationship is permitted under the Law.

The next category of requests addressed to the Commission concerns issues regarding the protection of the individuals' rights and the procedures for exercising the statutory rights of access to personal data or the procedures for approaching the Commission in the cases of violation of the Law.

To the requests, concerning the individuals' protection were prepared and sent detailed answers.

Taking into account the fields of activities of thr data controllers against which most of the complaints have been submitted by individuals, the following can be distinguished:

Telecommunications, information society sector	199 complaints;
Media sector	8 complaints;
Healthcare sector	5 complaints;
Banks and banking institutions sector	27 complaints;
Insurance services sector	11 complaints;

In 2011 at its regular meetings the Commission has considered 38 complaints inadmissible and 20 - invalid and the administrative proceedings related to them were terminated. Six complaints of this category were received in 2010.

Two of the decisions for complaints' inadmissibility were challenged in court by the individual, and in one of the challenges, the decision of the Commission has been confirmed, while in the second case the Administrative Court – city of Sofia annulled the administrative act, returning it to the Commission for further administrative proceedings.

The main reasons for the termination of administrative proceedings due to inadmissibility or invalidity of the relevant complaint are the lack of requisites stipulated by the law, which guarantee that the complaint concerns a particular individual as the bearer of the rights under the Law for Protection of Personal Data. The lack of signature or authentication of the sender of the corresponding complaint may pose a risk of issuing a non-persistent administrative act, insofar as the right under Article 38, Para. 1 of the LPPD is personal and the lawfulness of the personal data processing is subject to administrative proceedings pursuant to Art. 2, Para. 1 of the LPPD or violations of rights set in Chapter Five of the same Law.

The next category of complaints that were considered inacceptable with regard to the procedure covers complaints from representatives of legal entities which do not indicate violations of the LPPD. Complaints are also considered inadmissible where they do no indicate the perpetrator and their subject makes it impossible for the authority to identify the potential perpetrator - data controller.

In all these cases, to the senders of inadmissible complaints were sent messages following the way the relevant complaint was received (by e-mail address, correspondence address, by phone or pursuant to the rules and procedures stipulated in Art. 61 of the Administrative Procedure Code, APC) with instructions, how to correct the deficiencies of these complaints.

Another reason for the inadmissibility of complaints is the presence of rights of foreclosure under Art. 38, Para. 1 of the Law for Protection of Personal Data.

During the year 8 administrative proceedings initiated with complaints were terminated due to their withdrawal. After clarification of the facts and circumstances about the claims for infringement of rights in the relevant complaints and due to the satisfaction of the complainants' requests, they invoke their right to withdraw their complaints. The complaint withdrawal is an absolute impedeiment for further actions by the administrative authority.

Administrative proceedings in 43 of the complaints, received in 2011, were suspended due to pre-judicial proceedings under Art. 54 of the APC.

The above-mentioned administrative proceedings were initiated after complaints of individuals, claiming that without their knowledge services contracts have been concluded, and besides approaching the Commission, individuals have approached investigating authorities for the presence of potential criminal offences.

During the year administrative proceedings was resumed and completed on a complaint, suspended in the same year and on a complaint for which administrative proceedings was resumed in 2010. The Commission ruled on these complaints, rejecting them as unjustified. Based on the evidence obtained in the administrative proceedings, as well evidence obtained later in preliminary proceedings, it was considered that there is no breach of the Law for Protection of Personal Data.

At its open meetings the Commission examined the grounds of 105 complaints. Of that figure 21 complaints were received by the Commission in 2010, and 3 were returned by the Supreme Administrative Court (SAC) after the reversal (partial or complete) of an administrative act already issued in this regard. From all resolved complaints, submitted on the ground of Art. 38, Para. 1 of the Law for Protection of Personal Data, 63 were rejected as unjustified given the absence of legal offences. In these cases it was found that the relevant data controllers

have processed personal data in accordance with the rules set in the Law for Protection of Personal Data. 42 complaints were considered justified, for 10 of them compulsory instructions were issued to data controllers to stop the actions violating the individuals' rights, or to adopt measures for future protection of the processed personal data.

On 31 complaints the Commission has imposed administrative penalties on the ground of Art. 38, Para. 2 in conjunction with Art. 42 of the Law for Protection of Personal Data for established offenses committed by persons in their capacity as data controllers. The administrative penalties amounted to BGN 441 500.

The sanctions imposed were for infringements as follows:

• Violation of Art. 2, Para. 2, Point 3 of the LPPD (principle of proportionality of the processed data) – administrative penalties imposed in the total amount of BGN 75 000 for 6 cases of established infringements.

• Violation of Art. 2, Para. 2, Points 1 and 2 of the LPPD (the principle of personal data processing for specific, clearly defined and legitimate purposes) - administrative penalties imposed in the total amount of BGN 119 000 for 5 established administrative violations.

• Violation of Art. 2, Para. 2, Point 6 of the LPPD (obligation of data controllers to keep the personal data processed in a form which permits identification of data subjects for a period no longer than is necessary for the purposes of processing) – 1 administrative penalty imposed in the amount of BGN 30 000.

• For the personal data processing with no admissibility condition present under Art. 4 of the LPPD - administrative penalties imposed in the total amount of BGN 154 000 for nine administrative offences established. One of the sanctions was revoked.

• Violation of Art. 23, Para. 1 of the LPPD (the data controller obligation to adopt appropriate technical and organizational measures to protect data against accidental or unlawful destruction or accidental loss, against unauthorized access, modification or disclosure, and against other unlawful forms of processing) - administrative penalties imposed in the total amount of BGN 48 000 for established 16 administrative violations.

• Violation of Art. 22, Para. 5 of the LPPD (the data controller obligation to assist the Commission in carrying out its supervising activity) - one administrative sanction imposed in the amount of BGN 6 000.

• Violation of Art. 24, Para. 4 of the LPPD (the settlement of the relations between the data controller and the data processor by the means of legislative act, written contract or another act of the controller, defining the scope of duties assigned by the data controller to the data processor) - 2 administrative penalties imposed in the amount of BGN 9 500, one of them was repealed by the court.

At present, a proprietary sanction was voluntarily paid in the amount of BGN 12 000, imposed on a data controller of the telecommunications sector for violation of Art. 4, Para. 1 of the LPPD for unadmissible personal data processing.

Two court instances rejected a complaint submitted by data controller from the Media sector against a decision of the Commission by which the data controller was imposed proprietary sanction in the amount of BGN 2 500 as a result of infringement of the requirements of Art. 23, Para. 1 of the LPPD for the adoption of technical and organizational measures to protect the processed data against accidental or unlawful destruction or accidental loss, against unauthorized access, modification or disclosure, and against other unlawful forms of processing.

The Supreme Administrative Court has partially amended Commission's decisions, with regard to the amount of the proprietary sanction imposed in 2 cases, and one of the judgments is appealed at a higher court instance.

One of the decisions of the Commission, which imposed an administrative sanction in the amount of BGN 5 000 for violation of Art. 24, Para. 4 of the LPPD and BGN 15 000 for violation of Art. 4, Para. 1 of the LPPD, was revoked by the Supreme Administrative Court, because the data controller provided the court with the necessary evidence to confirm that its relationship with the data processor were governed by contract, which defined the scope of duties assigned by the data controller to the data processor, as well as evidence for admissibility of the personal data processing under Art. 4, Para. 1 of the LPPD. In this particular case the data controller failed to comply with the instructions of the administrative authority to provide the mentioned evidence concerning its legal interest in the administrative proceedings.

In contrast to 2010, in 2011, the Commission imposed one administrative sanction under Art. 38, Para. 1 of the LPPD in the amount of BGN 6 000 for non-co-operation by a data controller by the carrying out the supervisory powers of the administrative body in the proceedings.

Two of the Commission's decisions in 2011 were not appealed – they imposed an administrative penalty in the amount of BGN 11 000 for infringement of Art. 2, Para. 2 and Art. 4, Para. 1 of the LPPD, and an administrative penalty in the amount of BGN 1 500 for violation of Art. 23, Para. 1 of the LPPD. In the first case the offense is committed by an individual in the capacity of data controller for illegal distribution of personal data and in the latter case the data controller is media that has not adopted measures to protect personal data against unauthorized access and distribution.

It should be noted that in 2011 the Supreme Administrative Court confirmed a decision of the Commission, which in 2010 imposed administrative penalties on two data controllers in the total amount of BGN 27 000 for violations of Art. 4, Para. 1 and Art. 34a, Para. 1, point 3 of the Law for Protection of Personal Data, made in the execution of activities for marketing purposes.

Actions were taken for the initiation of enforcement proceedings by the National Revenue Agency (NRA) on the administrative acts mentioned above.

With regard to the established infringements of the Law for Protection of Personal Data there is a predominant non-compliance of data controllers with their obligation under Art. 23 of the Law for Protection of Personal Data to adopt the necessary measures to protect data against accidental or unlawful destruction or accidental loss, against unauthorized access, modification or disclosure, and against other unlawful forms of processing.

Two times when the Commission was approached, it has established that the relations between the data controller and data processor were not settled in accordance with the provision of Art. 24, Para. 4 of the Law for Protection of Personal Data.

The infringements of Art. 4 of the Law for Protection of Personal Data are less in number, but not in significance. In the most general case, the violation occurs by the the provision of personal data by one data controller to another.

The provision of personal data as type of data processing should be done when a condition for admissibility exists. In most cases data controllers believe that the existence of statute under Art. 3 of the Law for Protection of Personal Data of the party providing the data and of the party receiving it is a sufficient condition for the lawful processing of personal data, which will be provided and respectively received.

The Commission for Personal Data Protection has handled a specific case of distribution of personal data of former employees. The Commission was approached with complaint from an individual that a former employer - data controller – has disclosed personal data (full name and personal identification number) of a large number of people by sending e-mail messages and faxes. The administrative procedure established that the manager of the company has ordered an office employee to send letters to the company's clients, which contain the complainant's data. The Commission has issued a decision, which respected the complaint and imposed on the data controller a proprietary penalty in the amount of BGN 15 000 for violation of the provisions of Art. 2, Para. 2, Point 3 of the LPPD. This resolution was appealed and the SAC amended the administrative act only with respect to the amount of the penalty imposed by specifying the minimum for this type of breach – BGN 10 000 and confirmed the remaining part of the decision. The court decision was also confirmed by five members of the SAC. On the ground of Art. 43, Para. 3 of the LPPD in conjunction with Art. 178, Para. 3 and Art. 220, Para. 1 of the Tax-Insurance Procedure Code (TIPC) the administrative act was sent to the NRA for the initiation of enforcement proceedings.

In 2011, entered into force the Commission's administrative act, which provides compulsory instructions to the NRA with regard to giving identification numbers of people working as freelancers. In that particular case, the Commission received a complaint by a working notary, who while performing his duties has a BULSTAT registration with a particular identification number. However, by his application for registration under the Value Added Tax Act, he is given a VAT number, which reproduces the personal identification number of the person. In the issue of each bill (invoice) for the purpose of authentication the applicant is required to enter his personal identification number for his value added tax number, thus making it available to any third party and this could lead to personal data misuse. The Commission considered that the complaint was justified and issued a compulsory instruction to the NRA to revoke the registration under the Value Added Tax Act performed by entering personal identification numbers and to perform registration with BULSTAT identifiers.

The NRA challenged the decision of the CPDP. The Supreme Administrative Court in its three and five members committees, confirmed the Commission's decision, acknowledging that the BULSTAT registration, received by the notary in 2000 was made on the grounds of the Law on Property (LP). With the enforcement of the Law on BULSTAT Register (LBR) on 11.08.2005, Art. 3, Para. 1, Point 9 governs the obligation of persons exercising the notaries' activities to register with the BULSTAT Register. According to Art. 6, Para. 3 of the same Law "The BULSTAT code of the persons, foreseen in the law shall have 10 digits and shall coincide with the Personal Identification Number (PIN)." Meanwhile, according to § 2, Para. 2 of the Transitional and Final Provisions of the LBR, individuals under Art. 3, who were entered before the enactment of this Law in the Unified registry for identification of business and other entities (i.e. BULSTAT Register within the meaning of Art. 31, Para. 1 of the LP), operating in the territory of the Republic of Bulgaria in accordance with the LP, shall be deemed registered under this Law and shall retain their identification code. The Court agreed that the personal data processing, namely, personal identification number in this particular case as user identification code – results in data dissemination and disclosure, and the data cannot be protected under the LPPD as in fact it becomes available to unlimited number of persons that cannot be

foreseen or controlled following the obligation of the controller, hence making it impossible to protect the data from unauthorized access and against unlawful use, distribution or processing. As a result, the individual's personal data, his/her unique personal identification number, used for his/her identification as an individual and person in all areas of legal life is practically unprotected against use and abuse and the data controller is not able to ensure the protection of the processed (used) data in the manner provided in the special law, which constitutes a serious violation of the latter and is an immediate threat to privacy.

In 2011 as well, the Commission was approached with complaints against printed and other media for the distribution of personal data, contained in private or official documents. This is the case for the dissemination of a part of the list of shareholders attending the General Assembly of a company. That list clearly stated the names and personal identification numbers of the complainants. The facts presented in the complaint, the information obtained in the course of the administrative proceedings and the opinions expressed lead to the conclusion that even though the processing of personal data of the complainants was made for the purpose of specific journalistic publication, the data controller - the media – has not taken the technical and organizational measures set in Art. 23 of the LPPD to protect the data against unauthorized access or disclosure. In this case, the Commission imposed an administrative penalty - a proprietary sanction in the amount of BGN 1 500 because, the media as data controller has processed complainants' personal data without taking the necessary technical and organizational steps to protect data against accidental or unlawful destruction or accidental loss, against unauthorized access, modification or disclosure, and against other unlawful forms of processing, which constitutes a violation of Art. 23 of the LPPD.

The next category of complaints on which the Commission has issued decisions in 2011 are related to the dissemination of personal data contained in judicial acts. Although the issue of publicity of the acts was discussed in the past few years, at present there are cases of non-personification of personal data in judicial acts too. In one of the administrative proceedings the relevant court reacted promptly and deleted personal data from the relevant acts. These actions motivated the complainant to withdraw the submitted complaint and the administrative proceedings were terminated pursuant to Art. 56, Para. 1 of the Administrative Procedure Code.

2. Analysis of judicial practice

In May 2011, the Law amending the Administrative Procedure Code altered the jurisdiction of administrative acts issued by the Commission on the ground of Art. 38, Para. 2 of the Law for Protection of Personal Data. In this connection, the Commission's decisions on complaints of individuals, concering the violation of rights during the processing of their personal data is covered by the jurisdiction of the Administrative Court, Sofia City. Simultaneously, proceedings connected with the appealing against Commission's decision, initiated before the Supreme Administrative Court before the amendment of Art. 38, Para. 2 of the LPPD were closed.

In 2011, 37 proceedings were initiated before the Supreme Administrative Court and 22 of them concern appeals against Commission's decisions, 11 legal proceedings were started on cassation appeals of the Commission against first instance judicial acts issued by the SAC, and 5 - on cassation complaints instituted against first instance judgments confirming the Commission's decisions. Two judicial acts issued by the Administrative Court, Sofia City were appealed before the Supreme Administrative Court and one of the judicial proceedings was closed with confirmation of the first instance judgment.

Currently, 10 of the initiated proceedings have not been closed yet, 8 of them as a result of appealing against the Commission's decisions and were considered by the SAC as the first instance, and 2 judicail acts considered by the second committee, were instituted as a result of a cassation appeal of the Commission and on a data controller – a company.

During the year, the Supreme Administrative Court of first instance annulled 13 administrative acts issued by the Commission on the ground of Art. 38, Para. 2 of the LPPD, and after a cassation appealing by the Commission five members of the SAC ruled judgments with which 7 of the Commission's decisions were left operating, and on 4 of the proceedings the SAC confirmed the judgment of the first instance court. In 2 of the lawsuits the issuance of the corresponding judicial acts is forthcoming.

From the decisions that were subject to judicial review, two were partially repealed, and one of the Commission's decisions was amended the amount of the imposed an administrative sanction – a proprietary penalty.

The main motives for the repealing the Commission's decisions are that there is no violation by the processing of the personal data of the complainant who have approached the Commission; and the complaints were confirmed by the administrative authority.

It must be noted that an inconsistent judicial practice exists with regard to the assessment on whether the supply of documents containing

personal data, provided by public authorities for the purpose of legal proceedings to people with advocacy's rights without a court order, violates the rules for personal data processing from the relevant authorities that have provided the personal information.

In its final decision the Supreme Administrative Court assumed that, the personal data processing is legal when the data subject consent is obtained or a court certificate on the relevant lawsuit, which should serve infront of the state authority for the issuing of the requested document containing third parties' personal data is issued.

In another case, however, the three members committee of the Supreme Administrative Court assumed that the provision of personal data to the legal representative of a party in a particular lawsuit was done for the purpose of the proceedings and the court as data controller also performed its obligations to protect the personal data of the parites. Therefore, although the legal represantive did not obtain a court certificate from the court where the case is pending and with which the representative could obtain the documents provided, there is no unlawful processing of personal data of the parties taking into account the purposes of the special law – LPPD, and the legal representative did not violate the provisions of the law.

Next, the court reviewed Commission's decisions issued in connection with the distribution of personal data contained in minutes of municipal councils. Regarding the complaints received, the Commission considered that the publication of minutes of meetings of the municipal council of the relevant website without deleting the personal information contained, e.g. personal identification numbers, addresses, etc. represents unlawful processing of data subjects' personal data. In this connection, the Commission issued a compulsory instruction to the municipal council in its capacity as a local self-government authority in relation to Art. 24, Para. 2 of the Law on Local Self-Government and Local Administration (LLSLA) to establish rules concerning the obligation of the mayor of the municipality with regard to the publishing of the minutes of the municipal council and the adopted decisions on the website of the municipality, stipulated in Art. 22, Para. 2 of the LLSLA and Art. 69, Para. 7 of the Rules for the organization and operation of the municipal council, its committees and its interaction with the state administration. The Commission noted that the rules must regulate the powers of the mayor of the municipality to delete individuals' personal data contained in the municipal council acts, in the minutes that are published on the relevant website. That practice of the Commission was confirmed by the Supreme Administrative Court.

Following the change in the jurisdiction of appealing the Commission's administrative acts from first instance by the Supreme Administrative Court to the Administrative Court, Sofia City, 18 lawsuits were initiated before the latter in connection with the appeal of Commission's administrative acts. The Administrative Court ruled on five of them, repealed four of the appeals lodged against Commission's decisions and annulled one of them. In connection with the refusal and appealing of the judicial act, was iniciated a proceeding in the Supreme Administrative Court. By ruling, the court members rejected the interlocutory appeal of the Commission on the ground of its procedural inadmissibility – it was brought within the preclusive period under Art. 230 of the CPC against judicial act subject to appeal by an interlocutory appeal, but by unrealiable party.

In 2011, there is a trend for increasing the number of the confirmed Commission's decisions issued on the legal grounds of Art. 38, Para. 2 of the Law for Protection of Personal Data. This circumstance is due both taking into account the case law and the guidelines on the application of the law by the issuance of the Commission's administrative acts, and the increasing number of administrative acts as result of the increase in the total number of referrals of individuals pursuant to Art. 38, Para. 1 of the Law for Protection of Personal Data.

V. 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 the CPDP and its administration (RACLPDP), Ordinance № 1 dated 7 February 2007 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 the Administrative Offences and Sanctions (LAOS).

During the reported period, the Commission exercised control activities in the following areas:

- analyzing the current data controllers activities with respect to the compliance to the personal data protection regulations;
- assisting data controllers with consultations and guidance on the compliance with the regulations, on measures taken for the protection of the processed personal data;
- exercising direct control on the personal data controllers in the public and private sector;
- imposing sanctions under the LAOS for violation of the LPPD.

The control is exercised directly by the Chairperson and the members of the Commission who are assisted by the specialized administration. According to Art. 26 of RACLPDP, the Law Proceedings and Supervision Directorate (LPSD) through its structural unit – Control and Administrative-Penal Proceedings Unit 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.

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 the LAOS.

Total number of inspections carried out – 1252, of which:

- ex-ante – 1151,
- on-going – 74,
- ex-post – 27.

This data shows that most ex-ante inspections were carried out on the grounds of Art. 12, Para. 2 of LPPD. 1252 inspections were carried out in 2011, resulting in 1227 statements of findings and 25 inspections ended only in drafting statements for ascertaining administrative violations.

For comparison: in 2010 total 1537 inspections were completed **(Fig. 6)**.

1.1. Ex-ante inspections

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

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

In 2011 a total of 1151 ex-ante inspections were carried out compared to1432 in 2010 **(Fig. 7)**.

Of all ex-ante inspections carried out in 2011, 1100 ended in proposals for registration in the register under Art. 10, Para. 1, Point 2 of the LPPD and ended in termination of the registration procedure due to termination of the respective data controllers operation. 6 compulsory instructions were issued and after their implementation personal data controllers were entered in the register under Art. 10, Para. 1, Point 2 of the LPPD, and 1 is in the process of implementation.

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 applications and failure to send the required documents after the proper notification receipt. Due to the impossibility of completion of these inspections, the CPDP reached a decision and on the ground of Article 17b, Para. 3, Point 3 of the LPPD rejected the registration of 797 data controllers in the Register of data controllers and

the registers kept by them. This is also the reason for the decreased number of completed inspections of this type in 2011. After the publication of CPDP's decision, 68 controllers of this category sent the required documents for ex-ante inspections, and 67 of them were entered in the register under Art. 10, Para. 1, Point 2 of the LPPD, and for 1 DC the procedure was terminated.

1.2. On-going inspections

Although considerably fewer in number, the on-going inspections carried out pursuant to Art. 12, Para. 3 of the LPPD are more complex in legal aspect. In 2011 the Commission carried out 74 inspections of this type, compared to 93 in 2010 **(Fig. 7)**.

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

In the beginning of 2011, the CPDP adopted a Plan for carrying out on-going inspections at the initiative of CPDP for 2011 (the Plan). In connection with the preparedness of the Republic of Bulgaria to join the Shengen area and the personal data processing by the competent authorities, an Addendum to the Plan was also adopted by decisions of the CPDP dated 03.08.2011 and 14.09.2011, covering inspections of state authorities applying the Schengen acquis.

The Plan aims at enhancing the efficiency of the Commission's control activity through its further administrative strengthening, improving the organization of the supervision, elaborating the methods for consulting personal data controllers and individuals.

According to the Plan, the checklist criteria for selecting data controllers (DCs) are the following:

- DCs, whose activity is of public and social significance;
- DCs processing personal data pursuant to Art. 5 of the LPPD;
- DCs, whose processing endangers rights and lawful interests of individuals;
- DCs, where considerable errors and irregularities have been established during inspections carried out in previous years;
- DCs, where no inspections have been carried out at all.

The main tasks of the scheduled inspections are connected with the performance of the data controllers' obligations under Art. 17, Para. 1, Art. 19, Para. 1, Art. 23, Art. 25 of the LPPD, as well as the determination of the technical and organizational measures undertaken to protect personal data and assessment of their compliance with the protection levels set in the Ordinance. The inspections mainly involve registers containing personal data of individuals, customers (contractors) of data controllers, according to their main business.

In accordance with the criteria adopted in the Plan, the Commission appointed inspections of 52 personal data controllers operating in different sectors of the social and economic life.

15 inspections were carried out of data controllers in the state administration sector in relation to the accession of Bulgaria to the Schengen Area – National Visa Center and Counsular Office of the Republic of Bulgaria in the town of Nish, the Republic of Serbia at the Ministry of Foreign Affairs, National Bureau of Europol, Bureu SIRENE, Migration Directorate, Chief Directorate "Border Police" and 6 border crossing points with the Ministry of Interior, State Agency for Refugees, 21 data controllers, providing tourist services in mountain resorts, as well as controllers whose activity is of high public and social significance – for example, the planned inspections carried out in the administration of the Ministry of Regional Development and Public Works (MRDPW), the National Statistical Institute, United Bulgarian Bank, 3 DCs in the insurance sector, 2 DCs in the public utilities sector.

As a result of the completed planned inspections 18 statements of findings were drawn up, 11 compulsory instructions were issued and 18 statements on ascertainment of administrative violations were drafted.

1.3. Ex-post inspections

The third type of inspections is performed under Art. 12, Para. 4 of the LPPD, namely ex-post inspections carried out in connection with the execution of CPDP's decision or compulsory instruction and at its own initiative after receiving a signal.

In the year 2011 27 ex-post inspections were carried out, compared to 12 inspections in 2010 **(Fig. 7)**.

As a result of these inspections 20 statements of findings were drawn up, 4 compulsory instructions were issued and 6 inspections ended in drafting statements on ascertainment of administrative violations.

A differentiation by sectors was made in connection with the specific conditions for personal data processing. Upon performing its activity in 2011, the Commission carried out the following inspections by sectors:

№	SECTOR	NUMBER
1	Healthcare	612
2	Trade and services	153
3	Tourism	57
4	Legal and consultancy services	53
5	Transport	47
6	State administration	45
7	Social activities	40
8	Education and training	36
9	Construction	23
10	Sport activities	20
11	Financial and accounting services	18
12	Telecommunication and information technology and services	16
13	Political parties	14
14	Security services	13
15	Agriculture and forestry	12
16	Human resources	8
16	Real estates	8
17	Regional and municipal administration	5
17	Insurance	5
17	Finance	5
18	Other	66

The attention was drawn on the inspections of data controllers 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 or data the treatment of which endangers rights and lawful interests of individuals according to the Commission's decision.

1.4. Handling requests

Since the beginning of 2011, the Commission has received 102 requests by individuals containing claims for rights violated under the LPPD and various inquiries regarding important issues concerning the CPDP's competence.

Most of the requests received by the CPDP concern rights violated under the LPPD in the following sectors: telecommunication (15 requests), Internet (12), state administrations (11) and trade and services (10). The number of requests is considerably smaller in the financial sector (5 requests), media (2), healthcare (2) and political parties (2).

The CPDP received 6 signals for violation of the LPPD in connection with the elections held at the end of the year and 9 signals related to television games. After considering the requests, the requesting parties were sent the relevant answers, 19 statements of findings and 7 statements on ascertainment of administrative violations were drawn up, 3 were brought to the competency of other authortities, and on 5 of the signals compulsory instructions were issued.

2. Administrative penal activity

2.1. Compulsory instructions

On the ground of Art. 10, Para. 1, Point 5 of the LPPD, the Commission issues compulsory instructions to personal data controllers in connection with personal data protection.

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

In 2011, 30 compulsory instructions were issued compared to 12 in 2010. They are differentiated by sectors as follows: financial sector, state administration, public utilities, transport, media, trade and services, telecommunications, etc. The proportion of issued compulsory instructions depending on the type of violation is specified in the chart below **(Fig. 8)**.

Most often the instructions issued are related to findings on:

· the data controller had not taken appropriate organizational and technical measures to ensure the personal data protection level in accordance with the Ordinance. The most common omissions here concern the following:

- no specific measures were determined to ensure the necessary protection level of personal data processed on a technical device;
- no procedure was provided for destruction of data media;

• violation of the provision of Art. 18, Para. 3 of the LPPD, as the data controller undertook steps for data processing other than those declared in the initial application, without informing the CPDP of the change;

• prohibition for processing certain data categories;

• no period of data retention was specified;

• violation of the provisions of Art. 19 and Art. 20 of the LPPD for notification of individuals.

From all compulsory instructions issued 7 were executed within the terms set by the Commission, 3 were partially executed, and the remaining 20 are in the process of execution. Some of the data controllers underwent further follow-up inspections, but no violations were established.

2.2. Administrative penal proceedings

According to the provisions of Art. 43 of the LPPD, the ascertainment of violations, the issuing, appealing and execution of the penal decrees shall be applied in accordance with the order established in the Law on the Administrative Offences and Sanctions (LAOS).

The statements on ascertainment of administrative

violations (SAAV) of LPPD's provisions are issued by a member of the Commission or by officials duly authorized by the Commission. The penal decrees are issued by the Chairperson of the Commission.

In 2011, as a result of its control activity, the CPDP drawn up 44 SAAV for ascertained violations (compared to 36 in 2010) **(Fig. 4)**.

The most common violations of the LPPD are as follows:

• violation of the provisions concerning the data controllers' registration:

- for updating prior to making changes in the data of already registered data controllers (Art. 18, Para. 3);

- prior to the entry in the register under Art. 10, Para. 1 of the LPPD (Art. 17b, Para. 4 of the LPPD);

-prior to the processing (Art. 17, Para. 1 of the LPPD);

• violation of the provisions concerning the personal data protection measures – the required minimal technical and organizational measures were not undertaken to protect the personal data according to the rules adopted by the personal data controller (Art. 23, Para. 4 in conjunction with Para. 1);

• violation of the lawful personal data processing principles – to be processed lawfully and in a bona fide manner, to be relevant, proportionate with and not exceeding the purposes for which it is processed (Art. 2, Para. 2, Point 1 and 3 of the LPPD).

32 penal decrees (PD) were issued compared to 29 in 2010, as three PD were issued on the basis of drawn up statements of violations from 2010 **(Fig. 9)**.

Along with the penal decrees (PD) issued in 2011, fines and proprietary penalties were imposed in the total amount of BGN 198 500 compared to BGN 131 500 in 2010.

Under legally operating PD in 2011 the total amount of BGN 56 500 was paid compared to BGN 43 500 in 2010. There is a permanent tendency to the increase of the legally operating PD, the sanctions imposed in this regard and the amounts received.

In 2011, by motivated resolutions of the Chariperson of the CPDP on the ground of Art. 34, Para. 3 and Art. 54 of the LAOS, 2 administrative penal proceedings were terminated (compared to 3 in 2010), and that year there were no suspended proceedings on the ground of Art. 43, Para. 6 of the LAOS.

The main reasons for termination include the fact that the acts were drawn up for non-constituting actions or the 6-month preclusive period for penal decree issuing has expired due to delayed delivery of the SAAV by the municipalities.

As in 2010, difficulties were also experienced this year in delivering the prepared SAAVs through the municipalities in the country, according to the provisions of Art. 43, Para. 4 of LAOS. In some cases the SAAVs were delivered to persons without representative powers which require their appropriate returning and re-delivering.

No penal decrees have been repealed by court among those issued in 2011.

In 2011, from the lawsuits on PD resolved by court, issued in the period 2008–2011, 3 PDs were completely repealed, 5 PDs were confirmed, and on 4 of them reduction of the sanction was enacted. 30 appealed PDs are subject to judicial review.

10 PDs became legally operating in 2011 without being appealed.

The reasons of the court when making the decisions to reduce the imposed property sanctions included "lack of aggravating circumstances", such as first violation of the data controller and "lack of harmful consequences of the act".

The motives given by the court for repealing the penal decrees were that SAAV was not delivered to a person authorized to receive it and representing the company when imposing sanctions to a legal entity (PD № 5/2010 against "Aulet" EOOD, city of Vidin). In another case, the delivery of SAAV for a legal entity performed through a municipality was not duly executed due to the presence of ommissions in the enclosed power-of-attorney of the representative (PD № 19/2009 against "Sunshine Holiday" EAD, Sofia).

The case law in 2011 most significantly outlines the casus under PD № 8/2009 against "BTC Mobile" EOOD, Sofia, fully confirmed both by the first instance committee, and the Administrative Court, Sofia city. The decree imposed a proprietary sanction on the company in the amount of BGN 20 000 for the violation of Art. 2, Para. 2, Point 3 in conjunction with Point 1 of the LPPD, committed by copying and storing copies of identification papers of individuals - consumers of their services, thus the personal data processed was inproportionate and exceeded the purposes for which it was collected in the first place.

There is a positive trend in the case law also by the confirmation of PDs issued against legal entities engaged in the hotel business, regarding the registration as controllers in the register under Art. 10, Para. 1, Point 2 of the LPPD, prior to the processing of personal data of an unlimited number of individuals, updating before making changes in the data of already registered data controllers (Art. 18, Para. 3 of the 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, Para. 4 in conjunction with Para. 1 of the LPPD). Examples are PD № 11/2011 against "Agatha A" EOOD, PD № 24/2009 – "Plam L" OOD.

The abovementioned statistical data indicate increase in the efficiency of the administrative penal activity. The number of penal decrees repealed by the court as a result of admitted significant procedural

violations was minimized. The judgments and especially their motives are analyzed in depth by the Commission so that it could properly carry out its control activity.

This fact is due to the measures taken for enhancing the quality of the activities related to ascertaining LPPD violations and their recording according to the provisions of the LAOS.

The permanent tendency to increase in the results of the control activity of the CPDP in the past few years, especially in relation to different tasks concerning the accession of Bulgaria to the Schengen Area, calls for the maintenance of the required administrative capacity for their implementation.

VI. Analysis of the opinions expressed by the Commission

During the reporting period the CPDP expressed 50 opinions on the application of the Law for Protection of Personal Data on various issues, both of specific interest to certain data controllers, and issues of significant public interest (in parallel, the opinions expressed by the CPDP in 2010 were 46). The most recent and interesting cases on which opinions were expressed by the national supervisory authority in 2011 pursuant to Art. 10, Para. 1, Point 4 of the LPPD may be grouped as follows:

- Providing distant financial services by giving consent to electronic personal data processing (online);
- Holding elections for President and Vice President of the Republic of Bulgaria and for municipal councilors and mayors in 2011;
- Providing access to video recordings from video surveillance equipment in a hospital;
- Providing access to personal data in the National Schengen Information System;
- Requests for providing access to the National Population Database maintained by the Chief Directorate "Civil Registration and Administrative Services" (CRAS) with the Ministry of Regional Development and Public Works or the records of civil status;
- Providing personal data of Bulgarian citizens to the administration of the governing authorities of a European Union Member State;
- Processing personal data by controllers outside the EU;
- Processing personal data on current issues of public interest or important issues to state authorities.

1. In order to protect the public interest in connection with the growing trend for identification thefts through the misuse of personal data, the CPDP was approached by credit institutions on the possibility of providing financial services at a distance by electronically giving consent to the personal data processing:

Very important and significant issue, on which the Commission has worked during this reporting period, concerns one of the most important aspects of data protection and the safeguards for proper data processing - the consent of the persons their personal data to be processed by a certain controller. The issue of consent was discussed many times on EU level as well, as one of the forthcoming changes in the European legal framework is expected to be with regard to the form and manner of proof that a person actually gave his/her consent. On the occasion of requests made by personal data

controllers - credit institutions - the Commission has expressed opinions on whether, in cases of provision of consumer credit online it is enough to verify customer consent to the personal data processing by clicking the button below a declaration of consent preceding the approval by the company to conclude a contract, and if the consent logged on the the credit company server can be considered "explicit consent" given by the individual to the personal data processing under LPPD, wihout the person having a certificate for electronic signature. In this case, the Commission assumed that the unsigned document is a document by its nature, which however does not enjoy a formal evidentiary value with respect to the statement expressed therein and its author. When applying for a loan online the confirmation through the button for consent to the personal data processing under the declaration preceding the approval by the company to conclude a contract cannot be considered added information in electronic form or logically associated with the electronic statement, allowing the establishment of its authorship. Furthermore, it cannot be accepted that the consent of the individual to the processing of his/her personal data is obtained, if there is no link between the person whose data was submitted to the company and will be processed and the person carrying out the action on confirmation of the consent by "pressing the consent button". Regarding the second question raised, the Commission has ruled that the retained consent to the processing of the personal data of the data subject, on the credit company's server in the absence of a certificate of electronic signature, may be considered "explicit consent" only where the authorship of the certification statement, objectified in the relevant electronic document, can be ascertained without any doubts.

2. In connection with holding the elections for President and Vice President of the Republic of Bulgaria and for municipal councilors and mayors in 2011 and to ensure the uniform implementation and compliance with the provisions of the Law for Protection of Personal Data by the processing of personal data during the election by the competent persons, the CPDP ruled with three separate opinions:

The first one is on specific issues relating to starting the organization of the electoral process and its compliance with the requirements of the Law for Protection of Personal Data. The Commission expressed the opinion that the Central Election Commission (CEC) and the municipal election commissions are independent data controllers and they are obliged to register with the Commission for Personal Data Protection. The Sectional Election Commissions are data processors and their relations with the data controller (the Central Election Commission and the municipal electoral commissions) are governed by a statutory instrument – the Election Code. In addition, the Commission for Personal Data Protection exempted from registration all nomination committees under Art. 96 of the Election Code.

The second request for an opinion received by the Commission was related to the nomination of presidential candidate of the nomination committee, in particular to the specification of the data controller in this case. The Commission ruled that the data controller is the nomination committee of the voters to nominate an independent candidate for President of the Republic of Bulgaria in the elections for President and Vice President in 2011, rather than its members, and each member of the nomination committee is treated as data controller in respect of the liability under the LPPD. The Commission heavily emphasized that the exemption from registration of all nomination committees under Art. 96 of the Election Code does not exclude the fulfillment of any other data controller's obligations, arising from the LPPD and from the control of the Commission for Personal Data Protection. In this context, by the ascertainment of infringement or errors during the elections and in carrying out its control activities, the Commission for Personal Data Protection has the power to issue compulsory instructions relating to the personal data protection, to impose a temporary prohibition on the data processing (after prior notification of the corresponding data controller) or to impose administrative sanctions under Chapter Eight of the LPPD.

Despite the two opinions expressed on the LPPD's application in connection with holding the elections for President and Vice President of the Republic of Bulgaria and for municipal councilors and mayors in 2011, by their discussion the CPDP on its own initiative decided to express a **third opinion with compulsory instructions** on the personal data processing by holding all kinds of elections for the purpose of unification of the rules for processing personal data in the electoral process. In connection with this, the Commission expressed a general opinion, which provided specific recommendations and guidelines for the personal data processing by all parties involved in the electoral process - CEC, regional, sectional and municipal election commissions, CRAS, political parties and nomination committees. This opinion was made available to all its recipients - the Central Electoral Commission, registered parties and coalitions of parties for the elections for President and Vice President of the Republic, political parties registered for the elections for municipal councilors and mayors and the nomination committees registered for the elections for President and Vice President of the Republic.

3. During the reporting period, the Commission has also ruled on the right of access to video recordings of video surveillance equipment in

a hospital and whether "video surveillance" is "personal data".

In this particular case the Commission stated that video recordings from video surveillance equipment contain "personal data", as they include information which, within the meaning of Art. 2, Para. 1 of the Law for Protection of Personal Data can reveal the physical identification of the person recorded. On the ground of Art. 26, Para. 1 of the Law for Protection of Personal Data Protection any individual has the right of access to the personal data related to him/her (including data recorded by CCTV cameras). The access to personal data of a single individual recorded by CCTV cameras can be provided if it is technically possible to temporary remove the personal data of third parties which could be revealed in the realization of this right of access. In case it is not technically possible such personal data of third parties to be temporarily removed, the only legal basis for the implementation of the right of access would be to obtain the explicit consent from all other individuals - subject to the specific video surveillance.

4. An important question of public interest, on which the Commission was approached by the Ministry of Interior for the first time, concerns the provision of access to personal data in the National Schengen Information System.

The specific enquiry concerns the provision of information to third parties under the Law on Access to Public Information, which contains data for motor vehicles and persons search according to the Schengen Information System. In this particular case the Commission ruled that the details of car owners searched according to the Schengen Information System are "personal data" within the meaning of Art. 2, Para. 1 of the LPPD in conjunction with Art. 7 of Ordinance № Iz-2727 dated 16.11.2010 for the organization and functioning of the National Schengen Information System. In this regard, the Ministry of Interior's bodies: 1. Are unable to provide information about these individuals due to the lack of legal grounds for the access of "third party" to SIS data, which originates from the Convention implementing the Schengen Agreement in conjunction with Art. 4, Para. 1 of the LPPD and subject to the provisions of Art. 11 and Art. 14 of Ordinance № Iz-2727 dated 16.11.2010 for the organization and functioning of the National Schengen Information System. 2. May provide information on wanted motor vehicles (model; brand; frame number, engine number; gear-box number) for the purpose of exercising the legitimate interests of such third party with the authorization of the state which registered the relevant alert in the SIS.

5. In 2011 the Commission continued to be approached with requests for the provision of access to the National Population Database, maintained by the Chief Directorate "Civil Registration and Administrative Services" with the Ministry of Regional Development and Public Works.

In most of the cases, the opinion of the CPDP was requested by different data controllers in terms of the provision of access to the National Population Database. Data controllers justify the necessity of obtaining such access by the presence of their legitimate interest. It is noteworthy that such requests are made by different controllers operating in different business fields, for example companies providing detective services, corporate security, tracing and identification of persons, objects, facts and circumstances, energy companies, non-profit companies or for the purposes of research. In all cases the Commission expressed the general opinion that the Chief Directorate "Civil Registration and Administrative Services" with the Ministry of Regional Development and Public Works is allowed to provide information, containing specific personal data about specific individuals only on requests received by the relevant controllers, not access to the National Population Database for the purpose of exercising their legitimate interest under Art. 4, Para. 1, Point 7 of the LPPD and only after evidence of its existence in the manner set in the law.

A specific case with a request for access to the National Population Database has been reviewed by the CPDP in relation to the implementation of a project of national significance for the Republic of Bulgaria. Taking the specificities of the corresponding project into account, the Commission stated that in this case, Chief Directorate "Civil Registration and Administrative Services" is allowed to provide information containing personal data on requests received by the controller, but not access to the Unified System for Civil Registration and Administrative Services to Population (USCRASP) when evidences for the obligation to perform task of public interest are presented.

In two of the cases, the CPDP did not authorize the provision of data from National Population Database due to the lack of legal justification. The one relates to the conduct of a regional national history research, and the second - with the activity of a non-profit organization in connection with the monitoring of elections held for municipal councilors and mayors. The first case was regarding an application submitted by a citizen to access the municipal records of civil status (birth, marriage and death) for the period 1911-1965, in relation to the conduct of a regional national history research. The grounds specified by the applicant conducting the study on the necessity to review birth, marriage and death certificates that are stored in the municipal records of civil status are research of the demographic characteristics of 12 families. After considering the required information and evidence, the CPDP did not authorize the

applicant to obtain access to the municipal records of civil status due to the lack of legal justification within the meaning of Art. 4, Para. 1 of the Law for Protection of Personal Data.

Another question concerning the processing of data in the National Population Database is the case where the Commission received a request for authorization to provide USCRASP data relating to individuals involved in the electoral lists of certain localities including: full name, permanent full address and date of permanent address registration; current full address and date of current address registration. The request for providing data aimed at exercising civil control over the drafting and updating of electors lists and the accuracy of officials in the municipal administrations for the maintaining of the population register USCRASP. The request was based on the fact that the above information is necessary in terms of numerous inaccuracies ascertained in the electors lists published in the settlements and not on the websites of this municipality, and that these lists do not correspond to the cumulative results published on the website of CD CRAS as of 15.08.2011. Given that: the Electoral Code specifies in detail the provisions concerning the electors lists preparation; the process of their final preparation is dynamical and changes in them can be made until the election day; options are provided for the electors lists revision, for appealing the denials for deletion, entry or overwriting in a particular electors list; option is also provided for a judicial review of the competent authorities actions by the preparation of the lists, i.e. the bodies under Art. 40, Para. 1 of the EC, and that in order to protect the personal data of individuals, citizens have been given the possibility to change their entry in the electors list but only if they make the request in person or through an authorized representative with an explicit power-of-attorney. The Commission stated that in this case the conditions required by law for the provision of the requested information are not present and did not authorize the provision of data from USCRASP.

6. The Commission was periodically approached by diplomats to assess the lawful personal data processing and the provision of such data to foreign government authorities. This year two requests of this type are outlined:

One request was submitted by the Honorary Consul of a foreign official representation in the Republic of Bulgaria through the Ministry of Foreign Affairs regarding the receiving of personal data of citizens of the sending third country, who are temporary residents in the Republic of Bulgaria, as well as those who have received permanent resident status. In this case, the Commission stated that the Ministry of Foreign Affairs can provide information of individuals - citizens of the sending third country who are granted permit for long-term residence and permit for permanent residence in the Republic of Bulgaria (names and addresses of residence) after provision by the Honorary Consul of the sending country in the Republic of Bulgaria of information and evidence on: the need and legal grounds under the legislation of the sending country for the registration of foreign citizens in other countries, the purpose of the information processing and the possible recipients of information.

The second case, which the Commission has received regarding the diplomatic service, was at the request of the Head of Diplomatic Office of the Republic of Bulgaria in a European Union Member State. Request was made to the CPDP on what is the applicable law, and what is the appropriate manner of provision of personal data of Bulgarian citizens from USCRASP to foreign authorities of a European Union Member State, through diplomatic and consular missions of the Republic of Bulgaria and is authorization by the Commission for Personal Data Protection necessary in this case. The CPDP expressed the opinion that the provision of personal data by the diplomatic office of the Republic of Bulgaria to the administration of the governing authorities of a European Union Member State is made freely, under Art. 36a, Para. 1 of the Law for Protection of Personal Data, if of one of the admissibility conditions for data processing according to Art. 4, Para. 1 of the LPPD is present and after the foreign state authority to which the data is disclosed proves the legitimate interest and the diplomatic office is responsible for assessing the way the requested information will be drawn up and sent, as well as the technical and organizational measures for the protection of information by its provision. In cases where the data provision is justified by the need to provide services on the initiative of or for Bulgarian citizens, the provision is always free with the explicit and unambiguous consent of the individuals - Bulgarian citizens. The Commission for Personal Data Protection should be approached pursuant to Art. 106, Para. 1, Point 3 of the Law on Civil Registration in all cases where there is no explicit consent of Bulgarian citizens their personal data to be provided to foreign governing authorities and institutions, and foreign legal entities in order to be guaranteed the individuals' privacy and personal data protection.

7. Considering the need of registration of data controllers that process data, but are not established in the Republic of Bulgaria, or on the territory of a Member State of the European Union, the Commission had the opportunity to consider several specific cases.

The first issue on which the Commission has made statemet concerns a request for an opinion on the possibility of Google/Google Inc. to perform actions in recording objects to realize the service Google Street View in the Republic of Bulgaria. Before expressing its opinion on the case in question, the Commission examined the experience of the

European Union Member States on the application of Google Street View on their territory and the problems encountered in this regard. In this case, the Commission expressed the opinion that with regard to the processing of personal data for the purpose of the service provided by Google/Google Inc. - Google Street View - should be implemented the provision of Art. 1, Para. 4, Point 3 of the LPPD, i.e. the Law for Protection of Personal Data applies to the processing of personal data where the data controller is not established within the European Union and European Economic Area Member State, but for purpose of processing should be used facilities on Bulgarian territory, and in that case the controller - Google/Google Inc. - should appoint a representative established in the Republic of Bulgaria without this appointment releaving Google/Google Inc. from its responsibility. In this opinion the Commission also gave compulsory instructions with which Google Inc. as data controller must comply before, during and after the process of recording of data for the purspose of the Google Street View. The issued compulsory instructions relate to the protection of the individuals' rights and the filfillment of the data controller's (Google Inc. and its representative in the Republic of Bulgaria) statutory obligation to take appropriate technical and organizational measures, , and the latter were explicitly instructed: during the recording of street images from the cameras of Google Street View to prevent the collection (including accidental or incidental) of Wi-Fi data (data for wireless access points); to take measures to avoid the recording of payload data and other data directly related to persons (e-mail addresses, passwords, etc.); to inform the public about the rights of individuals regarding the processing of their personal data for the purpose of Google Street View; to take more restrictive measures on the technology used for blurring images of individuals in areas that are related or could be related to the processing of data of special nature, etc.

The Commission was also approached with a request to express an opinion under Art. 10, Para. 1, Point 4 of the Law for Protection of Personal Data concerning the procedure for registration of a single person limited liability company which organizes and conducts research and development activity in the field of natural and medical services as local representative acting on behalf of data controllers established in a third country - companies based in the USA. In this case the CPDP has expressed the opinion that companies established in a third country - the USA, are data controllers under Art. 1, Para. 4, Point 3 of the LPPD and the hypothesis stipulated in Art. 1, Para. 4, Point 3 of the LPPD is present – the data controller must use facilities in Bulgarian territory to process personal data and should appoint a representative established in the Republic of Bulgaria. The opinion also contained the manner and the procedure for registration of data controllers and of their local representative.

8. Except for cases with subject or enquiry that is common or similar to a large group of personal data controllers, the Commission has been approached with requests for opinions on current social topics that are of high public interest or relate to the exercise of state power.

An example of such an opinion is the enquiry whether the inspectorate of a certain ministry is entitled to request personal data (name, personal identification number and indication of living/ dead related parties - parents, spouses, children, siblings) from the National Population Database in connection with collecting information for the consideration of signals for the conflict of interest with respect to members of political cabinets, because the members of working parties who collect and process information on received signals are not officials, neither members of the inspectorate, nor members of other departments in the ministry and fulfill orders under civil contracts. In this case, the Commission has ruled that information containing personal data of related parties within the meaning of Para. 1, Point 1 of the Additional Provisions of the Law on Preventing and Detecting Conflict of Interest may be provided to the Inspectorate with the MRDPW for the fulfillment of the statutory powers to exercise supervision and carry out inspections under the Law on Preventing and Detecting Conflict of Interest only in specific cases, i.e. when a signal concerns the individual and actions on the consideration of the signal should be taken, e.g. the amount of information that can be provided should be proportionate to the purposes for which it is required.

Another significant problem, on which the Commission ruled, was set in the request for an opinion from the Ministry of Interior in connection with the maintaining of a public register of donations to the Ministry and the possibility this register to contain personal data of donors - individuals. The CPDP has expressed the opinion that the publication of personal data - name, within the meaning of Art. 9 of the Law on Civil Registration of individuals who are donors to the Ministry of Interior, in the public register for donation contracts received by the Ministry of Interior, maintained pursuant to the Internal rules of procedures for donation contracts, receiving and managing donations within the Ministry of Interior, constitutes processing of such data through its distribution. Such processing is permissible only after obtaining the consent of those individuals within the meaning of Art. 4, Para. 1, Point 2 of the LPPD in conjunction with Paragraph 1, Point 13 of the AP of the LPPD.

9. In connection with the policy to facilitate the procedure of providing administrative services to the Bulgarian citizens abroad by the obtaining

issued Bulgarian identification documents.

The Commission for Personal Data Protection received a request for an opinion on the possibility of transfer of personal data in the case of sending issued Bulgarian identification documents to applicants living abroad by courier or by mail. The Commission for Personal Data Protection has stated that applications for the issuance of Bulgarian Identification Documents or Bulgarian Identification Documents already issued can be sent to and from the Ministry of Foreign Affairs, respectively, to and from the relevant diplomatic or consular representation using the official channels or through a company certified to transfer valuables, which provides courier services in the cases where the Regulation on the Issuance of Bulgarian Identification Documents or another regulation explicitly allows this. In these cases, the processing of personal data contained in the Bulgarian identification documents shall be executed pursuant to Art. 4, Para. 1, Point 1 of the LPPD. The transfer of the company's shipment shall be lawful if the legislation of the corresponding state of residence of the Bulgarian citizen permits such transfer and the relevant individual whose documents are subject to transfer or to whom the documents relate, has expressed his/her explicit consent to this transfer within the meaning of § 1, Item 13 of the Additional Provisions of the LPPD, incl. the payment of the service. In addition to the opinion, the Commission also gave specific instructions on the actions to be taken so the transfer of Bulgarian identification documents could be lawful and legitimate in terms of personal data protection.

VII. Requests for authorization of personal data transfers

In 2011, the CPDP was approached by many data controllers with requests for authorization of personal data transfers to third countries - countries outside the European Union (EU) and European Economic Area (EEA). 21 administrative proceedings were brought before the Commission in connection with requests for authorization for personal data submission (for comparison, in 2010 were carried out proceedings for 35 transfer requests).

In cases, where data controllers transfer personal data to other controllers on the third countries territory, the CPDP issues a decision after an assessment of the adequate level of personal data protection provided in these countries. This assessment is carried out according to criteria set forth in the Law for Protection of Personal Data and the Rules on the activity of the Commission for Personal Data Protection and its administration (RACLPDP), such as: nature of the provided data, the data processing period, purpose of the personal data transfer, notification of individuals whose data will be provided about the purpose and the recipients of data in the third country, the statutory right of the individual to access the data and the possibility to correct or delete data, which processing does not comply with the LPPD, measures for the personal data protection taken in the relevant third country, as well as the possibility for compensation for damages suffered by the individual as a result of unlawful processing. It should be noted that the preferred means for demonstrating an adequate data protection level in the third country, respectively, of the recipient in the third country, is the use of the so-called Standard Contractual Clauses. Exporters of data present contracts containing commitments to comply with the Standard Contractual Clauses, specified in European Commissions Decision. Standard Contractual Clauses are applicable for transfers to all countries outside the European Union and the European Economic Area. They contain certain obligations for the controller, who submits the data to the controller on the territory of the relevant third country - recipient of the data, and both controllers are jointly liable for any violations of the clauses.

Following the control mechanism, set in CPDP's opinion from 2010, for personal data transfer by accredited organizations, operating in the international adoptions field, to any similar organization and/or central authorities under the Convention on the Protection of Children and Co-operation in Respect of Intercountry Adoption (Haque Convention), in 2011, the Commission has been repeatedly approached by these controllers

with requests for data transfers authorization.

The Commission has also received a large number of requests for transfers of employees' personal data by joint ventures or by companies 100% owned by foreign entities with buisness activity in Bulgaria with centralized data processing server outside the territory of the Republic of Bulgaria or by business entities that under concluded contracts for outsourcing, entrust and assign some of their internal activities to outsourcers.

Most often, the requests for the authorization of transfers concern the U.S.A., the Swiss Confederation, the Republic of India, Mexico, Malaysia, etc. Positive decision for the transfer was given in 20 cases. The majority of requests refer to the authorization of the data transfer from subsidiaries in the Republic of Bulgaria to the respective parent company in a third country or by the fulfillment of a contract concluded between the company - data controller in Bulgaria and other companies in a third country. In most of the cases, the technical and organizational data protection measures are settled in the internal rules of the relevant company or in a contract with included Standard Contractual Clauses for data protection. It was ascertained that in predominant number of cases data controllers require obtaining an explicit informed consent for the transfer of employees' data, collected for the specific transfer.

Some interesting cases were received - the CPDP has been approached with requests regarding authorization for the transfer of data recorded by technical means - biometrics and video surveillance data.

In the first case, the Commission received a request for authorization for the personal data transfer - scanned papillary images of palm to a company and non-profit legal entity in the USA in connection with the conduction of a computerized test in the Republic of Bulgaria, used for the matriculation of trainees in institutions providing higher business education worldwide. One of the main requirements for the test is the scanned papillary image of the palm of the candidates, participating in the test to prevent and oppose to any form of fraud and substitution of candidates, and on the other hand - maintaining the confidence in business schools, which matriculate trainees after the successful completion of this test. In this case, the CPDP issued a decision, which allowed the personal data controller - a local representative - to provide a scanned papillary image of the palm (biometrics) of individuals - candidates for the test in the USA. In this case the legal ground for the data transfer authorization is the presence of the consent of data subjects - test applicants - whose biometric data will be transfer.

In the second case the CPDP was approached with a request for authorization of personal data transfer - photos and video recordings of the data controller's employees and visitors taken in the premises of the controller to the parent company in the USA.

During the administrative proceeding, the Commission established the following shortcomings: none of the alternative conditions for admissibility mentioned in Art. 4, Para. 1 of the LPPD were present in the processing through "provision"; the advisibility of the requested data transfer for the category "visitors" was not proven; the amount of data, required for the transfer exceeded the admissible amount; the processing of personal data was incompatable with the specific purpose of the request - human resources management.

Considering the above-mentioned, the CPDP found that the collection of visitors' data "exceeds" (Art. 2, Para. 2, Item 3 of the LPPD) the processing of the employees' data. This in fact means "excessiveness" under Art. 2, Para. 2, Item 2 of the LPPD according to which personal data must be collected for specific, legitimate purposes and must not be further processed in a manner incompatible with those purposes. Therefore, the Commission issued a desicion, which did not allow the data controller to provide images and video recordings of the employees and visitors, taken in the company premises to the third country - the USA. The CPDP's decision is appealed before the Sofia Administrative Court, and is iniciated an administrative proceeding.

A specific case on which the CPDP expressed its opinion in 2011 was related to a request for data transfer by a religious organization to the Representation of the Church in a third country. However, considering the large amount of sensitive information – subject of the data transfer request – and the lack of additional information about the alleged existence of data subjects' consent, as well as the manner of transfer, the data controller was inspected. Based on the inspection's findings and after considering all circumstances, facts and evidence to the request, the Commission authorized the data controller to disclose personal data of individuals from the requested records "Staff" and "Membership" to the religious administration of the church in the third country for the purposes specified in the request, instructing the same that upon the provision of third parties personal data - parents, current and former spouses - and when these persons are not members of the church, the same must be asked for their explicit consent for the transfer.

VIII. Training

In 2011, the CPDP adopted a concept for conducting training and a Training Plan, launched a large-scale educational campaign. The current national goals and priorities were taken into account by the preparation and carring out of the training campaign with series of trainings aiming at improving the professional training of data controllers and data processors from the public authorities with access to the Schengen Information System considering the future accession of Bulgaria to the Schengen area. Along with conducting training on the SIS and as continuation of the 2010 practice were held seminars with representatives from local authorities and local self-government, the administration of the National Assembly of the Republic of Bulgaria. There was participation in the training courses at the Diplomatic Institute and the University of Library and Information Technology. Experts of the Commission participated in the training courses at the Diplomatic Institute and the University of Library and Information Technology.

In 2011, the training conducted by the CPDP was attended by data controllers from three groups - public sector, private business and academic community representatives. 22 seminars were held, of which 12 trainings of employees from institutions having access to the NSIS, 3 seminars with bodies of local self-government and local administration and the National Association of Municipalities in the Republic of Bulgaria, 2 trainings for the National Assembly, 1 training for the Diplomatic Institute and 1 for the academic community, 2 trainings for representatives of business entities (Kozloduy NPP and EVN), 1 training for the members of a professional organization (Bulgarian Pharmaceutical Union). 106 were the total institutions that sent representatives to participate in the training, among them 47 public sector institutions, 55 courts, 2 business entities and 1 professional organization. Training was conducted for the total number of 481 data controllers and data processors, of which 333 participated in the training for data controllers and data processors in the NSIS.

1. Training for data controllers conducted on the initiative of the CPDP

1.1. Trained government structures and institutions pursuant to the National Schengen Plan

In connection with the application of the Law for Protection of Personal Data by the personal data processing in the Schengen Information System, the CPDP organized training for all institutions listed in the National Schengen Action Plan, which was successfully completed in the period May-November 2011. More information on the training organized in connection with the processing of SIS data is presented in Section IX – "Readiness for supervision on personal data processing in the National Schengen Information System".

During the training the trainees were given the opportunity to present questions for discussion, case studies and problems in their current work, related to personal data, to improve the practical orientation of training and its applicability. Trainees used the opportunity and asked various questions that can be divided into two main areas - questions related to the duties of particular data controllers, and related to their rights and obligations as citizens of the Republic of Bulgaria.

The trainees discussed both general data protection questions, interesting for the trainees as citizens, and special cases related to their specific activity. Very interesting for the trainees was the responses to issues, concering the mobile operators and bank employees activities by collection and storage of personal data, personal data protection in cases of direct marketing as well as specific issues related to the collection of notary deeds by local authorities and access to personal data of taxi companies, real estate brokers and persons performing telephone scams.

The trainees paid particular attention to issues related to the CPDP's activity as well. Some of the discussed topics concerned inspections carried out by the Commission, the imposition of fines and their collection, the possibilities for personal data protection following the administrative procedures before CPDP, the procedures for data transfer to third parties.

The training sessions of controllers having access to the Schengen Information System, were very interesting for the trained institutions. Even before the Ministry of Interior launched the campaign, several thousand employees in the system expressed their willingness to attend the training seminar, but the lack of financial and human resources required the optimization of the number of trainees. Following the positive feedback from the trainees, the Ministry of Interior and the Executive Agency "Maritime Administration" officially expressed their wish to continue training in 2012, covering the structures of both institutions on central and regional leval.

1.2. Training of the local self-government and local administration bodies

The tradition of benefitial co-operation between the Commission for Personal Data Protection and representatives of local authorities continued in 2011 as well. 2 trainings were held - in the districts of Blagoevgrad and Vratsa, attended by 42 people and 1 training – for the National Association of Municipalities in the Republic of Bulgaria.

• District of Blagoevgrad

On March 10, 2011, the Commission for Personal Data Protection held training of the district and municipal administration staff, mayors and municipal secretaries of the district of Blagoevgrad. Trainees were introduced to current issues related to the personal data protection in the global and national scale, to the legal data protection framework and the CPDP's activities. In addition, participants were given materials containing main documents of the Bulgarian and international personal data protection legal framework, the reports of the CPDP to the National Assembly, the Commission's newsletters, frequently asked questions and their answers.

• District of Vratsa

On June 23, 2011, training was held in Vratsa District Administration. The training was attended by mayors and secretaries of the municipalities in the district of Vratsa, as well as by officials from regional and municipal administration. The training focused on the rights of individuals and the obligations of data controllers and data processors, the powers of the Commission for Personal Data Protection, proceedings before the Commission and other current topics concerning the personal data protection. Special attention was paid to issues related to the CPDP's information campaign aiming at explaining the rights of citizens in connection with the planned accession of the Republic of Bulgaria to the Schengen Area.

• National Association of Municipalities in the Republic of Bulgaria

The training intended for the National Association of Municipalities in the Republic of Bulgaria was attended by representatives of four administrative structures of the Association. This training course was the result of the initiative launched by the Commission for Personal Data Protection in 2010 for conducting specialized seminars for representatives of local self-government and local administration.

2. Training on data controllers' initiative

2.1. Training of data controllers from public institutions

As before, in 2011, data controllers were interested in the CPDP's training activities and expressed their wish for the training of their employees. The Commission for Personal Data Protection was invited by public authorities to conduct training for the administration of the National Assembly and to continue the successful practice from previous years of participation in training courses of the Diplomatic Institute at the Ministry of Foreign Affairs.

• Training of administration of the National Assembly of the Republic of Bulgaria

At the invitation of the National Assembly (NA) of the Republic of Bulgaria, CPDP experts held a two-day training session to the NA administration. The training was conducted in order to acquaint officials with the data protection legislation on national and European level, explain the basic concepts, emphasize on the individuals's rights and data controllers' obligations, the main powers of the Commission as an independent data protection authority, the methods of exercising these rights, and the required minimal organizational and technical data protection measures, which must be taken by each data controller to protect the processed data from unauthorized access or accidental destruction.

2 training seminars were held for employees of the National Assembly.

The first training was attended by representatives of the management of the administration of the National Assembly of the Republic of Bulgaria. The emphasis of this training was the discussion of specific cases and finding constructive solutions to issues and problems of a purely practical nature that had arisen, arise or seem likely to arise by the performance of the Parliament's administration activities. Attendees were generally introduced to the basic data protection definitions, the Commission's activities and the individuals' fundamental rights and the respective data controllers' obligations. The participants were given the opportunity to comment and ask questions and it was widely used by all of them. Mainly, the questions refered to the amount of information containing personal data in the shorthand records of the National Assembly and the amount of information provided to accredited journalists from different media.

The second training was attended by officials of the administration of the National Assembly of the Republic of Bulgaria. They were briefly introduced

to national and European data protection legislation, the basic data protection definitions were explained, and special attention was given to the individual's rights and data controllers' obligations. The attendees were introduced to the basic competences of the Commission as an independent data protection authority, the methods of implementation of these powers, and the required minimal organizational and technical data protection measures, which must be taken by each data controller to protect the processed data from unauthorized access or accidental destruction.

• Training in the Diplomatic Institute at the Ministry of Foreign Affairs - special course on "Consular Diplomacy"

In 2011, the traditional co-operation between the Commission for Personal Data Protection and the Ministry of Foreign Affairs was extended and developed with the special course on "Consular diplomacy" organized by the Diplomatic Institute. Experts from the CPDP actively participated in the course held in 2011. They presented to the participants in the training the Commission's main activities, the national and European data protection legal framework. The participants were introduced to the basic personal data processing rules and regulations. The training focused on the regime for the transfer of personal data to third countries as well as on issues related to their provision from one data controller to another or to data processor. Many cases were discussed concerning the requests of citizens for submission of information for individuals - Bulgarian citizens, situatied on the territory of a third country, the possibilities and procedure for its provision by the consulates.

3. Training of academic community

3.1. Lectures to the students from the University of Library and Information Technology

In 2011, as in the previous 2010, CPDP representatives participated in meetings with students from the University of Library and Information Technology, and presented the activities of the Commission and proceedings execised before it. The training was organized at the Commission's premisses, thus students had the opportunity to get acquainted with the work of the employees of its administration. Questions were answered on the Commission's practice by carring out its supervisory activities. The rights that any data subject has in relation to the handling of his/her personal data were also discussed.

4. Training of data controllers from the private sector

4.1. Kozloduy NPP

In June 2011, was held training for the officials, processing data in Kozloduy NPP. The CPDP team acquinted officials of the nuclear power plant with the data protection legislation, with their obligations by handling personal data and with the protection measures to be taken when processing data.

4.2. Bulgarian Pharmaceutical Union

In December 2011, training was held for representatives from the Bulgarian Pharmaceutical Union. By the training was taken into account the specific character of their work and the fact that they handle sensitive personal data concerning the individuals' health status. The training emphasized on the definition of specially protected data (sensitive personal data) and on the data protection measures.

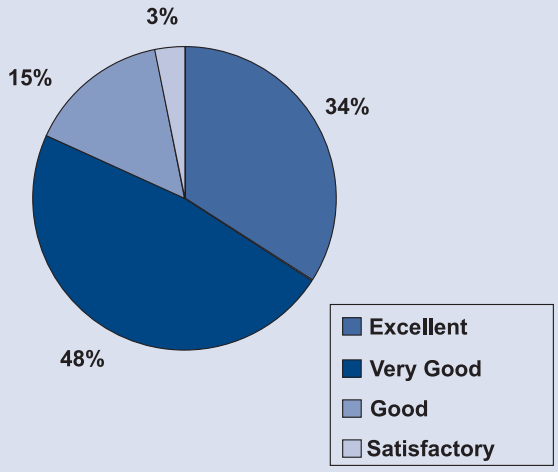
4.3. EVN Electricity Distribution Company

In 2011, the CPDP also trained data processing staff in one of the electricity distribution companies in the country - EVN. 2 seminars were held, during which the employees in the company were introducted in detail to the data protection process, their responsibilities and duties by the collection, processing and storage of their customers and contractors personal data.

5. Statistics and trends

In 2011, the training conducted by CPDP experts was attended by 481 data processors. The CPDP's conclusion is that the training resulted in a detailed introduction of the audience to the mandatory minimum of knowledge, skills and experience in data processing and the objectives set for this training were met. This is also confirmed by the feedback provided by the trainees who highly appreciate the learning process and knowledge obtained. The experience obtained and the training practice provided by the training team will contribute to the further improvement of the learning process.

On the basis of the summarized results the following assessment of the training was received:



From the comparative analysis of the results from the first training period 01.2011-06.2011, and the results from the second training period 07.2011-10.2011, it can be concluded that teaching teams were able to improve the quality and effectiveness of the conducted training. In the second period the positive ratings, included in the questionnaires, by the trainees increased - for the first period they were 76.15 %, compared to 85.16 % for the second. The increase in positive ratings is by almost 10 %. The overall satisfaction of trainees from the training increased as well. In the first period nearly 30% of respondents have completed the free text box "What did you dislike in the training" referring to different aspects they consider negative. In the second period, this percentage decreased to 15 %.

IX. State of preparedness for supervision on personal data processing in the National Schengen Information System

Numerous initiatives have also been taken in the direction of key significance for the CPDP - accession to the Schengen Area. A priority and permanent task for the Commission for Personal Data Protection in 2011 was the activity related to the preparation for exercising its competences as a supervisory authority by virtue of the Schengen Convention after the final accession of Bulgaria to the Schengen Area. The main objectives for the personal data protection in the pre-accession process result from the tasks set out in the National Action Plan for Implementation of the Provisions of the Schengen Acquis and the elimination of internal border controls as follows:

1. Training of data controllers and data processors in connection with their obligations arising from the Law for Protection of Personal Data and personal data protection in SIS

The compulsory training, intended for data controllers and data processors that process data in the Schengen Information System was of key significance. The general professional personal data protection training was attended by 333 employees whose duties will require working with NSIS and with personal data processed in the system by the members of the institutions authorized to receive information from the National part of the Schengen Information System. The series of trainings for these data controllers and data processors covered the organization of 12 individual courses following the "Training of Trainers" principle with a specially prepareded thematic content on all major personal data protection issues. The conduct of such training in the context of optimizing the government institutions' administrative capacity during the pre-accession process not only complied with the implementation of the National action plan for implementation of the provisions of the Schengen acquis and the elimination of internal border controls, but also with the obligation of the CPDP to organize and conduct personal data protection training. The Commission managed to fulfill this task stipulated by the National Plan before the end of the set deadline - December 31, 2011. During the reporting period the following structures were trained:

- Directorate "Migration" - Ministry of Interior;
- Directorate "International Operative Police Cooperation" - Ministry of Interior;
- Directorate "Bulgarian Identification Documents" - Ministry of Interior;

• Chief Directorate "Border Police" - Ministry of Interior;
• Chief Directorate "Public Order Police" - Ministry of Interior;
• Representatives of 28 Regional Directorates - Ministry of Interior;
• Visa Centre in the Directorate "Consular Relations" - Ministry of Foreign Affairs;
• Representatives of 55 appellate, district, regional and administrative courts;
• State Agency for Refugees with the Council of Ministers;
• National Investigation Service;
• Military Police Service;
• Customs Agency;
• Ministry of Justice;
• Executive Agency "Maritime Administration";
• Executive Agency "Railway Administration";
• Chief Directorate "Civil Aviation Administration";
• Prosecution of the Republic of Bulgaria.

The trainings held intended to produce double effect: on one hand, to improve the professional training on issues, concerning employees' personal data protection, and on the other – increased awareness and consciousness of the employees as citizens. The Commission expects that the training held following the "Training of Trainers" principle will contribute to the future multiplication effect of the results achieved. Moreover, in order to maximum allian the held trainings with the trainees' needs and considering their professional expertise and practice, different training sessions focused on different issues. The thematic content of the training included the legal framework of data protection, clarification of key concepts in the data protection field, personal data protection measures, the obligations of data controllers and the rights of individuals, as well as the roles and responsibilities of the CPDP. The training program on the data protection in the Schengen Information System also covered topics specifically targeted to data controllers, stipulated in the National Schengen Action Plan and tailored to their specific needs. They included an overview of the Schengen Agreement and the Schengen Area, clarification of the CPDP's Schengen information campaign, as well as the international co-operation in data protection sphere under the Schengen Convention.

2. Public awareness regarding the rights and obligations of citizens in relation to their personal data processed in the SIS

In pursuance of a task specified in the National Plan and together with the training for data controllers and data processors in the NSIS, the Commission for Personal Data Protection also held an active information campaign to inform citizens of the nature of the Schengen system and the consequences it has for individuals in terms of data protection.

The information activities focused on online distribution. Throught the second half of 2011 the Commission continued the promotion of information and educational content from the website of the CPDP via the websites of government institutions and partner NGOs. Many ministries and agencies published on their websites CPDP's current information materials concerning the rights of citizens by the processing of their personal data in the Schengen Information System. District administrations and many NGOs were actively involved in the promotion of CPDP's information campaign.

The main objectives, the content of the CPDP's campaign under the slogan "Data protection in the Schengen Area. Your rights" and the information on citizens' rights by the processing of their personal data within the Schengen Information System were widely covered by national media. They received a broad coverage in the regional newspapers and many online regional publications as well. The numerous publications and interviews of the Chairperson and the Members of the CPDP aimed mainly at informing the citizens and increasing their awareness on how their personal data is collected and processed and on the rights they have when they enter the Schengen Area.

Another significant part of implementing the 2011 CPDP's information campaign to raise awareness of the citizens about their data protection rights in the country and within the Schengen Area in the context of the accession of the Republic of Bulgaria to Schengen Area was the fifth celebration of the European Data Protection Day - January 28th, and the 30th anniversary of the European Convention 108 with a conference under the title of "CPDP - European standards of data protection. Bulgaria in Schengen". The conference was attended by official guests, representatives of the Ministry of Interior, representatives of NGOs and journalists from leading print and electronic media. The main emphases were placed on the European personal data protection standards and on the activities related to data protection in connection with the forthcoming accession of the Republic of Bulgaria to the Schengen area.

In order to provide direct and full access to all infor mation related to Schengen Area on CPDP's website, in 2011 measures were taken for the reorganization of the website by adding a separate submenu titled "Schengen Area". The new section contains the main documents on the implementation of the Schengen acquis, guidelines and best practices. In addition, the Commission for Personal Data Protection took part in the revision of the Bulgarian version of the Schengen Joint Supervisory Authority's website.

Following the objectives concerning the accession to Schengen, in July 2011 the CPDP sent a request to the national supervisory authorities of the Schen-

gen states asking them to share their experiences on the conducting of information campaigns for citizens' awareness rising with regard to Schengen and the Schengen Information System.

Questions were addressed about: activities for raising the awareness; the forms of co-operation chosen to extend the campaign scope; the available model forms to facilitate the exercise of citizens' rights; institutions that have participated in their preparation and the places where these forms are available; the options and manners to exercise the citizens' rights in third countries.

Based on the detailed information received on the experience of countries of the Schengen Area, the CPDP highlighted a number of good practices on how to achieve greater information impact and facilitate the procedures for citizens to exercise their rights. The results of this study and the recommendations given will be reflected in the planned information activity of the Commission for the year 2012.

At the end of 2011 the Commission approved educational text for raising citizens' awareness of their rights in Schengen, which is an addition to information brochures already distributed in 2010 and 2011. Besides that issue, the Commission approved other topics for raising the citizens' awareness, such as CCTV, identification cards copying and protection of children online, which will be subject to distribution in 2012.

3. Conclusion of bilateral co-operation and exchange agreements with regard to the application of the Schengen acquis provisions following the obligations of the Commission for Personal Data Protection as national supervisory personal data protection authority

To institutionalize the interaction between the Commission for Personal Data Protection and other national supervisory data protection authorities and to fulfill the task in the National Schengen Action Plan, in 2011, the Commission prepared a model draft international co-operation agreement dealing with the personal data protection co-operation. The purpose of the model draft agreement is to establish general principles and procedures for co-operation in the data protection field in interest of the citizens of the Republic of Bulgaria and any other country with which such agreement has been concluded. The draft agreement outlines the areas and forms of co-operation, as it is explicitly stipulated that the competent national authorities, which will apply the international agreement are the relevant data protection authorities of the countries – contractual parties.

After preliminary coordination of the draft international agreement approved by the Commission with the Minister of Interior and the Minister of Foreign Affairs, the Commission submitted the draft agreement to the Minister of Interior to carry out the procedure for coordinaion and approval pursuant to the Law for the International Agreements. The using of a model draft agreement will facilitate the consistency of the procedure for negotiating international data protection agreements and will ensure the equality in the relations of the Bulgarian supervisory data protection authority with the other countries' national authorities.

With decision of the Council of Ministers dated December 21, 2011 (Protocol № 49) the government approved the model draft agreement prepared by the Commission for Personal Data Protection as a basis for negotiations with Member States of the European Union, Member States of the European Economic Area and with third countries which ensure an adequate data protection level. It will be presented to similar supervisory data protection authorities.

4. Organizational and human resourses of the Commission for Personal Data Protection by opening 6 additional permanent positions and providing the relevant working places (the funds for the salaries for these newly opened positions should be included each year in the CPDP's annual budget)

To implement this task under the National Plan, the Commission has prepared amendments to the Rules on the activity of the CPDP and its administration. These amendments aim at strengthening the Commission's administrative capacity by opening 6 permanent positions and expanding the functional responsibilities of the specialized administration directorates with additional activities arising from the future Schengen accession. The newly opened positions will receive the required funding pursuant to the CPDP's annual budget for 2012 under Decree № 367 dated 29 December 2011 on the execution of the State Budget of the Republic of Bulgaria for 2012.

5. Additional activities not covered by the National Action Plan

Proceeding from the fact that the country's readiness for accession to the Schengen Area is a task of national importance, the Commission also undertook other activities within its competence that exceeded the tasks stipulated in the National Action Plan in the data protection field. By decisions of the Commission for Personal Data Protection dated 03.08.2011 and 14.09.2011, an amendment to the "Plan for on-going inspections on the initiative of the CPDP in 2011" was adopted. The scope of additional inspections covered the following personal data controllers: Ministry of Foreign Affairs - Consulate of the Republic of Bulgaria in Niš, the Republic of Serbia, the Ministry of Interior - Directorate "Migration", Chief Directorate "Border Police" – border checkpoint on the border with the Republic of Serbia, border checkpoint on the border with the Republic of Macedonia, border checkpoint on the border with the Republic of Turkey.

X. Contribution to the EU data protection policy

In 2011 the Commission for Personal Data Protection took serious part in the launch of several major European initiatives and engaged in the discussion of many current data protection issues. The authority made a significant contribution with the participation in public consultation on security breaches, amendments to the future legal framework and strengthening the role of national data protection supervisory authorities, European system for tracking terrorist financing and processing Passenger Name Record (PNR) data.

1. Public consultation on security breaches

The revised Directive on privacy and electronic communications (Directive 2002/58), which has already been transposed into the Bulgarian legislation through amendments to the Law on Electronic Communications, introduces the obligation of reporting of the so-called security breaches cases. These are breaches that lead to accidental or unlawful destruction, modification, unauthorized disclosure or access to personal data, transmitted, stored or otherwise processed in connection with the provision of public electronic communications service. The recent changes in the LEC (promulgated in State Gazette, issue 105 dated 29.12.2011 and effective from the same date) expand the powers of the Commission for Personal Data Protection by introducing an explicit obligation for legal entities providing electronic communication networks and/or services to notify the CPDP of any security breaches within three days of their establishment.

In order to establish the progress of the transposition process in individual Member States of the European Union, the European Commission launched a public consultation on security breaches. The Commission for Personal Data Protection actively participated in this consultation by providing answers to questions posed in advance related both to the general process of the Directive's transposition into the Bulgarian legislation and to its role of a supervisory authority by the processing of personal data in the telecommunications sector and security breaches.

Regarding the question which security breaches could affect negatively/adversely citizens, or companies' subscribers, respectively, the Commission stated that except for the types of breaches listed in the European directive (identification theft, false identification fraud, physical harm, significant humiliation or damage to reputation), as breaches adversely affecting the individual's privacy, may also be considered the breaches where processing exceeds the set purpose and all forms of breaches as defined in Directive 2009/136 (breaches that lead to accidental or unlawful destruction, loss, modification, unauthorized disclosure or access to personal data, transmitted, stored or otherwise processed in connection with the provision of public electronic communications service). CPDP is of opinion that the security breaches' notification does not affect the fulfillment of all obligations and the responsibility of the relevant legal entity, providing electronic communications services with regard to personal data protection, i.e. the fact that a legal entity has notified the supervisory authority of a security breach, does not relieve the entity from responsibility that this breach has occurred.

With regard to the personal data processing in the electronic communications field, the Commission stated that security breaches in this sector pose a significant risk of the personal data and privacy infringement. Therefore, the adoption by the relevant provider of public electronic communications services of appropriate technological measures to protect the data security should be subject to prior assessment by the national supervisory authority before the provider begins the personal data processing.

In connection with the study whether a common European model of inspections should be introduced, the Commission has expressed the position that the preparation and implementation of a standardized European model of inspections in the telecommunications sector would be possible and appropriate only if this model is not obligatory. The mandatory introduction of a common model would undermine the competence and independence of data protection authorities, which would be inadmissible. Such questionnaires could be prepared for different sectors to facilitate the work of the inspection teams at national level.

2. Amendments to the European legal data protection framework

In the context of the upcoming amendments to the European legal data protection framework, the CPDP received an official inquiry by the Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, which was sent to all other national supervisory data protection authorities in the Member States. The discussion focused on questions that were meant to identify problem areas requiring adequate and rapid changes on European level, as well as the trends for development, that are shared and supported by the Member States' supervisory authorities. Particularly relevant in this regard are the upcoming changes to ensure the recognition of institutional and operational independence of the personal data protection authorities. In connection with the questions put by Commissioner Reding, the Commission for Personal Data Protection participated in the work of the main advisory body within the EU – the Article 29 Working Party – on a joint contribution of the data protection authorities, by subitting its individual position as well.

The Commission expressed the opinion that strengthening the role of the personal data protection authorities relates to the provision of complete independence and adequate powers (the power of conducting investigations and enforcement of the legal framework and follow-up on the decisions' application) and resources (providing adequate financial, human and technical resources) by introducing the same provisions at national and European level. An appropriate mechanism to ensure financial independence is the provision in the legal framework of the obligation for debt collection from imposed administrative penalties to be deposited to the budget of the national data protection authorities.

According to the Commission's position, the scope of competence of supervisory data protection authorities should also cover the option for them to issue compulsory instructions on specific matters through which uniform rules could be stipulated for a group of personal data controllers. These instructions should be published in the official journal of Member States to ensure their publicity and for the purpose of achieving speed and efficiency the same should not be subject to appeal and should enter into force on the day of their publication. This would be an important preventive measure with regard to the personal data processing by the different controllers.

Regarding the current tendency to encourage cooperation between separate supervisory data protection authorities, the Commission defended the position that it is most important to find the right balance between the independence of the data protection authorities nationally and the co-operation which they will perform, and the possibility of a decision taken by one body to be considered by other bodies. The balance must be guaranteed by legal provisions in the future legal instrument and by mechanism for their implementation.

In its opinion to Commissioner Reding, the Commission for Personal Data Protection has identified the following areas of national law, requiring harmonization by the means of EU acquis:

- the possibility and the procedure for conducting joint inspections between national supervisory authorities;
- legal grounds, mechanisms and means to ensure an adequate personal data protection level in third countries when the transfer of data is done between data controllers that are public entities (e.g. ministries), given that these entities pursue the government policy of the country concerned in the relevant field and have no freedom of negotiations as individuals do;
- notification system;
- applicable law (especially when it comes to data controllers within the EU, or operating in more than one Member State, an EU Member State and/or third country, respectively);
- all new aspects outlined by the European Commission in the report on a comprehensive approach as subject to legal regulation.

In addition, the Commission has recognized that technical and organizational measures to protect the processed personal data should also be subject to mandatory harmonization considering that individual Member States currently have different legislative approaches and legal systems, and some of the activities on data processing, deleting, blocking, destruction should be synchronized as well. Furthermore, special attention must be paid that the future legal framework at European level stipulates general provisions on the control powers of supervisory authorities by data processing on the Internet, using CCTV surveillance, processing data of minors and underaged persons.

In order to make the legal framework consistent with the continuous changes in practice, the Commission has expressed the opinion that it is necessary to introduce a legal definition of the term "misuse of personal data", and Member States should have the obligation to provide for administrative sanctions at national level. Besides bearing administrative liability in cases of severe breaches in the personal data processing, bearing penal liability should also be provided.

In connection with the provision of data to third parties the Bulgarian supervisory authority is of opinion that there is a gap in the existing Directive regarding the possibility of an international organization to process personal data as a legal en-

tity. This is especially noticeable with regard to the personal data transfer to organizations such as the UN and NATO, as well as the EU itself. The Commission has considered important the introduction of uniform rules and procedures for data transfers to multiple subcontractors on contracts outside the EU. The case of the so-called intra-corporate transfers of data is particularly complex – this is the most common case of data transfers abroad.

It would be easier both for data controllers and individuals, as well as for data protection authorities if with respect to the provision of data to third countries (authorization regime), clear criteria and situations are stipulated where a permit issued by one supervisory authority should be respected by all other authorities. For example, where for the same purposes the same amount of personal data is transferred by one data controller or its subsidiaries to the same recipient in a third country.

Considering the necessity to facilitate citizens by providing them services, e.g. the "one-stop" principle, the Commission expressed the opinion that facilitation of procedures is possible only to data controllers and data processors. The first important element of the process of facilitating the operation of personal data controllers by the "one stop" principle is the introduction of a unified regime and form of notification. If such notification is made before the data protection authority in one Member State, it is appropriate that it can serve before the rest of the supervisory authorities in the EU as well.

In its position on the amendments to the legal framework, the CPDP admitted that it is necessary and appropriate to facilitate the following personal data processing activities: deleting, blocking, destruction, consulting, which can be done by introducing definitions of these terms, incl. of the notion "right to be forgotten", provision of mechanisms and procedures for their implementation and monitoring by supervisory authorities.

3. Terrorist Finance Tracking System

In connection with the initiative launched in 2011 to establish an additional European level tool to prevent terrorist financing, that is the Terrorist Finance Tracking System (TFTS), the Commission for Personal Data Protection has expressed its general position. The Commission agreed that the establishment and operation of a Terrorist Finance Tracking Program at European level would be a very important tool for the prevention, investigation, detection and prosecution of terrorism or terrorist financing. However, since the operation of such system involves some restrictions on the citizens' privacy and imposes the provision of data (including personal data) to the USA and/or other third countries, the purpose for establishing the system must be very well defined and justified. Therefore, the Commission supported the position, expressed by other countries as well, that the establishment of a European Terrorist Finance Tracking System should have the principal purpose of ensuring the EU citizens' secutrity and not be governed solely by the need to provide data to the USA regarding the implementation of the Agreement between the EU and the USA on the processing and transfer of financial communications from the European Union to the United States for the purpose of the Terrorist Finance Tracking Program.

The Commission noted that the legal instrument, by the means of which this EU program will possibly be established, needs to stipulate regulations to ensure the balance between the purpose and necessity of introducing a system for tracking the financing of terrorism and the respect for personal data, respectively, taking measures for their protection. In this regard the strict enforcement of the proportionality principle by the provision of data to third countries should be the most important factor.

The Commission for Personal Data Protection supported the European Commission's opinion, expressed in the document "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a European Terrorist Finance Tracking System: possible options" that the main tasks of the system should be provided with appropriate legal instruments at EU or national level or in a common European and national legal act.

With regard to the privacy aspects that should be considered by the establishment of the European program, the Commission noted that the future legal framework of the Terrorist Finance Tracking Program needs to stipulate clear and detailed provisions concerning data protection, to emphasize the supervision of the personal data processing and the cooperation mechanism between the relevant na-

tional and European authorities.
With regard to the choice of a European level structure, which can be entrusted with the functioning of the European Terrorist Finance Tracking Program, the Commission deemed the following criteria significant: functional competence, cost and cooperation mechanism with national authorities.

4. Processing of Passenger Name Record data

Regarding the current issue, concering the necessity of the processing of Passenger Name Record data in 2011, the Commission for Personal Data Protection has regularly expressed positions on two main documents:

- on the Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;
- on the draft Agreement between the European Union and the United States of America on the transfer to and use of Passenger Name Record data by the United States Department of Homeland Security.

On the proposal for an EU Directive for introducing synchronized rules for the use of this data across the European Union, the Commission has expressed its general support to the proposal in terms of its relevance and usefulness. The Commission noted that the adoption of this European act will facilitate the collection of data, both by law enforcement authorities for the purpose of investigation of terrorism and serious crime, and by the passengers on their travel. The regulation of the European PNR system by the means of the Directive will allow supervisory data protection authorities to apply clear rules for carrying out controls by the processing of PNR data.

Given that the data processing for the purpose of national security generally restricts the control powers of supervisory authorities, the Commission has recommended that the Directive should provide for the powers of national supervisory data protection authorities with regard to the collection of PNR data and its proportionate use by law enforcement authorities.

In its position, the Bulgarian supervisory authority marked the need of clear and detailed provisions of the interaction and compatibility between the future PNR system and the API data, the Visa Information System (VIS) and the Schengen Information System. Reference is made that the PNR system will contain national information on passengers not only to international destinations, but also on intra-country flights. The Commission emphasized that the Proposal on the Directive introduces obligations only to air carriers, but the fact that PNR data is collected and processed by other legal persons as well (e.g. travel agencies, sites to buy tickets) must not be overlooked. The Commission expressed its opinion on the relevance of setting up obligations for data entry in the PNR system of those legal persons too.

In the analysis of the proposed Directive, the CPDP made a critical comment that there is no clearly defined right of informing the individuals by the procesing of their PNR data and there is a lack of regulation of the obligation to delete data after the fulfillment of the processing purpose. Moreover, there is no provision for protection of the rights of minors and underaged persons that will be part of the PNR system when using the services of the air carrier.

The Commission has explicitly expressed its opinion that when defining the notion of PNR data is obligatory to be determined in detail the specific data categories which will be covered and to which the Directive will apply.

The Commission has provided specific comments and suggestions on the draft texts of the Directive in the course of its discussion throughout 2011.

In connection with the discussions on the draft Agreement between the European Union and the United States of America on the transfer to and use of Passenger Name Record data, the Commission for Personal Data Protection has stated two opinions: an opinion on the conclusion of agreements for the personal data transfer to third countries and a specific opinion on the draft bilateral agreement between the EU and the USA.

The Commission has carefully considered the following requirements related to the personal data protection: the principles of proportionality and purpose limitation to minimize the amount of data to the amount required to achieve the objectives set; the prohibition of processing sensitive data; the use of Push system as means of transmitting data; clear rules for monitoring and reporting on the processing of personal data; clear safeguards for the protection of personal data, or ensuring the appropriate technical and organizational protection measures, respectively; compliance of the data storage/retention periods with the purpose for which the data is transmitted; regulation of the individuals' right of access to their data; the right of information and right of seeking protection through administrative or judicial procedures; consideration of the existing EU data protection legislation, or the negotiation process in other agreements between the same parties, respectively.

In relation to specific texts in the draft agreement, the Commission supports the comprehensive data regulation and the general avoiding of sensitive data of Passenger Name Records data. Disagreement was expressed with the possibility such data to be retained for a period of time (regardless of the fundamental data collection prohibition) as defined

by U.S. legislation for the needs of specific ongoing investigation. We consider such a possibility for further storage and use of sensitive Passenger Name Record data unacceptable and disproportionate to the objectives of the agreement.

The Commission has recognized as a positive development the fact that the draft agreement provides for clear rules for monitoring and reporting on personal data processing. Multi-layered control is introduced with purpose- orientated data processing which will be exercised by a number of privacy protection officials with a certain degree of autonomy from the Department of Homeland Security and other key institutions, such as the Office of Inspector General, the Audit Chamber and the United States Congress.

Analyzing the final version of the draft agreement as of December 2011, the Commission assumed that all significant Member States considerations and comments have been taken into account, including those of the Republic of Bulgaria and it expressed the position that the text of the agreement offers reasonable balance between the protection of national security and the personal data protection.

The Commission has also recognized the necessity of co-operation and exchange of information, including Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorism and terrorism-related crimes in cases where the Passenger Name Record system is the only source for the identification of potential terrorists and no other relevant information is available.

By completion of negotiations on the draft Agreement between the European Union and the United States of America on the transfer to and use of Passenger Name Record data by the United States Department of Homeland Security, the Commission has recognized the positive development in the text of the Agreement and has therefore expressed general support for its signing and subsequent conclusion.

5. Transposition of Framework Decision 2008/977/JHA

In 2011, the process of transposition into the Bulgarian legislation of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters was completed. In the Republic of Bulgaria the requirements of the Framework Decision were transposed through amendments to the LPPD. With their enforcement on October 22, 2011, Bulgaria fulfilled the obligation to take national measures to comply with the provisions of the Framework Decision and established uniform rules for the personal data processing- subject of exchange between EU Member States and bodies or information systems, created on the basis of the Treaty on European Union or the Treaty on the Functioning of the European Union. Statutory changes were made and proposed by an interagency working party formed on the initiative of the Commission, as the Commission for Personal Data Protection played a key role in the entire process of transposition of the Decision.

The most significant result of the made legislative changes is the stipulation in the general Law for Protection of Personal Data of special rules for the personal data processing which fall within the scope of the Framework Decision, i.e. data processed in the framework of police and judicial co-operation in criminal matters. With the amendments made to the LPPD is presenved the possbility for a special law governing the special rules related to the processing of personal data from national registers when it comes to data concerning national defence and security, public order, combating crime, criminal proceedings and execution of penalties. However, when data concerning public order, combating crime, criminal proceedings and execution of penalties is obtained by other Member States or information systems in the framework of co-operation in criminal matters, such data should be processed pursuant to the rules and procedures of the general Law for Protection of Personal Data– LPPD, and not following the relevant special law regulating the corresponding area of public relations. Thus, the amendments produce the following legal effect: for national databases, the relevant special law is applied, that allows for exeptions from the general data protection regime, while for data obtained under the Framework Decision 2008/977/JHA, the regime laid down in the LPPD is applied.

XI. Co-operation of CPDP with other government bodies at national level and international co-operation with similar supervisory bodies, Working Parties and Joint Supervisory Bodies. Regional co-operation

1. Co-operation at national level

The horizontal nature of data protection makes Commission's interaction with other institutions and organizations more and more urgent and current. In 2011, the traditional co-operation between the data protection authority and the Ministry of Interior continued. Their joint work found expression in issues directly affecting the jurisdiction of both structures, as well as in initiatives of national and international interest. Their collaboration was extremely beneficial with regard to the preparation of national positions on matters concerning the EU Terrorist Finance Tracking Program, the collection of Passenger Name Record data within the EU and in connection with bilateral exchange of information with the USA, as well as their joint participation in Working Parties on specific issues. The participation of all competent authorities of the Ministry of Interior in work meetings concerning the access to retained traffic data and the conducting of training for employees at the departments having access to NSIS data are evidence of a good dialogue and mutual support.

The opinion, expressed by the CPDP, with which the Commission authorized the transfer of official documents (including Bulgarian identification documents) by mail or by certified couriers, directly resulted in amendments to the Law on the Bulgarian Identification Documents, iniatated by the Ministry of Interior. Commission experts were invited to participate in the work of the specialy created interagency working party.

The same opinion of the Commission strengthened the bilateral contacts of the institution with the State Commission on Information Security (SCIS) and the Ministry of Foreign Affairs. The participation of CPDP's representatives in the working party for the optimization of the courier routes by the transportation of diplomatic correspondence was insisted by the Ministry of Foreign Affairs and was hosted by SCIS. The cooperation between the three institutions continued also in the discussions of possible changes in the relevant legislation concerning the transfer of diplomatic correspondence in the diplomatic service.

Another joint activity with the SCIS was the participation of the CPDP in the consultations on concluding a bilateral agreement on mutual protection and exchange of classified information in the field of industrial security between the Republic of Bulgaria and Canada. The participation of the data protection authority aimed at providing a national data protection system in the Republic of Bulgaria, paying particular attention to the minimum data protection level. Clarifying the data controllers' obligation to take technical and organizational data protection measures was an important stage in the harmonization of the classification levels for information security, applicable in both countries.

Good institutional relationships between the CPDP and the Ministry of Foreign Affairs in connection with the processing of personal data for the purpose of the diplomatic service continued in 2011 too. The Commission was periodically approached by diplomatic missions or by the "Consular Relations" Directorate - Ministry of Foreign Affairs, with requests for expressing an opinion on specific cases from the Bulgarian diplomats' practice that affect the provision of personal data of Bulgarian citizens abroad. The data protection training held for the Ministry staff, conducted under the Schengen obligations, was considered very useful.

The obligation of our country for the implementation of EU legal acts in various fields has contributed to laying the foundations of the Commission;s good institutional co-operation with other relevant ministries at national level. The implementation of Regulation 211/2011 on the citizens' initiative led to the establishment of a national mechanism for interaction between the institutions involved in its implementation - the Ministry of Transport, Information Technology and Communications (MTITC) and Chief Directorate "Civil Registration and Administrative Services" – the Ministry of Regional Development and Public Works. The practical implementation of the Regulation is forthcoming, given that it starts operating from 01.04.2012. Currently, the CPDP and the MTITC are in the process of discussing the optimal methods of interaction in order to ensure the proper implementation of the Regulation at national level.

The proposal for a Regulation on the implementation of administrative co-operation via the Internal Market Information system, which is under discussion at EU level, required the setting up of a temporary working party to the Council for European Affairs with the joint participation of several ministries and institutions. Under the leadership of the Ministry of Economy, Energy and Tourism and the Ministry of Transport, Information Technology and

Communications, the CPDP nominated representatives to participate in the work of the group. Due to the nature of the information system and the need to process personal data from different fields, contained in that system, the CPDP's expertise is an important prerequisite for the preparation of national positions on the draft Regulation. The work on this initiative is still forthcoming.

Representatives of the Commission took part in an interdepartmental working party led by Chief Directorate "Civil Registration and Administrative Service of the Population", whose task was to draft and propose measures for protection against counterfeiting and forgery of documents issued on the basis of acts of civil status. For best solution of the task assigned, comprehensive implementation of legal regulations and organizational and technical tasks shall be performed. These specific activities should be implemented in their logical sequence, as they are connected and the absence of any component of the proposed measures would lead to unenforceability or compromise of the rest of the measures for protection of the documents issued on the basis of civil status records.

The active work for the preparation of amendments to the Law for Protection of Perosonal Data in order to implement the provisions of Framework Decision 2008/977/JHA greatly contributed to the strengthening of institutional relations between the CPDP and the Ministry of Justice. The collaboration continued in the process of preparation of amendments to the Law in its consideration by the Council of Ministers and the National Assembly, and subsequently in the notification process of the European Commission for fulfiling the obligation for transposition into the national legislation. The established professional contacts and reliable relations will be of great importance in the future transposition of other EU legal personal data protection instruments.

In 2011, on the occasion of the World Consumer Day and on the initiative of the Commission for Consumer Protection a temporary consulting office was opened which provided expert advice and information to mobile services users. This initiative involved combined teams of the Commission for Consumer Protection, Commission for Personal Data Protection, Communications Regulation Commission and representatives of mobile operators. The interest of the citizens to the temporary consulting office was great and visitors were mainly concerned about problems related to the transfer of numbers from one mobile operator to another, the termination of temporary contracts, the provision of clear and accurate information about relevant mobile services and contracts.

During the reporting period in connection with the fulfillment of their duties, representatives of the Commission for Personal Data Protection regularly communicated with many other institutions and administrations, such as the Public Administration Directorate and the Institute of Public Administration with the Administration of Council of Ministers, Ministry of Finance, National Audit Office, Ministry of Defence, Ministry of Labour and Social Policy (MLSP) and Chief Labour Inspectorate with the MLSP, National Revenue Agency and the National Social Security Institute.

In 2011, the Commission continued its successful co-operation with government bodies and NGOs to promote via their websites the content of the specialized section "Schengen Area" on the CPDP's website. The CPDP's campaign was supported by 11 ministries and 22 regional administrations (10 of them have published information and educational text of the information campaign on the home page of their websites), the National Association of Municipalities in the Republic of Bulgaria, "Customs" Agency and e-newspaper "Customs", International Organization for Migration, etc.

2. International co-operation with similar supervisory authorities and international organizations

In 2011, the Commission for Personal Data Protection continued its active participation in the process of preparation, revision, co-ordination and implementation of European legislation on data protection and the right to privacy, as well as exchange of information and experience on existing and newly emerged issues, bilaterally, at European and world level.

Along with the European contribution of the Commission to important issues related to the data protection future, the CPDP consulted and responded to a number of individual inquiries from Bulgarian and foreign individuals and organizations in connection with the use of Bulgarian and European data protection legislation.

Following the general trend for amendments to the data protection concerning their updating, their better interpretation by the data protection authorities and familiarizing the citizens with their rights related to the processing of their personal data, were held discussions on the envisaged changes in Convention 108/81/CE for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Commission for Personal Data Protection presented an opinion on the proposed changes concerning the scope of the Convention, clarification of the terms therein, including the data protection principles, the data conrollers' obligations, the individuals' rights and data protection authorities' powers and data transfers rules. Currently, the changes

in the Convention are subject of discussion within the T-PD (Consultative Committee of Convention 108/81/CE for the Protection of Individuals with regard to Automatic Processing of Personal Data). Considering the recommendations of the Schengen evaluation mission in 2009 relating to strengthening of international co-operation with other bodies and organizations in the data protection field, the Commission informed the Secretariat of the Council of Europe of its wish to participate fully in the work of this international forum.

In addition, the CPDP expressed its position on other important issues, both with regard to other documents of the Council of Europe (including the Convention on Access to Official Documents), and to the United Nations in connection with Resolutions 1888 and 1989 of the United Nations Security Council for the differentiation of two sanction regimes for the international terrorist organization "Al Qaeda" and the Islamist movement "Taliban".

In 2011 as a new initiative was defined the adoption and implementation of Regulation 211/2011 on the citizens' initiative. The Commission appointed its representatives to participate in the discussions on the practical implementation of Regulation's provisions, which together with the other competent Bulgarian authorities, would work on the establishment at national level of smooth mechanism to implement the Regulation. This European act allows for a referendum on matters of key significance for the European Union, which requires personal data processing and introduces mechanisms for ensuring data safety, respectively, the data controllers on Bulgarian territory, who will collect and process information in this regard should observe their obligations.

Another important issue in 2011, following the introduction of uniformed European system to be foreseen in the new European legal data protection framework, was the personal data controllers' registration in the CPDP, and in this regard was exchanged information on inquiries received by other data protection authorities. The Commission also received numerous inquiries from foreign entities on the matter.

Interesting activity during the year were the questionnaires of the Center for Historical Research and Documentation on War and Contemporary Society and the International Association of Privacy Professionals, based in the USA, concerning the data protection and privacy legislation in Bulgaria, the data controller's requirements and the competence of the Commission under the Law for Protection of Personal Data, and the 2010 practice on the matter. After a detailed analysis of the questions posed, both cases received specific and comprehensive information on the relevant issues.

With regard to the bilateral co-operation, the Commission received a request for information from another data protection authority regarding the national practice by supervising the use of the Visa Information System. The response provided by the Commission clarified the specifics of the current legislation on these matters, the competent authorities and bodies to work with VIS, data processing purposes, the control powers of the Commission and the practical conduct of data protection inspections, which are realized on the basis of a questionnaire prepared in advance for the purpose of the relevant inspections.

Regarding the use of the system for co-operation in the field of consumer protection, the Commission received a questionnaire on the current status of data protection in the Republic of Bulgaria. A number of issues were posed, especially regarding the rules and procedure of access to personal data collected in the system.

During the reporting period the Commission received an inquiry on legal practice connected with the handling of telephone numbers and other numeric data (e.g. IP addresses), as personal data, and information was provided on the practice of the Supreme Administrative Court of the Republic of Bulgaria, including on CPDP's decisions.

In 2011, the Commission for Personal Data Protection actively used the opportunity to share practice and information on data protection legal provisions and their practical implementation in other EU Member States on two issues that emerged in the course of activities and on which was necessary to be expressed an opinion. The first issue was related to the request made by the US-based company Google Inc. for the implementation of the program Google Street View in Bulgaria. In this regard, analysis was made of the information received from 18 data protection authorities, 13 of which are located in EU Member States. Based on the analysis of the other data protection authorities' practice, the Commission for Personal Data Protection expressed its official opinion on the requirements for the personal data protection that must be met by Google Inc. in conjunction with the Law for Protection of Personal Data, and gave specific instructions in this regard.

The second issue was related to a request received in the Commission on installing cameras to perform CCTV surveillance in hospital's operating rooms and a request for information was sent to other data protection authorities on the legal regulation of this issue and their practice. Information was exchanged with 16 data protection authorities.

In connection with an inquiry by the Slovenian data protection authority, the Commission for Personal Data Protection sent information about the transposition into the Bulgarian legislation of the revised Directive 2002/58/EC of the European Parliament and the Council on the processing of personal data and the protection of privacy in the electronic communications sector and the competent authori-

ties in case of personal data security breach and by the transfer of messages through electronic communications network.

3. Participation in working parties and international events

In connection with the annual celebration of the European Data Protection Day (28 January) and the 30th anniversary of the adoption of Convention 108/81/CE, in January 2011 numerous events were organized, where many issues were discussed in relation to the new challenges to the personal data protection, the required amendments to the legal framework and the need of synchronized international regulations in the privacy and data protection field.

In 2011, the Commission for Personal Data Protection continued its effective participation in the meetings of the Joint Supervisory Authorities of Europol, Schengen and Customs, the Working Party on Police and Justice, as well as the specialized Eurodac Supervision Co-ordination Groups and the Customs Information System, where some specific issues were discussed in relation to: the terrorist finance tracking program; future development of the supervisory authorities; the rules for access and data processing in specialized information systems; implementation of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters; changes in legislation; the implementation of the prepared Catalog for Privacy Impact Assessment and the supervision and co-operation with other international bodies and data protection institutions.

The main issues discussed in the Joint Supervisory Body of Europol in 2011 were the results of the inspection on the implementation of the Terrorist Finance Tracking Program. Among the covered areas during the inspection were the type of personal data to be exchanged and clarification of the powers of Europol and the competences of Joint Supervisory Authority by data transfer to the USA. It was decided that after the completion of each action under the Program records should be provided, which should be subject to review by the Joint Supervisory Authority.

Another important aspect of the work of the Europol Supervisory Body during the year was the preparation of the concept for Europol analysis work files, including the options to refine the access criteria, the criteria for entering information in the files, the categories of data entered and how will the security structure look like.

That year discussions were also held on methods to reform the Europol's legal framework that should reflect the current developments and the impact made on society by information technology.

At the annual meetings of the Joint Supervisory Authority of Schengen the results of inspections on the implementation of various provisions of the Schengen Convention were subject of discussion. The discussion focused on all aspects, required technical equipment and documents for the major review of the Schengen Information System (SIS I+4All), forthcoming in 2012.

Another significant part of the work of the Schengen Supervisory Authority, having direct impact on citizens, was analyzing the results of the pan-European survey on the right of access to information in the Schengen Information System. The survey contributed to the definition of the basic differences that exist regarding the right of access depending on whether or not a country is a member of the Schengen Area in order to overcome them. Important issues were also considered in order to achieve greater efficiency in processing citizens' requests for access in cases when the process involves several countries - what should be the language of requests, what sould be the data collection period, what actions should be taken in case of refusal, and the role of data protection authorities.

An important activity of the Eurodac Supervision Coordination Group in 2011 was the preparation and conducting of an inspection on the advance data deletion in the Eurodac system and the adoption of a Report on Results. The Commission for Personal Data Protection contributed in answering to the questionnaire distributed to Member States, and the made comments were included in the final report.

2011 was also important to strengthen the co-operation of the Eurodac Supervision Group with organizations such as "Amnesty International", the United Nations High Commissioner for Refugees Agency and the European Council on Refugees and Exiles. The stronger co-operation aims at creating new ways to share information and will contribute to the exchange of experiences, best practices and the execution of joint actions.

Important issues were discussed with regard to the Working Party on Police and Justice, *inter alia:* an Action plan on the implementation of political priorities set out in the Stockholm Programme for the area of justice, freedom and security and a joint study on the practices of processing and further use of DNA profiles in the work of law enforcement authorities.

In 2011 the Commission participated in the meetings of the Art. 29 Working Party and its subgroups, where important issues were discussed relating to the personal data protection, such as: Safe Harbor Agreement and the mechanisms to protect privacy and personal data set out therein; update of the provisions of Convention 108/81/CE, clarification of terms of Directive 95/46/EC and other related EU

privacy abd data protection legal acts; consideration of the Annual Report of the Art. 29 Working Party, in which the Commission made contribution, covering: the amendments to the Law for Protection of Personal Data; CPDP's activities connected with reporting the progress on Schengen; specific cases addressed in the Commission; information on the practical execution of the foressen activities; new powers in connection with the adoption of European legal instruments; discussing the changes that are proposed in Directive 95/46/EC; recognition of the adequacy of data protection in third countries – in 2011 the opinion of New Zealand was discussed and adopted, the decision of the European Commission is forthcoming; evaluation of the adequacy of data protection in Mexico and Israel; examining draft legislation related to e-security and activities related to the police and justice; the personal data protection within the internal market information system and the Consumer Protection Co-operation System; combating money laundering; issues related to products and services offered in the telecommunications sector.

The CPDP continued its active participation in the International Working Group on Data Protection in Telecommunications, which during the reporting period mainly discussed issues related to Internet search engines, electronic payments, e-mails, privacy in social networks, the use of mobile devices, geolocalization and biometrics data, software offering Internet services, recording of the visitors to web pages, processing of personal data during the transfer of information between computers in a network.

In June 2011, in Budapest, the Republic of Hungary, an International Conference on Data Protection was held which reviewed issues related to the amendments to the data protection legal framework and the implementation of these provisions, and the problems associated with them.

At the 13th Annual Meeting of the Central and Eastern Europe Data Protection and Privacy Authorities participants discussed amendments to the legal framework, the existing practices in the implementation of legal acts, and several similar data protection authorities expressed their willingness to receive more detailed information on the CPDP's activities and expanding bilateral co-operation.

In November 2011, 33rd International Conference of Data Protection and Privacy Authorities took place in Mexico City, Mexico. The main purpose of the event was the establishment of privacy and personal data protection rules, standards and methodologies and their global application, as well as achieving closer co-operation between data protection authorities. The conference outlined the following guidelines for future development in the data protection field: strengthening the independence of the data protection authorities; consistency of the objectives of the system; the role of the court in respect of data protection; increasing public awareness; efficiency and speed of application of decisions; the power and importance of the data protection authorities; the application of the notification regime and accountability of personal data controllers; education and training in the data protection field, co-operation and unification of requirements for the owners of large databases; scientific research and personal data protection; personal data by disasters, accidents and subsequent reintegration; the role of technology professionals in the data protection authorities; the establishment of common criteria for protection (special data protection and privacy certification).

4. Regional co-operation

In 2011, the Commission for Personal Data Protection developed a dynamic regional co-operation through the exchange of bilateral visits, signing of joint documents and participation in various regional initiatives.

The Commission participated with its representative in the realization of the planned inspection under the Police Cooperation Convention for Southeast Europe on the status of personal data protection in the Republic of Albania, in order to assess whether or not an adequate data protection level was implemented/established in the country. The other signatories of the Conventions are: Bosnia and Herzegovina, the Republic of Macedonia, the Republic of Moldova, the Republic of Romania and the State Union of Serbia and Montenegro. Following the inspection, the CPDP expressed the position that there is no reason to prevent the exchange of information containing personal data with Albania, for the purpose of and in accordance with the provisions of the Police Cooperation Convention for Southeast Europe. However, reservation was expressed on the proposed amendment to the Procedural rules regarding the criteria for assessing the personal data protection.

In 2011, discussion was also initiated on matters related to co-operation in the justice and home affairs area within the Eastern Partnership, where the Commission supported the European Commission's position on the need to encourage the Eastern Partnership countries in the ratification of international legal instruments in the data protection field, to adopt the necessary national legislation and establish the required bodies. The Commission stated that the special character of the set activities and data protection legal acts as well as of the exchange of information on various issues should be taken into account and an adequate data protection level in countries not members of the EU and the European Economic Area should be guaranteed.

In the period 9 - 10 June 2011 the Commission for Personal Data Protection welcomed a delegation of the Directorate for Personal Data Protection of Macedonia. During the two-day visit the Bulgarian and Macedonian data protection authorities discussed a wide range of topics covering both current developments and legislation relating to personal data in both countries, and participation in various public initiatives and projects.

The visit ended with the signing of a Declaration on Mutual Co-operation, which will allow for the expanding of bilateral relations in various priority areas, for example, the privacy in the process of technological development and increasing the awareness of citizens about their data protection rights.

Additionally, both parties reviewed a draft Memorandum of Co-operation with the State Office for Data Protection of the Republic of Ukraine to enhance institutional capacity for the personal data protection.

XII. Administrative capacity and financial status

1. Administrative capacity

1.1. Total number of permanent employees

In 2011, the total number of permanent employees of the CPDP is 81. This figure includes:

• Employees employed under full-time contracts for January – November 2011:
- under official contracts – 49;
- under labor contracts – 19.

• Vacant positions:
- under official contracts – 13;
- under labor contracts – 1.

During the reporting period, 7 employees were employed in total: under official contracts – 6, and under labour contract – 1. The official contracts of 6 employees were terminated. 3 employees were reappointed under official contracts for the replacement of an absent employee. There are no employees promoted to higher rank or higher post during the reporting period.

No competitions for vacant positions in the administration of the CPDP were held in 2011.

1.2. Training of employees

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

As in previous years, in 2011 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 for increasing the quality of activities in the respective units;

• Timeliness - the training should correspond to the changes in legislation relating to the CPDP activities and the best national and international practices;

During the reporting period priority was given to those training courses that would help to increase work efficiency and contribute to reaching the CPDP's objectives.

At the beginning of 2011 an Annual Training Plan was drafted and approved with two main activities:

• Mandatory training - for employees appointed for the first time as civil servants;

• Specialized training – for professional development and qualification rising.

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

The IPA mandatory training was attended by 3 newly appointed civil servants at expert position and 1 newly appointed civil servant at managerial position.

The IPA specialized training, connected with the CPDP's annual priorities for the reporting period, was attended by 44 officers. This training is related to professional development and qualification rising of the CPDP's administrative staff.

In January 2011 a seminar was organized from the Commission entitled "CPDP - European data protection standards. Bulgaria in Schengen.". The seminar was attended by members of the CPDP, administration officials, representatives of the Ministry of Interior and the media. The Commission presented and analyzed relevant data protection issues, and new changes in European data protection legislation and the activities under the forthcoming accession to Schengen.

In order to improve the administrative capacity of the employees of the CPDP, on 9 and 10 November, 2011, a seminar was held, which examined the latest data protection developments and acivities. During the seminar, attention was given to the following main topics: problems with the use of electronic communications and tasks arising from Regulation № 211/2011; amendments to the Law for Protection of Personal Data in the context of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

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

• "Management of health and safety at work"

• "Recent changes in the Law on Public Contracts (LPC)" and

• "Protection of classified information" with the participation of 13 employees in total.

Compared to 2010, in 2011 there is greater interest for participation in courses and programs to raise the officials' qualification.

The overall assessment of the effectiveness of the training sessions held indicates a connection between the training process and execution of the CPDP's objectives, tasks and priorities. The skills acquired by the employees are used in their usual activities.

1.3. Appraisal of employee performance

The annual appraisal of employee performance (employees under official and labor contracts) in the administration of the CPDP provides the appraising manager with objective information about:

• the level of professional qualification of employees in the relevant department and the compliance of their professional qualification with the requirements set out in the job descriptions;

• identifying the development for each employee to improve his/her professional competence;

• improving relationships in the work process including between superiors and subordinates, and to improve teamwork;

• creating environment for the realization of fair and transparent procedures for professional and career development of the CPDP's employees.

In compliance with the Ordinance on the rules and procedures for the appraisal of employees in the public administration sector in the period from June 1 to July 15, 2011, an interim meeting was held between the apprasing manager and the appraised employee, and in November 2011 - a final meeting between them.

2. Procedures under the LPC and the Law on Small Public Contracts (LSPC)

In August 2011, two procedures were initiated under Art. 2, Para. 1, Item 2 of the Ordinance for the award of small public contracts with subject-matter: development of software for a "Paperless Meeting-Management System" and development of software for the "Improvement of a Call Center". The procedures have been successfully completed and contracts were concluded with the participants ranked first.

In October 2011 procedures were initiated under Art. 2, Para. 1, Item 2 of the Ordinance for the award of small public contracts with subject-matter:

- Selection of provider of telecommunications services for GSM standard – 2012;
- Delivery of automobile fuel and accessories in 2012;
- Selection of service centers for the repair of the motor vehicles of the CPDP in 2012.

The procedures have been successfully completed and contracts were concluded with the participants ranked first.

For the optimization of the administrative capacity of the CPDP, it is essential to move the CPDP in a building provided for free management by virtue of RMS № 566/2011. The realization of this goal is driven by the need to create conditions for the normal functioning of the institution and is in direct link and relation to the EU idea to create legal safeguards for the institutional, financial and material competence and independence of national data protection supervisory authorities in different Member States.

3. Budget

By means of the Law on the State Budget of the Republic of Bulgaria (LSBRB) for 2011 and Council of Ministers Decree № 334 dated 29.12.2010 on the implementation of the state budget of the Republic of Bulgaria for 2011, the operating budget of the CPDP was approved to the amount of BGN 2 560 000.

During the year the budget of the Commission was increased by an amount of BGN 1 400 000, by an adjustment made by the Ministry of Finance in connection with Decision № 582/2010 of the Council of Ministers on the provision of a part of a property - public state property – to the CPDP free of charge.

In pursuance of Decision № 566/22.07.2011 of the Council of Ministers to repeal Decision № 582/2010, a proposal was made to the Ministry of Finance and an adjustment was made to transfer funds amounting to BGN 1 400 000 to the budget of the Ministry of Defence for the purpose of repair and use of the building.

After these adjustments, the budget of the CPDP remained unchanged in the initially approved amount of BGN 2 560 000.

The costs incurred by providing the activity of the Commission for Personal Data Protection and its administration come to the total amount of BGN 2 344 993, or 91,6 % of the approved estimates for the year. The types of costs distributed by sections of the Unified Budget Classification (UBC) are presented in the following table:

Section	Cost Description	Amount (BGN)
01-00	Salaries and wages for staff employed under labour and official contracts	862 978
02-00	Other remunerations and payments for the staff	69 157
05-00	Compulsory social securities paid by employers	223 779
10-00	Allowance	1 108 360
52-00	Acquisition of tangible fixed assets	17 935
53-00	Acquisition of intangible fixed assets	62 784
	Total budget expenditures	**2 344 993**

In 2011, revenues of BGN 75 700 were reported, representing administrative fines and property sanctions imposed by penal decrees issued by the CPDP as a public authority under the LPPD. As the LSBRB for 2011 enacts, all amounts submitted to the budget account of the CPDP of fines and penalties are transferred as revenue for the state budget.

XIII. Priorities of the CPDP for 2012

1. The following CPDP's activities started in 2011 will remain priorities in 2012 due to their constant and fundamental nature:

• **Participation in activities related to changes in European data protection legislation and implementation of European legal personal data protection instruments.** Regarding this priority, the active participation and national contribution to the expected proposals of the European Commission for the amendment to Directive 95/46 will be the main direction in the work of the supervisory authority in 2012. Activities will be initiated on the national implementation of Regulation 211/2011 on the citizens' initiative and the national and European co-operation with respect to its specific application, as well as review and assessment of the Data Retention Directive. The activities on current EU issues will remain on the agenda, such as processing of Passenger Name Record data, exchange of information and data within the Internal Market Information system and the introduction of a European Terrorist Finance Tracking Program. One of the main challenges will be the participation of the Bulgarian supervisory authority in the development of European instruments (including legal) to ensure better protection against cybercrime and to ensure the privacy and personal data protection in the telecommunications sector.

• **Continuation of effective information and educational activities** on various aspects and among different target groups in society:

- Expanding the information campaign and raising the awareness of citizens about their data protection rights, including in connection with the forthcoming accession of the Republic of Bulgaria to the Schengen Area and the Visa Information System;
- Specialized information aimed at young audiences and their parents, on the threats online.

In 2012, the Commission will continue the implementation of its consistent policy of development and positive institutional publicity, transparency and openness in the exercising of main activities, of successful partnership and collaboration with other state bodies, with representatives of civil society and with the media.

• **Exploring the needs of data controllers for data protection training.** In this area of activity in 2012 the Commission will emphasize on upgrading and improving the results it has already achieved. To carry out this priority, a special questionnaire was developed by the Commission which aims at providing "feedback" between data controllers and the CPDP and the circulation of this questionnaire in

2012 will be realized simultaneously in the following manners: electronically, via the Registry and Reception desk of the CPDP, in the course of the supervisory acivities of the Commission by conducting ex-ante, on-going and ex-post inspections, via the web site of the CPDP, as well as via the exchange of correspondence during the review of administrative proceedings before the CPDP.

2. An important priority for the Commission in 2012 is to lay the foundations of the new activities following the new supervisory data protection authority's powers obtained with the latest amendments to the Law for Protection of Personal Data in 2010 and 2011, as follows:

• **Conducting negotiations and concluding co-operation agreements with similar supervisory data protection authorities.** In connection with this, in early 2012, the Commission for Personal Data Protection will present to similar supervisory data protection authorities, the model draft agreement on co-operation in the personal data protection field, approved by the Council of Ministers as a basis for negotiations. To organize the execution of these new powers, the Commission will set up expert groups to prepare and conduct negotiations with the data protection authorities in particular countries.

• **Amendments and supplements to the personal data protection legal acts.** The Commission considers that it is extremely important to harmonize Ordinance № 1 on the minimal level of technical and organizational measures and the admissible type of personal data protection with the latest developments in technology and the additional safeguards for data security. Adopting legislative changes in the Regulation on the activity of the CPDP and its administration also aims to contribute to the optimization of the supervisory authority with regard to the procedures that were brought to its attention, and regulate the rules for data controllers' deletion in accordance with the recent legislative changes.

• **Issue compulsory instructions concerning the retention and access to traffic data in accordance with the Law on Electronic Communications.** This new competence of the Commission aims to establish clear and uniform rules for all entities involved in the process of retention of traffic data to enable the supervisory authority to fully exercise its supervisory functions under the Law on Electronic Communications.

3. In accordance with the stated priorities of the Government of the Republic of Bulgaria to build e-Government, the Commission considers the electronic services it provides to citizens as a part of the country's e-government.

To achieve this priority, the Commission will continue its co-operation with institutional bodies, setting up the e-government to include the data protection authority among the first departments to provide e-services. The maintenance of public records and the registration of data controllers will continue to be build on the basis of the "one stop" technology.

Fig. 1

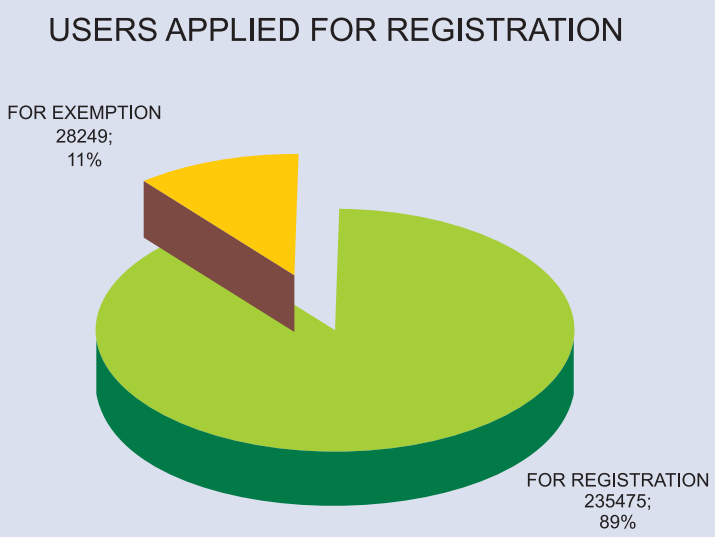

USERS APPLIED FOR REGISTRATION
FOR EXEMPTION
28249;
11%
FOR REGISTRATION
235475;
89%

Fig. 2

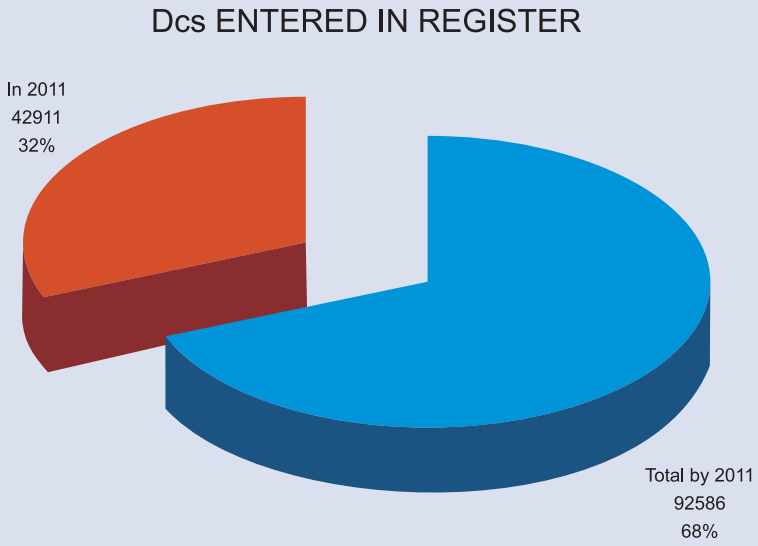

Dcs ENTERED IN REGISTER
In 2011
42911
32%
Total by 2011
92586
68%

Fig. 3

Dcs EXEMPTED FROM REGISTRATION

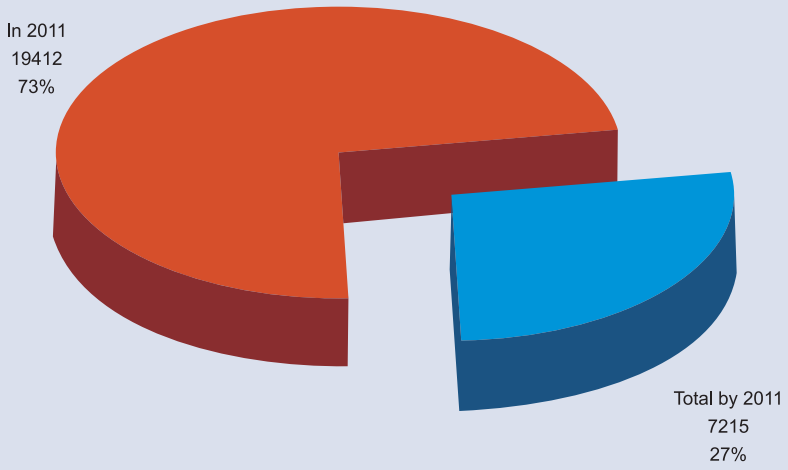


Fig. 4

Dcs USING UES BY DOCUMENT SUBMISSION

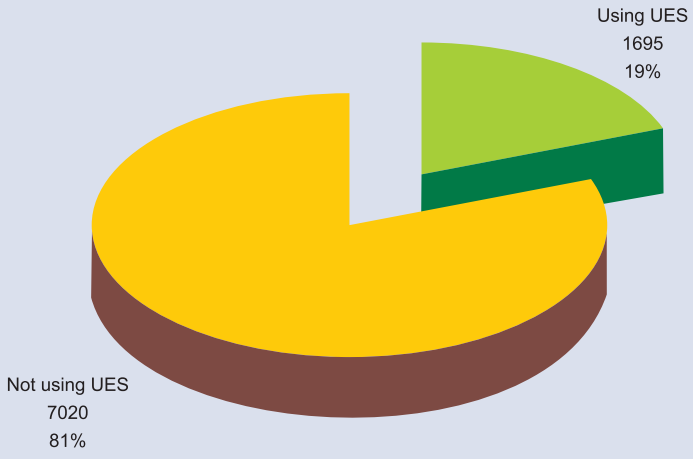


Fig. 5

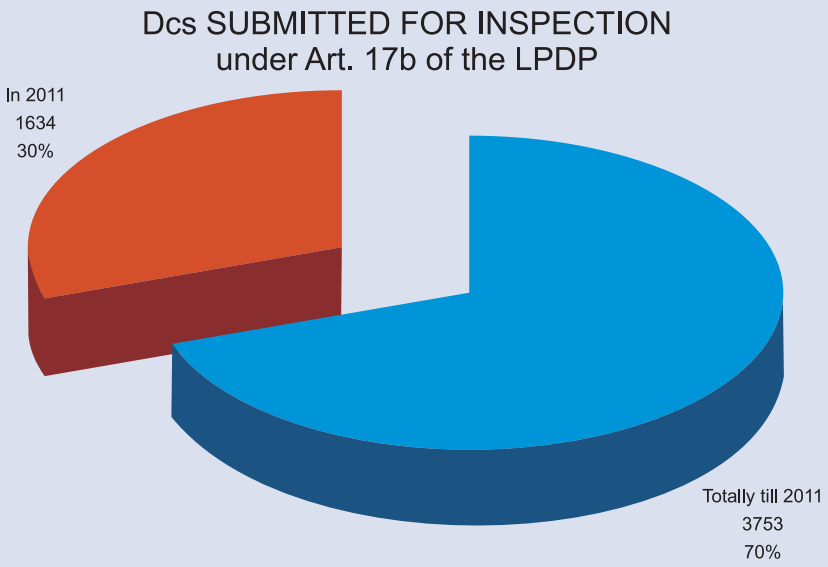

Dcs SUBMITTED FOR INSPECTION
under Art. 17b of the LPDP
In 2011
1634
30%
Totally till 2011
3753
70%

Fig.6

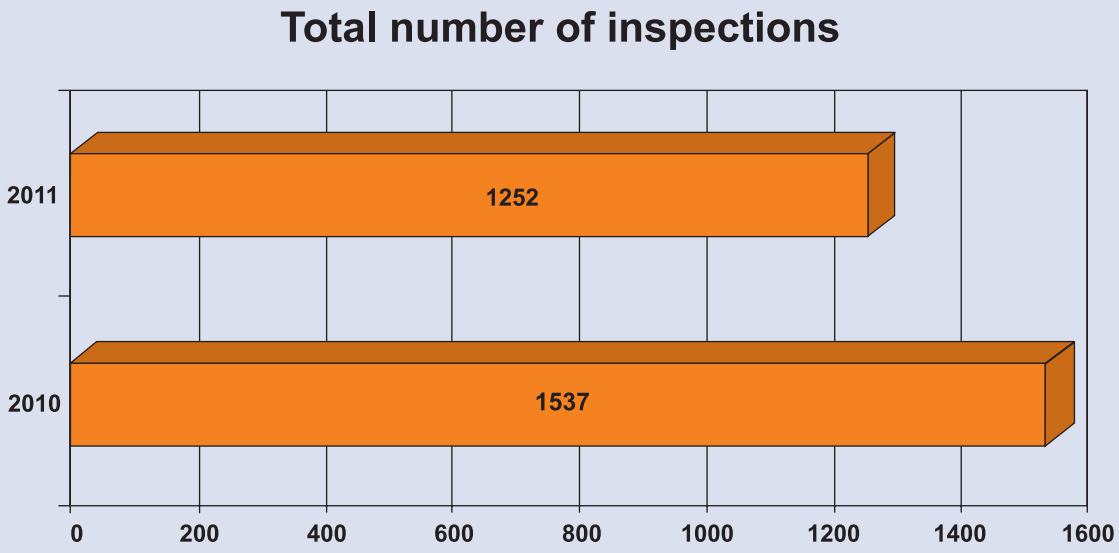

Total number of inspections
2011
1252
2010
1537
0
200
400
600
800
1000
1200
1400
1600

Fig. 7

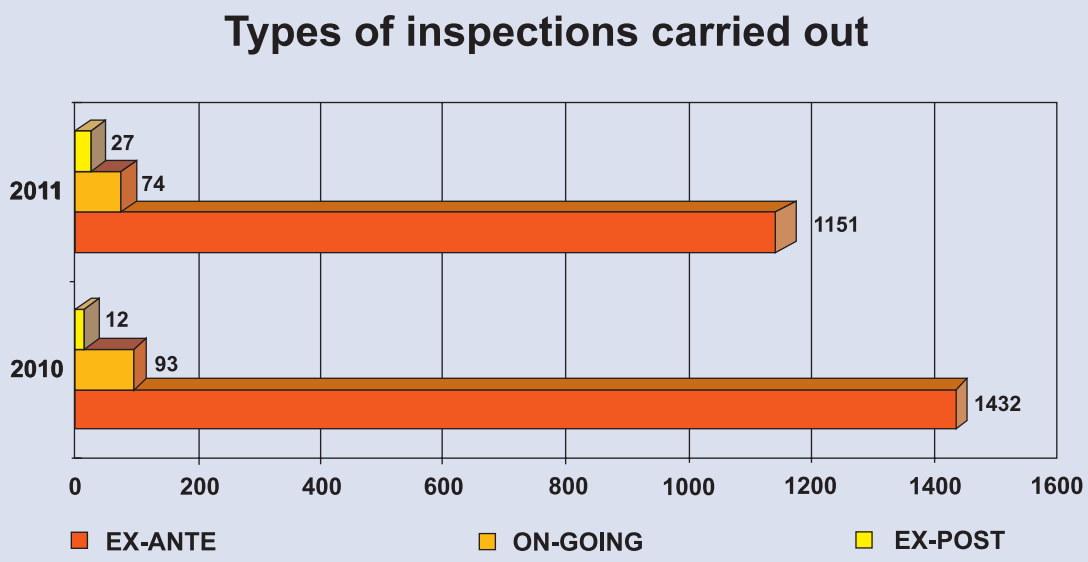

Types of inspections carried out
2011
27
74
1151
2010
12
93
1432
0
200
400
600
800
1000
1200
1400
1600
EX-ANTE
ON-GOING
EX-POST

Fig.8

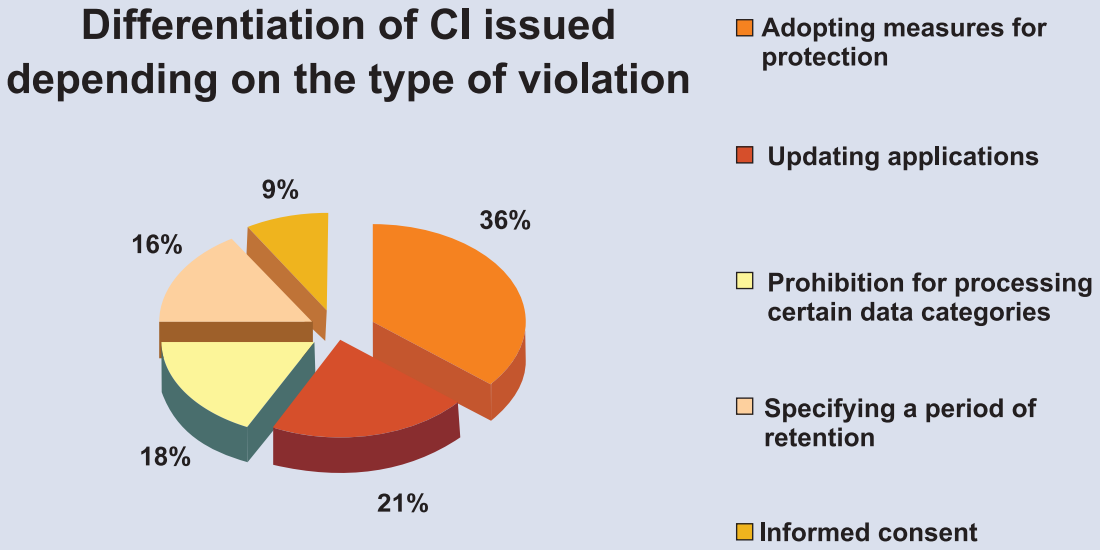
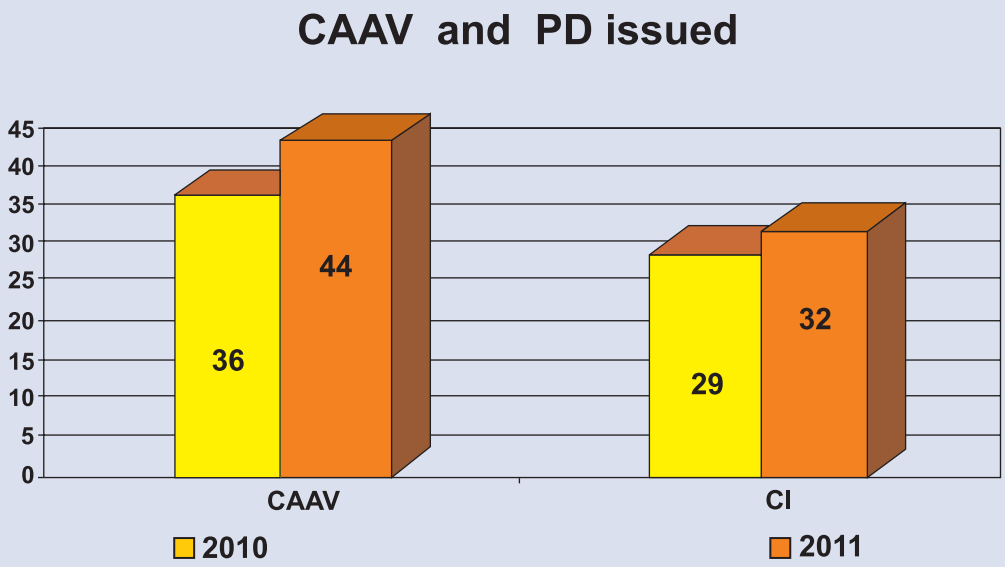

Differentiation of CI issued depending on the type of violation
9%
36%
16%
18%
21%
Adopting measures for protection
Updating applications
Prohibition for processing certain data categories
Specifying a period of retention
Informed consent

Fig. 9


CAAV and PD issued
45
40
35
30
25
20
15
10
5
0
36
44
29
32
CAAV
CI
2010
2011