OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

Report
on the State of Personal Data Protection and Activities of the Inspector of Georgia

2015

www.personaldata.ge

TABLE OF CONTENT

Published with the financial assistance of the European Union and UNDP.

INTRODUCTION

Reporting period for 2015 was very important due to implementation of personal data protection legislation and development of court practice; also, activation of supervision system over the investigative activities related to wiretapping and computer data and increase of citizens' complaints. It is worth mentioning that European Commission Report for 2015 gives positive evaluation to the reform in the area of personal data protection, undertaken within the scope of the European Union Visa Liberalization Action Plan; the implementation index of the activities under the National Action Plan of the Association Agenda between Georgia and the European Union must also be highlighted. In 2015, the Office of Personal Data Protection Inspector became the member of unions of International and European Data Protection Authorities; it was represented at the Council of Europe's special committee and bureau, which carried out intensive work on modernizing Council of Europe Convention and the General Data Protection Regulation of the European Union.

As a result of inspections, trainings, consultations, close cooperation with public and private institutions by the Personal Data Protection Inspector in 2015, number of violations have been eradicated; certain processes of data processing be it technical or legal, have been improved and brought to compliance with law. Despite the achievements, there still are lots of challenges related to privacy guarantees, implementation of personal data protection standards and reduction of threats of illegal data disclosure. For these reasons, this report describes the results of the response to violation of personal data protection legislation, main trends, recommendations for improvement of the state of personal data protection and areas of privacy that have been subject to wide public discussions last year.

GROUNDS AND PRINCIPLES OF DATA PROCESSING

GROUNDS AND PRINCIPLES OF DATA PROCESSING

In accordance with Article 1 of the Law of Georgia on Personal Data Protection, "… the purpose of this Law is to ensure the protection of human rights and freedoms, including the protection of the right to privacy, in the course of the processing of personal data".

In order to achieve this purpose, it is important that principles envisaged by law are upheld at all stages of personal data processing and relevant legal ground is identified, as this particular unity ensures fair balance between citizens' right to privacy and interests of data controllers.

As a result of examination of the complaints and conducted inspections by the Inspector in 2015, it was determined that one of the main problems still is non-compliance to the data processing principles. Organizations (data controllers) do not have specific and clear purpose for data processing; thus, information is being processed inadequately and disproportionately to the purpose; and in most cases the term of data storage is still not defined.

Organizations' access to large volumes of personal data or outdated information creates certain obstacles for the citizens in the course of obtaining different services and exercising their rights; in some cases, due to past conviction record or disclosure of health data, several citizens have been subjected to certain discriminating treatment.

In public sector, multiple duplication of electronic bases containing personal data without due assessment are frequent. For instance, in several organizations, several copies of one and the same electronic database are kept – each copy for different purpose, while it is quite possible to maintain the database within one domain and provide access by other bodies through relevant technical means. It would ensure proportionate processing of data, their updating, and protection and also cost reduction as a result of optimization of the processes.

In 2015 there were cases when public and private organizations have processed personal data, including special category of data without legal grounds. Often, when checking legitimacy of data processing, organizations fail to identify proper grounds and are unable to present proper legal arguments for owning the data or for otherwise utilization of such data. During the reporting period, facts of single or multiple exchange of personal data between public agencies on the basis of oral agreement or memorandums lacking specific legal ground were identified, while, current legislation requires regulation of such cases by the normative act. Legislation in force authorizes public agencies to create, manage and permanently update databases and grant access to information to other public agencies for the purpose of fulfilment of their respective functions imposed by law. One of the good examples is the State Service Development Agency; one of the key functions of this agency is maintenance of common population register, registration of civil acts, and issuance of identification documents. In order to fulfil the functions imposed by legislation, different public agencies need permanent access to such data and for this purpose, on the basis of relevant normative acts information is requested and received through technical channels. Such regulation helps to avoid database duplication, use of outdated and inaccurate data; furthermore data are being processed purposefully and other organizations receive those data only, which they need to fulfil their functions.

During the reporting period, 41 citizens applied to the Office of Personal Data Protection Inspector with the request to take action against the cases of data processing without legal grounds, violation of data processing principles, unsubstantiated public disclosure and unauthorized access to data by public and private organizations. As a result of examined complaints and inspections 18 cases of unsubstantiated data processing and violation of data processing principles have been identified. Consequently, part of the organizations was imposed administrative sanction – a fine or a warning, and in some cases, sanctions were not imposed due to expiry of two month period from the date of commission of violation, as established by current legislation. Nevertheless, the organizations were given mandatory instructions in order to eradicate the gaps existing in relation to data processing.

This report includes examples of violations identified by the Office of Personal Data Protection Inspector during 2015; generalization of these violations clearly depicts real state and problems of personal data processing without principles established by law and due legal grounds.

Access to Credit Information

In accordance with rules and procedures established by the commercial banks operating in Georgia, information containing personal data of those persons who have current, outstanding or poorly fulfilled liabilities towards commercial banks is handed over to the organization founded by commercial banks – JSC "CREDITINFO Georgia". This organization permanently receives information about debtors from all commercial banks operating in Georgia. As a result of processing of received information, all stakeholders (commercial banks, microfinancing organizations, etc.) enrolled into the organization's system have technical access to information regarding data subject's liabilities towards specific financial organization. Commercial banks transfer such information upon individual's consent, though in several cases examined by the Inspector, the consent obtained from the debtor concerned transfer of information to JSC "CREDITINFO Georgia" for a specific purpose and for the interest of the relevant creditor and not for different purpose or for disclosure of such information to persons with other financial interests.

In 2015, a citizen applied to the Inspector and asked for response action; the citizen stated that one of the microfinance organizations checked his/her data in the database of JSC "CREDITINFO Georgia" without his/her consent. During examination of the case it was established that the microfinance organization had citizen's consent on data processing on the basis of loan agreement, within the scope of loan relations. Though, upon expiry of debt relations the microfinance organization once again checked the information about the person in the database without his/her consent, for the purpose of offering a new credit product. During examination of the complaint the Inspector identified that the microfinance organization acted beyond the authorization granted by the citizen and violated the law while checking individual's data, as the organization had no relevant grounds for data processing – namely, the consent. The law of Georgia on Personal Data Protection defines the consent of a data subject as "free consent of a data subject, after receiving relevant information, on his/her data processing for a specific purpose, expressed orally, through telecommunication or other relevant means, which can clearly indicate the will of a data subject". In order for the data subject to be properly informed about the purpose of the consent on data processing and its out-

comes, it is important that he/she receives clear and specific information about the purpose of data processing before such data subject expresses his/her will. The will expressed upon receipt of such information can be used as the ground for data processing.

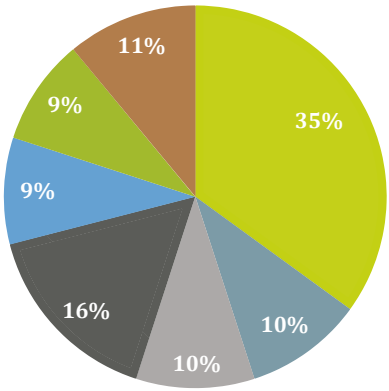
During examination of this case it was also identified that JSC "CREDITINFO Georgia" made citizen's information readily accessible without any prior mechanism of checking legal grounds.

In addition, current legislation does not establish any specific regulations with regard to operation of JSC "CREDITINFO Georgia", unlike financial institutions; operation of financial institutions, including protection of customers' rights, is precisely regulated by different normative acts. JSC "CREDITINFO Georgia" maintains one of the largest databases in the country, which currently contains data on 2 206 180 persons; despite this number, protection and access to information (including its issuance in exchange of payment) is not regulated on a normative level.

Despite the fact that Personal Data Protection Inspector immediately responded to unlawful access to the databases of JSC "CREDITINFO Georgia", the measures taken by the Inspector may turn out to be insufficient for preventing threats related to absence of due regulations. For eradicating risks of inappropriate processing of financial data and effective protection of citizens' rights, it is recommended to create additional mechanisms on the legislative level.

CITIZENS' COMPLAINTS

Topics



120
COMPLAINTS

- **Direct marketing**
- Failure to provide information to citizens
- Disclosure of data without legal grounds
- Data processing without legal grounds and in violation of principles
- Legality of access to data
- Legality of video-audio recording
- Legality of data processing by law enforcement authorities

In Total

54

Organizations Were Inspected

Unauthorized Access to Information Kept in Databases by the Personnel

In order to uphold principles of lawfulness and obtain public trust, it is important that citizens have the feeling that their information, collected by any organization, can only be accessed for legitimate purpose and only when necessary and with pre-established needs. This issue becomes even more urgent when the data controller is a law enforcement body. The Ministry of Internal Affairs of Georgia is one of the largest public agencies that processes huge amount of personal data for fulfilling its duties prescribed by law. Databases of the Ministry of Internal Affairs contain information that relates to: criminal and administrative liability, ownership of the transportation means and driver's license, crossing border by individuals, drug tests, missing persons, wanted persons, etc.

Considering volume of information processed at the Ministry and number of people employed by the organization, the risk of unauthorized access to personal data must be taken into account. Therefore, it is important that data controllers, especially the big ones, clearly and comprehensively define access rules and ensure strict control over lawful use of such information by their employees, and timely detection of cases of unauthorized access.

During 2015, the Ministry of Internal Affairs of Georgia regulated the issues of employee access to the Ministry's information resources; it established time limits for storage, deletion and archiving of personal data in the Ministry's filing systems; control over employees' lawful access to databases has become stricter. Access to archived information resources is allowed only on the basis of well-reasoned written application.

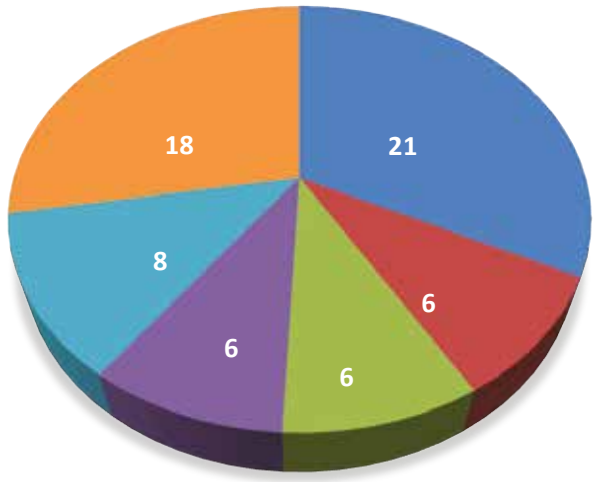
In 2015, the Personal Data Protection Inspector examined several cases of personal data processing by the Ministry of Internal Affairs of Georgia. In some of the cases violation of personal data protection legislation was not established or no responsibility was imposed due to expired term; in two cases the Ministry was imposed an administrative sanction - fine in the amount of GEL 2000. One of the violations was identified during examination of citizen's complaint. In particular, the citi-

zen stated that while driving his/her own vehicle, he/she noticed another vehicle that was noticeably maneuvering in his/her vehicle's vicinity. In several minutes the complainant received an SMS on his/her cellphone from an unknown number. According to the SMS, the sender was the driver of the above-mentioned vehicle; he/she indicated that he/she worked at the Ministry of Internal Affairs of Georgia and obtained complainant's telephone number and other personal information at the Ministry. The Personal Data Protection Inspector examined the issue of unlawful access to citizen's data. It was established that the driver of the vehicle was not the employee of Law Enforcement body, though he obtained personal data of the complainant for his/her personal reasons, and with the help of the Ministry's employee. The Ministry responded to this fact and the employee, who obtained information without proper legal grounds and handed it over to third party, was subjected to disciplinary responsibility. Despite the above, the Ministry was fined in GEL 2000 for processing of data without due grounds.

The Ministry of Internal Affairs of Georgia appealed the decision of the Inspector at the Tbilisi City Court; the motive of the appeal was that due to off-duty access to citizen's data the Ministry's employee received strict warning and therefore, the Ministry was not supposed to be imposed additional administrative responsibility. The court (case N4/563515) did not share the position of the Ministry and upheld the Inspector's decision.

In total 64 cases of violation were identified in 2015; in 23 cases the sanction could not have been imposed due to expiry of 2 months' time limit. 41 organizations were imposed administrative liability in terms of fines or warnings.

DETECTED VIOLATIONS



Lawfulness of Drug Registry

For public sector, the Law of Georgia on Personal Data Protection entered into force in 2012. Since then, many data processing procedures have been regulated and put into legal framework. Though, examination of citizens' complaints by the Inspector in 2015 revealed cases when public organizations processed and disclosed data only on the basis of oral agreement between the heads of such organizations, and without any legal grounds.

In order to ensure lawfulness of personal data processing, data controllers are obliged to process, including to obtain, transfer and provide access to personal data maintained in their respective databases in accordance with the law, in particular, the Law of Georgia on Personal Data Protection. Only a verbal agreement between the parties or a written memorandum does not constitute a proper precondition for data processing. Existence of clear legal regulation is particularly important in case when citizens' rights, such as right to employment, are limited as a result of data processing.

In 2015, a citizen applied to Personal Data Protection Inspector; the citizen stated that in 2014 he/she was subjected to voluntary drug test at one of the structural units of the Ministry of Internal Affairs of Georgia and the test showed that he/she had consumed drugs. In this regard, the Administrative Protocol was drawn and sent to the court. During the proceedings, the citizen presented the evidence that he/she lawfully consumed drug preparation – by doctor's prescription. Due to absence of the fact of the offence, the court made the decision to terminate the case. Despite the fact that the court did not establish the fact of administrative misdemeanor, the complainant's name was still kept in relevant drug record information database of the Ministry of Internal Affairs of Georgia and of the LEPL the L. Samkharauli National Forensics Bureau. The complainant stated that such record endangered his/her employment and requested the Inspector to ensure that the inaccurate information was deleted.

During examination of the complaint it was established that current legislation requires registration of only those persons, who have drug addiction or are non-medical consumers of narcotics. The applicant belonged to neither of these categories.

In addition, current legislation does not envisage the possibility or obligation of the Ministry of Internal Affairs of Georgia and other public or private institution to provide information to the drug record information database of LEPL L. Samkharauli National Forensics Bureau. Keeping such records is the obligation of the institution authorized by the Ministry of Labor, Health and Social Affairs of Georgia; such institution is authorized to maintain the Unified Information Bank for drug-addicted persons and consumers of substances under special control in accordance with Article 36 of the Law of Georgia on Narcotic Drugs, Psychotropic Substances and Precursors, and Drug Assistance; though, as of today there is no such institution with the above authorization defined. During inspection it was also established that in 2010, narcological database of the Ministry of Internal Affairs of Georgia and the drug registration information database of the National Forensics Bureau were stored in one server on the basis of the verbal agreement of the heads of both organizations; these data were made readily accessible to members of both organizations, without the issue being regulated by legislative or normative act.

Thus, disclosure of the complainant's data by the Ministry of Internal Affairs of Georgia to LEPL L. Samkharauli National Forensics Bureau and the complainant was registered by the Bureau in information database without proper legal grounds for processing. Due to the above-said, the organizations were imposed an administrative sanction –fine. Also, the Ministry was tasked to terminate provision of the information about the complainant to LEPL L. Samkharauli National Forensics Bureau; LEPL L. Samkharauli National Forensics Bureau was tasked to delete incorrect information from its database. It is worth mentioning that the organizations disagreed with the Inspector's decision and appealed it at court. The court (case N4/504715) fully shared the Inspector's position and upheld her decision.

DISCLOSURE OF PERSONAL DATA

DISCLOSURE OF PERSONAL DATA

"*Every citizen of Georgia shall have the right to become acquainted, in accordance with a procedure prescribed by law, with the information about him/her stored in state institutions as well as official documents existing there unless they contain state, professional or commercial secret. The information existing on official papers pertaining to individual's health, his/her finances or other private matters, shall not be accessible to anyone without the consent of the individual in question except in the cases determined by law, when it is necessary for ensuring the state security or public safety, for the protection of health, rights and freedoms of others".*

The Constitution of Georgia, Article 41

The issue of relationship between personal data protection and access to public information was on top of the agenda last year. Number of requests for consultation from public authorities and non-commercial legal entities and practice also showed that requests for public information mostly concern persons' qualification, salary and criminal record.

It must be taken into account that information about person's income or financial status constitutes personal data. Though, information about public officials, due to high public interest towards their performance and due to principles of transparency, is more open and accessible than information about other persons. In accordance with the General Administrative Code of Georgia, public body is obliged not to disclose personal data (without the consent of an individual or in cases prescribed by the law – without reasoned court decision), with exception of public officials' (and of candidates' nominated to such positons) personal data. Therefore, the General Administrative Code of Georgia allows for publication and disclosure of information to interested individuals on public officials, including their salaries and amount of bonuses.

It is important that data controllers demonstrate particular caution with regards to publication of special category of data, which fall under different legal regulation. Publication of sensitive data requires written consent of an individual and the administrative body is obliged to protect such information from disclosure until such person expresses will of disclosing the information.

It must also be mentioned that despite high public interest, current legislation does not envisage the possibility of disclosing special category of data, such as medical record of public officials, without their consent. As per Article 6 (3) of the Law of Georgia on Personal Data Protection, in the course of the processing special category of data, publication of data or its disclosure to a third party without the consent of a data subject shall be prohibited. Though, legislation allows for disclosure of the information containing personal data if such information is depersonalized. Data depersonalization should be done in a way that makes it impossible to link them with a data subject, or would require disproportionately huge efforts, costs and time to establish such a link.

Because of high interest towards the issue, the Office of the Public Defender (Ombudsman) of Georgia and the Office of Personal Data Protection Inspector commenced working on joint recommendations. By the Inspector's initiative, in December 2015 a working meeting was held regarding protection of personal data in court system. The meeting was attended by the judges of the Supreme, Appellate and City courts of Georgia, and court staff members responsible for issuing public information. The meeting addressed the issue of balance between access to public information and protection of personal data, as well as promulgation and publication of court decisions; the need for regulations for publication of court decision became very much obvious at the meeting. Starting from January 2016, with the initiative of the Supreme Court of Georgia, a special working group was established for the purpose of developing the rules of publication of court decisions; the working group includes members of the Inspector's Office.

It must be mentioned that in case if different standard is introduced for publication of court decisions, the need for legislative amendments might arise. With regards to the issue of publication of court decisions, the balance between access to information and the interests of personal data protection must be kept.

In accordance with Article 28 of the General Administrative Code of Georgia, "Public information shall be open except as provided by law and considered as personal data, state or commercial secrets".

The procedure of case examination by the common courts of Georgia is comprehensively regulated by current legislation. In accordance with the Organic Law of Georgia on Common Courts, every case in court shall be tried at an open session, except as provided by law;

a court decision shall be pronounced publicly in every case. In addition, law allows for audio and video recording of the trial. In accordance with Article 3 of the Law of Georgia on Personal Data Protection, - this law shall not apply to processing of data for court proceedings – as it may damage the proceeding itself before the final decision of the court is rendered. In light of the above-said, it is obvious that personal data protection regulations do not apply to court proceedings. Though, once the final decision is announced, the purpose of the court proceedings is accomplished and data controllers, including courts, are obliged to comply with relevant standards of data processing.

In accordance with Article 2 (a) of the Law of Georgia on Personal Data Protection, court decision, which contains data on an individual, represents the document containing personal data; those court decisions which contain information about individual's racial or ethnic affiliation, political affiliation, religious or philosophic beliefs, membership in trade unions, health record, sexual life, criminal record, administrative detention, putting a person under restraint, plea agreements, diversion, granting the status of victim, also contain special category of data.

In accordance with current legislation, in order to uphold important public interest, and also protect legal interests of a data controller or third party (and in other cases established by Article 5 of the Law of Georgia on Personal Data Protection), publication of a court decision is allowed only in case if it does not contain special category of data. Publication of court decisions containing special category of data is only allowed upon depersonalization or by data subject's consent.

Attention should be paid to the form of depersonalization of personal data. In accordance with the Law of Georgia on Personal Data Protection, depersonalization of data is defined as a type of modification of data that would make it impossible to link them with a data subject, or would require disproportionately huge efforts, costs and time to establish such a link. Same approach is adopted by the Court of Justice of the European Union in case *Nikolaou V Commission of 12.09.2007*. The court defines that publication of information that does not indicate to a person, though easily allows for his/her identification, should be considered as processing of personal data.

During the reporting period a citizen applied to the Inspector; the citizen stated that during court dispute he/she found out that the opponent had knowledge of his/her past convic-

tion. The citizen requested the Personal Data Protection Inspector to study the lawfulness of collecting and processing data related to his/her conviction. Another citizen applied to the Inspector's Office with a similar request, and stated that one of the non-governmental organizations disseminated information as if he/she was convicted for particularly grave crime. As a proof, the copy of a court judgement was referred to. Despite the fact that personal data in the court judgement were encrypted, non-governmental organization was convinced that the judgement related to commission of a crime by the complainant. The complainant indicated that he/she had no past conviction and that the judgement published by the Tbilisi City Court referred to other person; the facts stated by the organization were not accurate and aimed at discrediting the complainant.

Examination of the issue revealed that in both cases the court issued a copy of the judgment as public information, without personal data, in an encrypted form, by indicating only the initials. Despite encryption of the information, it is important to point out that in cases under examination the court was requested the copies of judgements on specific individuals (with indication of their first and last names) and the court issued the information about the persons mentioned in the request. Thus, just a mere fact that the name of the data subject was encrypted in the judgement, was not sufficient to consider the case as issuance of information in a depersonalized form. In the above-mentioned cases the recipient of the information could easily, without extraordinary effort, link the initials mentioned in the judgement to an individual and identify him/her. The court did not assess whether the form they choose to issue the judgment allowed for identification of the person. Thus, by the Inspector's decision it was established that the case involved disclosure of special category of personal data in violation of the law.

Disclosure of Special Category of Data of Students by the School

A non-commercial legal entity addressed the Personal Data Protection Inspector and stated that they applied to one of the public schools and requested public information for protection of the rights of persons with disabilities, for ensuring facilitation of their teaching on environmental issues and assessment of their educational needs in the above-mentioned measures. Despite the fact that the legal entity did not request information containing personal data, the information received from the school contained students' personal information; in particular, it included individual learning

plans for students with disabilities, which together with the information on learning process contained information about health-related issues of students, their names, grade, names of their parents and teachers.

On the basis of the received information the public school was subjected to inspection. Inspection revealed that before the information was issued, the school administration informed the parents about the request for students' individual learning plans; the parents were asked if they agreed to issue students' health information on which the parents provided their written consent.

Despite the fact that there were legal grounds for data processing, the inspection revealed that the school insufficiently studied the legitimate purpose, which was intended to be achieved by obtaining the identification information of students by the recipient. Request for public information, submitted to schools aimed at provision of environmental learning support, and identification of assessment measures for educational needs of students with disabilities for which provision of information without identification of students with disabilities would suffice.

The Law of Georgia on Personal Data Protection provides high standards of protection of health-related information as a special category of data and states that processing of such data is prohibited unless relevant exceptions directly envisaged by the same law apply. As the risk of moral damage is high, processing of health related information, and particularly its issuance or making it otherwise accessible, requires legal grounds as well as legitimate purpose. When the case concerns issuance of health data of a juvenile, special attention must be paid to the assessment of risks related to further usage of such information.

Each time such information is issued, legitimate purpose for the attainment of which information is provided must be examined pursuant to Article 4 (c) of the Law of Georgia on Personal Data Protection. Also, data can only be issued in amount that is necessary for achieving specific purpose. Therefore, the school was supposed to depersonalize the data and issue it in a form that would not allow identification of students. As issuance of information containing students' personal data violated Article 4 (c) of the Law of Georgia on Personal Data Protection, the public school was imposed administrative liability in terms of warning.

Data must be processed:

OVERSIGHT OVER COVERT INVESTIGATIVE ACTIVITIES

OVERSIGHT OVER COVERT INVESTIGATIVE ACTIVITIES

"Everyone's private life, place of personal activity, personal records, correspondence, communication by telephone or other technical means, as well as messages received through technical means shall be inviolable. Restriction of the aforementioned rights shall be permissible by a court decision or also without such decision in the case of the urgent necessity provided for by law.

No one shall have the right to enter the house and other possessions against the will of possessors, or conduct search unless there is a court decision or the urgent necessity provided for by law".

The Constitution of Georgia, Article 20

The authority of investigative and operative agencies to intervene into persons' privacy for the purposes of criminal investigation, crime prevention or state security, is internationally recognized standard; though, such authority should be subject to strict regulation and intervention into person's privacy should be proportionate to the legitimate purpose. In accordance with the Criminal Procedure Code of Georgia, covert investigative activity must be based on urgent public need and should be an appropriate and proportionate measure to achieve legitimate purpose. In addition, scope (intensity) of covert investigative activity should be proportionate to legitimate aim.

As per Articles 136, 137, 138 and 143[1] of the Criminal Procedure Code of Georgia, in order to obtain wiretapping records, data stored in computer systems or data storage devices, internet traffic data, or other content for the purpose of criminal proceedings, it is necessary to have a judicial warrant or prosecutor's resolution in case of emergency. Principles under Article 143[2] of the Code aim at keeping fair balance between the State's interest to respond to crime and inviolability of individual's privacy.

By virtue of the legislative amendments enacted in 2014, the Law of Georgia on Personal Data Protection became applicable to the automatic processing of data for the purposes of crime prevention, investigation, operative-investigational activities and protection of public order regarded as state secret; the Personal Data Protection Inspector became authorized to control covert investigative activities and activities in data banks of authorized bodies. By virtue of the legislative amendments in force since March 31, 2015 the Personal Data Protection Inspector became authorized to carry out oversight over the investigative activities under Articles 136-138, and Article 143^1 (1, subparagraphs „a" and „b") of the Criminal Procedure Code of Georgia. Therefore, the Report includes Inspector's activities for 9 months regarding covert investigative actions.

In order to effectively exercise the authority granted by the law, the Law Enforcement Oversight Unit was established at the Inspector's Office. The key functions of the Unit include: to ensure efficient monitoring over covert investigational activities and activities carried out in data banks by authorized bodies; to analyze information provided by the court, prosecution and electronic communication companies; to inspect the legitimacy of data processing by the law enforcement bodies, etc.

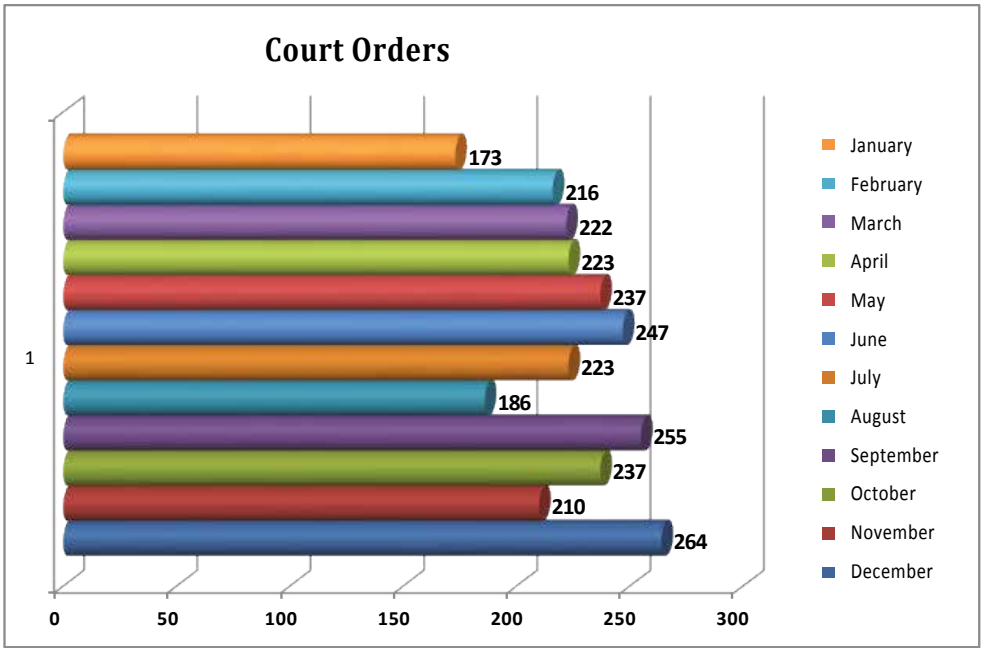
Starting from March 31,2015, a two-stage electronic monitoring system over covert investigative activities – wiretapping has been launched; the list of possible incidents has been defined and the escalation matrix and response mechanisms have been developed. In order to ensure oversight by means of two-stage electronic system, IT Department of the Inspector's Office moved to 24-hour operational mode; IT Department ensures technical monitoring and management of two-stage electronic system and local information systems. Before wiretapping and recording of telephone calls, existence of a court order/prosecutor's resolution is checked and compliance of the data in such a court order/prosecutor's resolution to the electronically initiated request by the Operative-Technical Department of the State Security Service is verified. Legal interception system is allowed to open the requested channel and conduct wiretapping only if all data match. In addition, time limit for covert investigative activity, which targets specific telephone numbers, is under strict

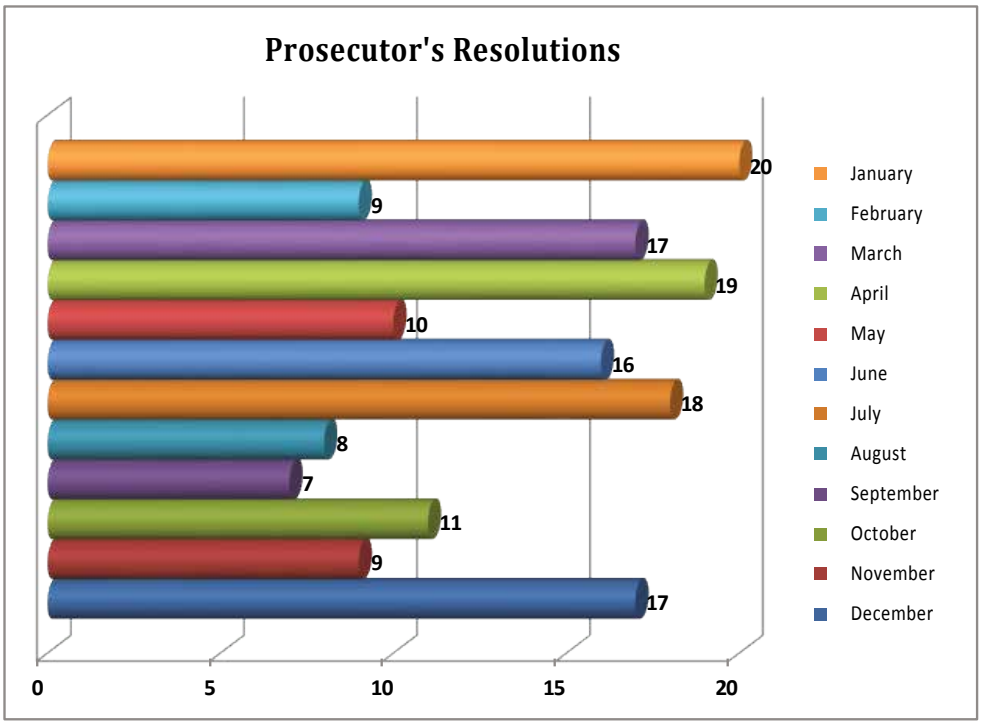
control. If Operative-Technical Department of the State Security Service fails to terminate wiretapping upon expiry of the time limit defined by the court order/prosecutor's resolution, the Inspector closes the channel by means of the electronic system and terminates wiretapping.

Pursuant to Article 35^1 (4) of the Law of Georgia on Personal Data Protection, the Personal Data Protection Inspector conducts monitoring of operations performed within the data bank of an authorized body through a special data bank electronic control system and the inspection of the lawfulness of data processing by a data controller/a data processor.In consideration of the fact that synergy of technical and program solutions for data bank electronic control system is not yet finalized and in 2015 Operative-Technical Department of the State Security Service did not automatically submit data on activity logs in databanks to the Inspector, to fulfill an oversight function envisaged by the law, the Inspector launched inspection of Operative-Technical Department of the State Security Service in November of 2015 in order to examine lawfulness of the activities carried out in databanks.

The Inspector's Office regularly conducts statistical and content analysis of received court orders and prosecutor's resolutions.

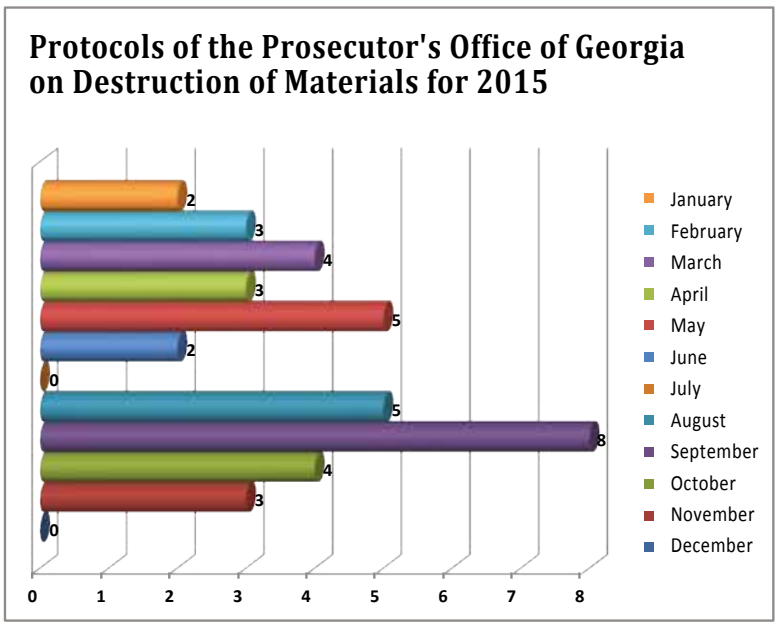
During the reporting period, analysis revealed that from statistical viewpoint, motions requesting document or information on the basis of Article 136 of the Criminal Procedure Code of Georgia are most frequently satisfied. Most rare are the rulings/decisions related to postal-telegraph transfer control and current cellection of internet traffic data.


Court Orders
1
173
216
222
223
237
247
223
186
255
237
210
264
0
50
100
150
200
250
300
January
February
March
April
May
June
July
August
September
October
November
December


Prosecutor's Resolutions
20
9
17
19
10
16
18
8
7
11
9
17
0
5
10
15
20
January
February
March
April
May
June
July
August
September
October
November
December

Certain discrepancies have been identified in small part of court orders on covert investigative activities in 2014-2015. In particular, in some cases court orders did not include time limits for covert investigative activities or there was discrepancy in the data of the subject of covert investigative measure or implementing agency. In case of prolongation of the time limit of covert investigative measure, specific time limit was not indicated. As per the data from 9 months of 2015, due to the above reasons, on average in four cases per month the Inspector's consent was not obtained on opening the channel and wiretapping.

In order to register the protocols on finding the covert investigative activity illegal and on destruction of obtained materials, the Inspector's Office developed technical architecture and established an electronic database, which is used to store, compare and analyze the court orders on finding the covert investigative activity illegal and prosecutor's protocols on destruction of obtained materials.



In 2015, 26 cases have been identified, when protocols on destruction of materials obtained on the basis of investigative activity, which were found illegal, were not provided in a timely manner. Upon Inspector's request, the Chief Prosecutor's Office provided necessary documentation. Several consultation meetings were held and the Chief Prosecutor's Office was recommended to provide protocols on destruction of materials obtained on the basis of investigative activity.

The Office of Personal Data Protection Inspector separately analyzes the information regarding transfer of electronic communication identification data (when transfer does not occur by technical means of real time transfer), which is handed over from electronic communication companies to law enforcement bodies. In accordance with the law, electronic communication companies must inform the Personal Data Protection Inspector within 24 hours from the moment of information transfer to law enforcement agencies. In the beginning of 2015, several consultation meetings with electronic communication companies were held and a common standard form and procedure for submission of information to the Inspector's Office was established.

Processing of Electronic Communication Identification Data by the Law Enforcement Agencies for the Purposes of Investigation and Operative-Investigative Measures

Besides oversight over covert investigative activities, the Inspector monitors personal data processing by law enforcement agencies. In 2015, one of the biggest challenges was compliance with the principles of electronic identification data processing, identification of grounds and development of relevant procedures by the law enforcement agencies in terms of crime investigation and operative-investigative measures.

In 2015, Law Enforcement Bodies Oversight Unit conducted 20 inspections; 6 of them involved facts of violations identified as a result of registration of covert investigative activities and analysis of information provided by electronic communication companies; in particular, violation of established rules of processing electronic communication identification data by the investigative agencies of the Ministry of Internal Affairs and electronic communication companies.

During the reporting period, territorial bodies of the Ministry of Internal Affairs of Georgia requested electronic identification data, such as telephone number, IMEI code, demographic data of a specific owner of a SIM card of an operating company, IMEI code of a telephone, into which the number was activated and also, besides the specific SIM card, the data on the SIM card, which was activated in illegally misappropriated mobile phone. The Ministry of Internal Affairs of Georgia substantiates the request for information by the general norms of the Criminal Procedures Code of Georgia as well as Article 3 ("a") of the Law of Georgia on Operative and Investigative Activities, according to which the objective of operative-investigative activity is detection, elimination and prevention of crime or other illegal activities and Article 2 ("b") of the same law - "official obtaining of factual data by operative officer or an investigator from forensic, operative-investigative or other data storage source, which have substantial importance for fulfilment of the objectives under Article 3 of this law". In addition, the Ministry explained that IMEI code and the information whether a different SIM card was activated in a particular mobile phone are the identification data for the lost item – electric technical device

– mobile phone and not the person, and therefore such data cannot possibly infringe the rights of persons protected under the Law of Georgia on Personal Data Protection. The Ministry considered that in this case the information referred to the object and not to a particular person; requested information did not contain additional information that would facilitate further identification of a person and therefore, it could not be regarded as a personal data.

As a result of examination of the case, the Personal Data Protection Inspector determined that electronic communication identification data had to be requested from electronic communication company in accordance with the rule established by Article 7 (3) of the Law of Georgia on Operative and Investigative Activities. This implies that the body carrying out operative-investigative activity can obtain electronic communication identification data from the electronic communication company in accordance with the rule established by Chapter XVI[1] of the Criminal Procedure Code of Georgia, by the court order or prosecutor's resolution in the following cases: searching for a missing person; searching for a defendant or a convict for presenting him/her to relevant authority, if he/she avoids the preventive measure or a sentence imposed on him/her; searching for property lost as a result of crime.

Also, the issue of considering IMEI code as a personal data was examined; it was mentioned that in accordance with Article 2 ("a") of the Law of Georgia on Personal Data Protection, personal data (hereinafter 'the data') is any information connected to an identified or identifiable natural person. A person shall be identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural or social features specific to this person. In accordance with Article 2 ("r") of the same law, identification number is a personal identification number or any other identification number defined by law, which is connected to a natural person and may be used to retrieve data from the filing system (where the identification number is also processed) or to disclose them. In accordance with the Law of Georgia on Operative and Investigative Activities and Law of Georgia on Electronic Communication, IMEI code is identification data of electronic communication, namely, it is data that is required for identification of user's (including natural person's) communica-

tion device or possible device. Therefore, IMEI code is an identification number envisaged by law, which is connected to an identified or identifiable natural person. In addition, the Law of Georgia on Operative and Investigative Activities and the Criminal Procedure Code of Georgia stipulates legal possibilities and mechanisms of identification of a natural person by means of IMEI code by the body carrying out operative-investigative activity as well as the body carrying out criminal proceedings, which means that the above-mentioned bodies can indirectly identify the natural person by means of IMEI code.

Despite the fact that due to expiry of two-month time limit it was impossible to impose administrative sanction in 6 cases of violation identified in 2015, by the Inspector's decision, the Ministry of Internal Affairs of Georgia and Electronic Communication Company were tasked to process electronic communication identification data only in accordance with the rules established by law; Illegal practice of requesting electronic communication identification data on the basis of a letter only has been eradicated.

You have the right

To know

- what type of data are being processed about you, for what purpose and on what ground;
- who processes them and to whom they were issued;

To be interested

- How the data were collected;
- Whether it is obligatory or voluntary to provide information;

To request

- Correction, updating, addition, blocking, deletion or destruction of wrong, inaccurate, outdated data;
- Termination of data processing and withdrawal of your consent;

To appeal

- Unlawful data processing and to apply to the Personal Data Protection Inspector or court.

VIDEO-AUDIO MONITORING

VIDEO-AUDIO MONITORING

Principles and norms of the Law of Georgia on Personal Data Protection establish strict regulatory framework, which is necessary for protection of universally recognized rights and freedoms in a democratic society. In addition, the state is obliged to establish legal mechanisms that ensure high standard of protection of these rights. In light of the above, the legislator authorized a data subject (citizen) to decide himself/herself who to authorize to process personal data, for what purpose and in what amount. Exception to this rule is only allowed in cases prescribed by law, when public and private interests might surpass citizen's interests. Video surveillance constitutes such an exception. It must be noted that video surveillance in public areas differs from other means of data processing, as data processing for high public interest considerations does not depend upon the will of a data subject. Therefore, the law strictly defines the purpose of data processing via video surveillance, such as crime prevention, protection of public order, protection of personal safety and property, protection of juveniles from harmful influences, protection of secret information.

Video surveillance must be used when necessary and not as an additional mechanism of citizens' control. Moreover, in accordance with the law, in case of installation of video surveillance system, all data controllers are obliged to place relevant warning sign in a visible place in order to ensure respect to and protection of citizens' rights through informing them about such processing.

In 2015, the Office of Personal Data Protection Inspector examined legality of data processing via video surveillance in many private or public organizations. As a result of examination, several cases when video surveillance systems had audio recording function were identified; thus, organizations were using audio monitoring in line with video monitoring for different purposes.

Examination of citizens' complaints and conducted inspections in 2015 revealed that video-audio monitoring by different systems was particularly frequent in service domains (retail points, pharmacies, financial organizations). Data obtained as a result of video-audio monitoring were mainly used for improvement of service quality and control of employees.

Pursuant to the Law of Georgia on Personal Data Protection, data may only be processed for specific, clearly defined lawful purposes. It is not allowed to further process data for other purposes incompatible with the primary purpose. The same law clearly defines purposes of video surveillance at workplaces – i.e. protection of person's safety, property and also, secret information; achievement of the above purposes by other means has to be impossible. Use of video recordings for controlling the employees is obviously beyond the scope of purpose of data processing established by law.

In 2015, on the basis of citizens' complaints and requests by different trade unions as well as at its own initiative, the Office of Personal Data Protection Inspector examined legality of video monitoring at 11 organizations; out of this number, additionally audio monitoring was carried out at 6 organizations. Despite the fact that the Law of Georgia on Personal Data Protection clearly and precisely establishes the rule and legitimate purposes of video surveillance in the street, public transport, at outside perimeters of public and private institutions, at the entrance to the buildings and at workplaces, as a result of examination it was established that majority of the organizations use video surveillance recordings for other purposes, which are incompatible with the law.

Retail Sale Networks

During the reporting period, on the basis of Trade Unions' request, the Inspector's Office examined legality of employees' and consumers' personal data processing via video monitoring in network retail points of two large sales companies.

As a result of inspection it was determined that video surveillance system in companies' retail points was installed for the protection of property and personal safety purposes, though video surveillance was also used to control quality of service rendered by the employees.

In the retail points of one of the companies, video cameras installed in the inner perimeter of the facilities were used for permanent video surveillance for the purposes of monitoring quality of service, to control sales personnel and their appearance. In case if an employee failed to fully comply with service standards, he/she would be held responsible. In some cases, video monitoring is used to control time of employees' arrival and departure at from the workplace.

In the retail points of the second company, primary goal of video monitoring was not to control quality of service rendered by the employees. However, if during video surveillance the security officers noticed violation of internal regulations or Code of Conduct by an employee (such as untidy salesman/woman; use of mobile phones while on duty, etc.), such facts would be communicated to the Manager of the facility for further response.

The Inspector considered that established practice of video monitoring by the companies was not compliant with the law, since the law clearly states that the purpose of video surveillance at workplace may only be safety of an individual and property, protection of secret information, which cannot be achieved by other means. Controlling the service rendered by the company employees, timely arrival at workplace and compliance with existing regulations does not constitute legal purpose of video monitoring established by law.

Companies violating the rules of video monitoring were imposed a fine in GEL 500 each; the companies were also instructed to terminate use of video recordings for controlling employees.

Pharmaceutical Networks

Last year, the Inspector's Office became aware of the fact that three pharmaceutical companies carried out video monitoring in their networks as well as audio recording of communication between the customer and the pharmacist. Due to the scale and sensitivity of the issue, at the Inspector's initiative, legality of data processing as a result of video-audio monitoring was examined in all three pharmaceutical companies. As a result of the inspections it was established that video monitoring of internal and external perimeters was carried out for the purposes of protection of property and security. Meanwhile, in total of 365 drugstores through the microphones mounted at the cash desks, recording of communication between the customers and pharmacist for control of service quality was carried out during 24/7.

The fact of obtaining information on customer's health conditions directly or indirectly by pharmacies when purchasing medication, which in itself resulted in higher degree of intervention into customer's privacy, was also taken into consideration.

Despite the fact that pharmaceutical networks had legitimate aim to control quality of service at their networks, the Personal Data Protection Inspector deemed data processing in such a form and scope disproportionate and inadequate to the legitimate purpose. Audio monitoring constituted disproportionate intervention into consumers' privacy and was not complaint with the principle of proportionality stipulated in Article 4 of the Law of Georgia on Personal Data Protection.

By the Inspector's decision, all three companies were imposed a fine in GEL 500 each for administrative offence envisaged by Article 44 of the Law of Georgia on Personal Data Protection; they were instructed to terminate audio monitoring and to destroy all materials. The Inspector's decisions were appealed at the court. The court did not grant the appeals and upheld Inspector's decisions.

Banking Institutions

On the basis of a citizen's complaint, the Personal Data Protection Inspector studied legality of video-audio monitoring carried out by one of the commercial banks. As a result of examination of the circumstances of the case it was established that commercial bank carried out video surveillance for the purposes of security and protection of property, as security and property risks are particularly high due to specifics of banking operations. Video monitoring warning signs were placed at the head office of the company and its branches, at the entrance doors – in compliance with the Law of Georgia on Personal Data Protection.

In addition, the commercial bank was conducting audio recording in case of client's complaint, in order to clarify the details of financial operation between the bank and the client, and to check and verify client's verbal order and information provided to him/her by the bank clerk. Therefore, the commercial bank was conducting audio recording in order to prevent fraud and for inquiry purposes and also, to protect interests of data subjects (employees and clients); in case if employee's error is detected the client is compensated for the incurred loss and in case if wrong information is indicated by the client, it is established that employee acted in good faith.

The Inspector's Office requested information from Data Protection Authorities (DPAs) of different countries and held consultations regarding current practice and legal regula-

tions of audio monitoring of communication between financial institutions and clients. On the basis of the analysis of the information received from European DPAs it was established that international experience is not homogenous. Legality of audio monitoring depends on the purpose of data processing; particular attention is paid to compliance with principles of data processing and providing information to data subjects.

During assessment of proportionality of data processing, the Personal Data Protection Inspector took into consideration the purpose of data processing and volume of processed data. The Inspector deemed that audio monitoring of communication between the employees and clients carried out by the commercial bank was proportionate to the purpose of data processing, as: audio recordings were used only in case of complaints/claims and not for any other purposes; audio recording devices were installed only in those client service areas where clients give verbal orders for financial operations, including cash operations; bank clients and employees had the right to deny audio recording of their conversation; in case of client's complaint/claim, if his/her will about any of the services was expressed orally, there was no alternative way/evidence other than audio recording available to check what information was exchanged between the client and the bank employee. Nevertheless, the bank was instructed to properly inform data subjects regarding the purpose of audio monitoring and right to refuse to such processing.

Results of examination of citizens' complaints and conducted inspections, as well as international practice show that audio recording by any organization does not immediately constitute a violation of law and in some cases resort to such systems is permitted. Legality of audio recording must be assessed on case by case basis, where activities of a data controller, category of processed data and data subject, scope of intervention into privacy and etc. shall be considered.

Assessment of Coverage of Video Monitoring

One of the political organizations addressed the Office of Personal Data Protection Inspector. The organization stated that opposite to the central facade of the building of their political party there was a lighting pole, on which the Ministry of Internal Affairs of Georgia installed high resolution video surveillance camera which has maneuvering, observation and zooming functions. As per the complaint, video surveillance camera

was directed towards the entrance booth in the yard of the Party's central office; as such cameras have maneuvering capability, this camera was observing the working space of the Party's building.

On the basis of received information, inspection of the Ministry of Internal Affairs of Georgia and its authorized body - State Security Service was carried out. Installing photo and video equipment in the streets and on the external perimeter of the building by the Ministry of Internal Affairs of Georgia serves the purposes of public order, in particular: crime prevention; safety of individuals and protection of property; public order; protection of juveniles from harmful influence; traffic safety and other purposes established by law.

Location of video equipment is selected in consideration of traffic incident statistics, intensity of traffic and other threats related to traffic. At the moment of inspection, the Ministry could not provide written justification of the decision regarding installation of the equipment at that particular address.

The Inspector took into account the fact that due to technical parameters and capabilities of the video camera installed at the above address, the coverage of video control could also include different buildings and institutions in addition to the road, including the head office of the political party. Video control over the building and adjacent territory could facilitate direct and/or indirect identification of party members, supporters, office workers and visitors. Thus, direct and/or indirect processing of special category of data, namely information regarding persons' political affiliations, was made possible, which contradicts to the purposes of video surveillance.

In order to avoid disproportionate and inappropriate processing of special category of data and at the same time to ensure fulfilment of legal purpose of data processing – i.e. security, public order and crime prevention – the Ministry of Internal Affairs of Georgia was instructed to adjust the angle of the surveillance camera, its focus and movement trajectory in a way that monitoring did not cover central office of the political party and its entrance, with exception of cases when LEPL ,,112" would receive a call regarding an incident. Also, the Ministry was instructed to assess the need of video monitoring by the camera operating in a test regime and to provide information about such need and final decision to the Inspector.

PROVIDING INFORMATION TO THE DATA SUBJECT

PROVIDING INFORMATION TO THE DATA SUBJECT

Pursuant to Article 41 (1) of the Constitution of Georgia, every citizen of Georgia shall have the right to become acquainted, in accordance with a procedure prescribed by law, with the information about him/her stored in state institutions as well as official documents existing there unless they contain state, professional or commercial secret. Article 21 of the Law of Georgia on Personal Data Protection guarantees the right of data subjects to request information. Citizen has the right to request information regarding processing of his/her data from private or public data controllers; data controller is obliged to provide the following information: which personal data are being processed; the purpose of data processing and the legal grounds for such processing; means of collecting data; to whom his/her personal data were disclosed; and the grounds and purpose of such disclosure. The citizen should be provided with the above information immediately upon request, or within 10 days after the request, if for responding to the information request it is required to retrieve and process information at another institution or structural unit or to consult with either one; to retrieve and process voluminous documents not linked to each other; or to consult with structural unit of a data controller located in another populated place, or with other public agency.

With regard to the personal information kept at public institutions, the law establishes the right of a person to access his/her personal data and to obtain copies of such data for free, except for cases when payment of a fee is required under the legislation of Georgia.

In consideration of number of complaints submitted to the Inspector's Office and requested consultations, citizens' interest regarding their personal data kept by different institutions has significantly increased in 2015. During the reporting period the Inspector's Office examined 11 complaints where citizens requested information about the ways different organizations used to obtain information about them or providing them with copies of their data. The citizens stated that data controllers failed to provide requested information within the time limit established by

law. 6 facts of violation of the rule of informing data subjects were identified in 2015. During examination of one of the complaints, the Inspector found the LEPL Social Service Agency in breach of the law. Also, when examining the complaint regarding alleged violation of the rules of informing data subjects, one of the insurance companies was found in breach of the law. The citizen stated that the representative of an insurance company contacted him/her on his/her mobile phone for several times. The complainant further explained that he/she wanted to know where the insurance company got his/her telephone number and other data, the representative of the company replied that they had access to the databases of one of the mobile communication companies. Later, the complainant addressed the representative of the company via e-mail and requested information about the means of obtaining his/her personal data; in response the data subject was informed that the company used different ways to collect information, including websites and old databases of partner companies.

During examination of the complaint it was identified that information about the source of personal data provided by the insurance company was not accurate – the company obtained complainant's personal data by means of a telephone call made by the complainant in past. Despite the citizen's request to provide him/her with accurate information in writing, the insurance company failed to provide information within the time limit established by law.

in 2015

1215

Consultations were Provided

Consultation Topics

Biometric and special category of data
6 %

Video-audio surveillance
6 %

Access to databases
7%

Publication of / access to data
23%

Data transfer abroad
5%

Data subject's right and data security
9%

Direct marketing
9%

Principles and legal grounds
17%

Filing catalogues
10%

Legality of data processing by law enforcement
6 %

Other
2%

Right to Access to Data Kept at Public Bodies and to Obtain Copies of Such Data

A citizen addressed the Personal Data Protection Inspector and requested examination of the fact of violation of rules regulating provision of information to the data subject on his/her personal data processing. The complainant stated that disciplinary proceedings were initiated against him/her at one of the universities, as a result of which he/she was imposed a disciplinary sanction. The complainant stated that he/she addressed the university in writing and asked for copies of disciplinary case materials, which he/she never received from the university. During the process of examination of the complaint, the complainant received requested documentation 26 days after the request was made.

The university had no precise regulation which would clearly establish rules and time limits for requesting information by a data subject and for responses to such requests by the university.

The Inspector found that in order to protect data subject's rights guaranteed by the Constitution of Georgia and by the Law of Georgia on Personal Data Protection, it is important that data controllers take legal, technical and organizational measures so that the right of a data subject to receive information is effectively realized within reasonable time limits. To this end, data controllers should establish clear procedures for requesting and issuing information and ensure their accessibility. In addition, time limit for receiving information should be reasonable and should ensure balance between the legitimate interest of a person requesting information and ability of a public institution to properly process and issue requested information.

DIRECT MARKETING

DIRECT MARKETING

Like in previous years, majority of citizens' complaints and consultations delivered by the Office related to direct marketing in 2015. Direct marketing via advertising SMSes was paid particular attention to. Compared with the previous year, level of citizens' reporting has significantly increased during the reporting period. In 2015, 41 citizens applied to the Inspector with a request to study facts of violation of direct marketing rules; 21 cases of violation of direct marketing rules have been detected and 19 organizations were imposed a fine in the amount of GEL 3000.

In 2015, majority of direct marketing organizations implemented the opt-out mechanism which allows the recipient of the SMSes to send given text to a specific number and thus, refuse processing of his/her personal data for direct marketing purposes. The data of one of the advertising companies can be used as an example of implementation of such mechanism in practice and its effectiveness, according to which 311 962 subscribers used the opt-out mechanism.

Violations identified in 2015 mainly involved absence of opt-out mechanism from direct marketing or malfunctioning of such a mechanism. In some cases, companies continued sending advertising messages after 10 working days from the date they received opt-out notice from data subjects. Data controllers, which send advertising SMSes through different data processors, did not take into consideration the possibility of repeating telephone numbers and did not request information from the data processors about those telephone numbers, whose owners already opted out from direct marketing.

In light of current practice, in order to ensure compliance of direct marketing with the law it is important that all organizations carrying out direct marketing establish effective and accessible opt-out mechanism. Also, organizations carrying out direct marketing should monitor data processing by data processors, and should have information about those data subjects who opted-out from direct marketing.

Before citizens' personal data are used for direct marketing purposes, they must be informed in advance about use of their data for such purpose in order to avoid sending spam messages. Citizens should have the right to opt-out from spam SMSes in a way that ensures that they are not denied the service.

In June 2015 the Inspector was informed that LTD "Magticom" sent SMSes to its subscribers and informed them that changes were introduced to standard agreement according to which "subscriber agreed to receive advertising and informational messages from LTD "Magticom" and its partner/contractor organizations". The company also informed the subscribers that they could opt-out from spam SMSes by sending a text with the title of a sender to the relevant number. The Inspector's Office immediately launched examination of the case. It was important to establish whether the subscriber had the possibility to refuse to adhere to such provision of the agreement; or if the subscriber agreed to conditions provided by the agreement, whether he/she could later reject not only a specific offer, but any advertising offers from all "Magticom" partners. After communication with LTD "Magticom", the company took the Inspector's recommendations into consideration and provided subscribers with the opportunity to opt-out from all "Magticom" advertisements by sending a message to number *182#.

Use of Internet Links to Opt-out from Spam SMSes

As a result of examination of citizens' complaints, it was determined that in most cases the opt-out mechanism from spam SMSes was an internet link provided in the text message, which was not assessed as adequate and easily accessible measure by the Inspector.

In this regard, attention shall be paid to the Inspector's decision by which she found one of the companies in breach of the law. According to the decision, when sending the text message to the citizen, the company violated the Law of Georgia on Personal Data Protection, as the opt-out mechanism from direct marketing was the webpage of the company. Reference to the internet link was not deemed to be accessible and adequate means for terminating data

processing for direct marketing purposes in circumstances when owners of telephone numbers could have no access to internet. The court shared the Inspector's position and stated that indication to the website in the SMS was insufficient to realize a right granted to the data subject by the provision regulating such relationships; the website was not evaluated as an easily accessible mechanism to request to terminate use of personal data for direct marketing purposes.

Furthermore, it must be noted that in accordance with the information received from mobile phone operators (LTD „Magticom", LTD „Geocell", LTD „Mobitel"), number of subscribers registered in their network significantly exceeds the number of subscribers with mobile internet. In 2015, out of 4 949 535 subscribers, only 1 766 313 were using mobile internet. Therefore, the opt-out mechanism that requires access to internet cannot be deemed as an adequate and accessible measure.

When assessing accessibility and adequacy of the opt-out mechanism from direct marketing, its cost shall also be taken into account. In case the cost of the opt-out mechanism is higher than standard cost of the short text message established by mobile operators, it shall not be deemed as an accessible and adequate measure.

Direct Marketing via E-mail and Other Forms of Telecommunication

Besides an SMS, companies often use e-mail and other forms of telecommunication for offering their goods or services. When carrying out direct marketing, organizations shall take into account that rules related to direct marketing set forth in the Law of Georgia on Personal Data Protection equally apply to sending advertisements via e-mail and other forms of communication as to short text messages.

In 2015, the Office of Personal Data Protection Inspector was informed that one of the companies was sending advertising messages through "Viber", an electronic communication program; however, the messages did not provide for

an opt-out mechanism. During inspection the company confirmed the fact of sending advertising messages via "Viber". It was also established that sending advertising messages by "Viber" was a new product of one of the advertising companies. A message included advertising photo of the company, its telephone number and webpage, however it did not provide for an opt-out mechanism.

It is notable that Article 8 of the Law of Georgia on Personal Data Protection obliges the data controller (the goal of which is to send advertising messages) to comply with the rules applicable to direct marketing. Therefore, data controller bears responsibility for violation of these rules. Thus, organization that makes the decision on carrying out direct marketing shall assess the compliance of the service offered by the companies, including the opt-out mechanism from direct marketing, with the law.

DATA TRANSFER TO ANOTHER STATE AND INTERNATIONAL ORGANIZATIONS

PARTICIPATING IN LEGISLATIVE PROCESS

DATA TRANSFER TO ANOTHER STATE AND INTERNATIONAL ORGANIZATIONS

Trans-border flow of personal data still remained important issue in 2015. Bilateral and multilateral cooperation agreements between Georgia and other countries, international activity of Georgian companies, establishment of branches of foreign companies and investment projects provide ground for increased level of trans-border data flow. Many private institutions operating in Georgia transfer data abroad upon the request of foreign shareholders and partners.

It should be mentioned that in 2015, particular attention was paid to transfer of personal data and security of transferred data while concluding international agreements with other states and international organizations. Several public agencies addressed the Inspector's Office for consultations related to international agreements to be concluded and their content. In 2015, the Inspector reviewed and prepared recommendations on 7 draft international agreements submitted by the Ministry of Foreign Affairs of Georgia.

Existence of data protection guarantees in Turkey and three international organizations (the Commonwealth of Independent States, Interpol and Central Asian Regional Information and Coordination Centre for Combating Illicit Trafficking of Narcotic Drugs, Psychotropic Substances and their Precursors (CARICC)) was assessed during 2015.

In 2015, the Office of Personal Data Protection Inspector received 5 applications for permission to trans-border data flows in line with data protection legislation, 3 applications were submitted by the Ministry of Internal Affairs of Georgia.

PARTICIPATING IN LEGISLATIVE PROCESS

Significant data protection reform is ongoing within the European Union and Council of Europe in response to the challenges of the modern world. Namely, the European Union works on General Data Protection Regulation and on the Directive related to Protection of Personal Data in Police and Criminal Justice Sectors. The Council of Europe is working on modernization of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. These documents set common standard of data protection and establish effective mechanisms to protect data and enforce data protection legislation.

As party to the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and to Association Agreement with the European Union, Georgia undertook international obligations to ensure high level of data protection in compliance with European standards. Draft legislative amendments elaborated by the Inspector's Office are aiming to fulfill above mentioned obligations; prepared amendments will harmonize Georgian data protection legislation with European Union and Council of Europe new regulations.

The legislative amendments foresee application of data protection law to automatic processing of personal data for purposes of crime prevention, investigation, operative-investigative activities and protection of public order regarded as a state secret, as well as to semi-automatic and manual processing of such data. Additional grounds for processing of special category of data such as state of health if it is necessary for protection of legal interests of a person with disability, a person receiving support or socially vulnerable person, processing of sensitive data in cases which are directly prescribed by the Georgian Law on Official Statistics, for the purpose of functioning common analytical system of migration data, by archive fund and the archive established on the basis of law are envisaged by the proposal.

It should be stressed, that according to the amendments audio recording will fall under special regulation. The issue is important in circumstances when such type

of data processing constitutes a common practice. The legislative amendments prepared by the Inspector's Office also relate to direct marketing. The idea to create a unified web portal, which will allow citizens to use one-stop shop to opt out from undesirable advertising messages selectively, is proposed.

For promotion of lawful data processing and prevention of possible violations, the legislative proposal foresees possibility of voluntary inspection of data controllers and data processors. Legislative amendments foresee significant changes to the rules regulating examination of data subject's complaints and conducting inspections. Procedures of inspection, conditions for initiation, suspension and termination of the proceedings are improved; rights and obligations of the parties participating in the case proceedings and ways of collection of evidence are specified. Besides, legislative amendments aim to establish effective mechanisms for enforcement of Inspector's decisions that is an important step for development of the data protection sphere and implementation of European standards. Proposals also include amendments to the Code of Georgia on Administrative Offences. As two-month limitation period for imposition of administrative liability significantly hampers the ability of the Inspector to adequately respond to offences, increase of the time limit up to one year is recommended. Besides, taking into account European practice, draft legislative proposal includes stricter responsibility for large-scale data breaches (concerning more than 100 data subjects).

The draft legal amendments were brought to discussion with the representatives of the Parliament of Georgia, different Ministries, Legal Entities of Public Law, private sector, international and non-government organizations in September, 2015. Their opinion was taken into account and reflected in the final draft document; currently the document undergoes legal expertise by the experts of the Council of Europe.

In 2015 the Inspector's Office fruitfully cooperated with different committees of the Parliament of Georgia, such as Human Rights and Civil Integration Committee, Legal Committee, and other sector specific committees. Expert opinions and recommendations were provided to relevant committees in order to improve legislation. Within the scope of consultations and legal expertise, in order to ensure compliance with personal data protection legislation, orders of the Government

of Georgia, different draft legal acts prepared by the Ministries and Legal Entities of Public Law, agreements and memorandums related to data processing were examined.

The Inspector's Office revised the draft Ordinance of the Government of Georgia on Adoption of the Rule of Provision of Relevant Equipment/Devices to Socially Vulnerable Population in relation to Transition to Digital Overground Broadcasting, and also the draft Law of Georgia on Enforcement of Noncustodial Penalties and Probation from the perspective of compliance with personal data protection legislation. According to the draft law, National Probation Agency and its territorial units were authorized to process special category of data and biometric data of the convicted persons; for this purpose, they were authorized to have direct access to data generated through automatic and semi-automatic means by state and non-governmental institutions. The Inspector's Office found it appropriate to define special purpose of processing of special categories of data and to specify databases to which direct access had to be provided.

The Office of Personal Data Protection Inspector revised different issues of legislative regulation related to access to database of LEPL State Services Development Agency; for instance:

1. The draft Ordinance of the Government of Autonomous Republic of Abkhazia, according to which IDP Settlement and Social Protection Unit under the IDP Issues Department of Autonomous Republic of Abkhazia was granted authority to request personal data kept at the Legal Entity of Public Law – State Service Development Agency under the Ministry of Justice of Georgia, for the purpose of creating unified database for IDPs and vulnerable categories;

2. Draft Ordinance of the Government of Georgia on Approval of the Statute of the Ministry of Finance of Georgia;

3. Draft Ordinance of the Government of Georgia regarding approval of the state program on Internship Rules and Conditions in Public Bodies.

Structural and procedural changes made in order to ensure institutional development and increased effectiveness of the Inspector's Office during the reporting period should also be underlined. Statute of the Office of Personal Data Protection Inspector was renewed; Employees' Code of Ethics, which sets norms and standards of conduct, was prepared; issues of employees' conflict of interests, relations with third parties and protection of confidential information were regulated.

The rule of inspection of the legality of data processing in public and private institutions was developed and approved; it regulates principles, purposes and basic procedures of inspection of the legitimacy of data processing by data controller or data processor.

Every Act in Internet Leaves Trace!

RAISING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES

INTERNATIONAL AND BILATERAL COOPERATION

RAISING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES

Since Personal Data Protection Inspector presented the annual report for 2014 at the Parliament of Georgia, the legislative body adopted a resolution to increase quality, effectiveness and accessibility of the Personal Data Protection Inspector; the resolution included a recommendation regarding promotion of visibility of the Inspector's Office and raising citizens' awareness on their right to personal data protection. Raising public awareness on personal data protection related issues has been one of the priorities of the Inspector's Office since its establishment. As a result of the Parliament's recommendation, its importance was once again outlined.

In order to implement personal data protection standards in Georgia participation and taking of interest in the process by every citizen is particularly important. This can only be ensured when public is properly informed. Therefore, public awareness campaign in 2015 paid significant attention to cooperation with media and informing journalists about the Inspector's activities and personal data protection regulations. To this end, training for media representatives was carried out, which facilitated the increase of media interest towards the Office of Personal Data Protection Inspector. The Inspector and representatives of her Office always made a use of the time allocated to them by the media to provide public with the information they need and are interested in.

Different printed materials prepared during 2015 served the purpose of raising awareness on personal data protection. Such materials included booklet on data subjects' rights, bilingual poster on personal data processing at border-crossing, which was placed at checkpoints of Tbilisi, Batumi and Kutaisi airports.

The Office prepared a Public Service Announcement, which was being aired for several months by 24 central and regional TV channels. As a result of the advertisement, awareness of the Office significantly increased, which had impact on the growth of citizens' reporting level.

Special attention was paid to the juveniles and students in the awareness campaign. In 2015, 9 public lectures for students were held in Tbilisi and regions; 12 informational meetings were held with the representatives of private and public sector and civil society organizations in big cities of Georgia: Gori, Telavi, Kutaisi and Batumi. Consultation meetings were held with representatives of the Government Administration of the Autonomous Republic of Adjara, Ministries of Education, Culture and Sport, Health and Social Affairs, and representatives of Tbilisi, Batumi and Kutaisi Assemblies and Municipalities.

In cooperation with Public Service Halls and Public Centers, International Data Protection Day was celebrated nationwide on January 28, 2015; the Inspector's Office participated in the event dedicated to Independence Day of Georgia on May 26 and provided thousands of citizens with information about importance of personal data protection and ways to address the Inspector.

Information on the activities of the Office of Personal Data Protection Inspector is disseminated via the website and different social networks. In order to make all news regarding personal data protection available, and to raise public awareness on the activities of the Inspector's Office, the Office web portal www.personaldata.ge is used quite actively. In 2015, number of webpage visitors has doubled, and number of social media users has tripled. The official webpage also gained the consulting function. Data controllers and citizens have the possibility to receive responses regarding the subject of their interest online. Decisions of the Personal Data Protection Inspector were made publicly available on the webpage, without identifying individuals. In 2015, electronic register of filing system catalogues has also been introduced; on the one hand it allows organizations to electronically update the catalogues, and on the other hand it gives the possibility to interested persons to check what type of data are being processed by public and private organizations.

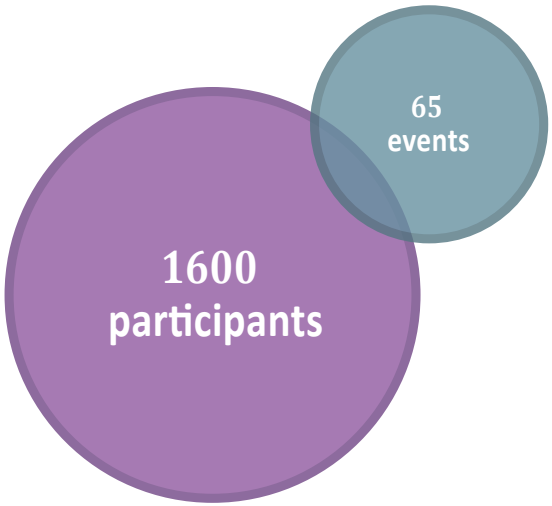
Photo/video/poster competition announced by the Inspector's Office also served the purpose of raising public awareness; more than 60 individuals participated in this contest.

The Inspector's Office participated in different forums and conferences, including VIII Regional Conference on Georgia's Cyber Security and Information Technology Development and Internet Freedom Forum.

During the reporting period, the Inspector made several public statements regarding privacy, which have become subject to public discussion and investigation in 2015. Among these issues following shall be highlighted: dissemination of information related to privacy of Late Prime Minister Zurab Zhvania and Raul Usupov; statement of journalist Eka Mishveladze; also dissemination of audio recordings of communication posted on Ukrainian website as well as videos of facts of torture and inhuman treatment. In order to protect rights and dignity of victims of torture and their family members and to protect juveniles from harmful influence, the Inspector addressed the Ministry of Internal Affairs of Georgia and electronic communication service providers with a specific recommendation and called them to discuss possibility of limiting access to those foreign internet resources, where the above videos were posted. The Inspector also addressed media outlets, organizations and citizens to refrain from further distribution of videos of torture, especially in public and internet domains. The Inspector offered legal consultation to journalist Eka Mishveladze and the member of Tbilisi Assembly Aleko Elisashvili with regards to their public statements on illegal surveillance.

In order to implement legislation in practice and to raise data protection standards, educational activities undertaken by the Inspector's Office carry particular importance; such activities include trainings for the employees of public and private organizations. During 2015, 49 trainings were conducted, covering up to 1300 employees of Ministries of Finance, Defense, Environment and Natural Resources, Internal Affairs, Prosecution, Public Service Hall and other institutions and 172 representatives of private organizations. Important achievement of 2015 is increased access to trainings, not only in the capital, but also in the regions. The Office introduced a new training module; by online registration, representatives of small and medium businesses, local self-governments, Legal Entities of Public Law and interested individuals can participate in such trainings.

Trainings and Public Lectures



In 2015 several organizations were added to the list of educational organizations that are partners of the Personal Data Protection Inspector. These include: Penitentiary and Probation Training Center, Dental Clinic Management School, NIMD School of Democracy and Legal Education Support Fund. Intense cooperation was launched with the Parliament of Georgia, Tbilisi Municipal Assembly, Tbilisi City Hall and Non-commercial Legal Entity Kindergarten Management Agency for organizing trainings on data protection.

In order to implement proper practice of personal data protection, the Office continued working on thematic recommendations; recommendations issued in 2015 relate to processing of biometric data and protection of personal data on the internet.

INTERNATIONAL AND BILATERAL COOPERATION

The Office of Personal Data Protection Inspector actively participates in the process of implementation of National Action Plan for Georgia-EU Association Agenda and Georgia-EU Visa Liberalization Action Plan.

In 2015 the European Union Assessment Mission studied the mandate of the Personal Data Protection Inspector, the activities of the Office and specifics of its operation in details. As a result, the European Commission positively evaluated the reform of personal data protection and considered the commitments under the Visa Liberalization Action Plan concerning personal data protection to be fulfilled.

Representation of the Office of Personal Data Protection Inspector on international level has significantly increased in 2015; the Office was accredited as a full member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and became a member of Global Privacy Enforcement Network (GPEN).

The Personal Data Protection Inspector and representatives of her Office actively participated in different international meetings and conferences, such as 4th Internet Forum held in Stockholm; 27th working meeting of Data Protection Authorities in Tirana; the European Conference on Data Protection Authorities (Spring Conference) in Manchester; international conference "Population Registration, Personal Data Protection and Right to Privacy" held in Bishkek; 17th meeting of Central and East European Data Protection Authorities (CEEDPA) in Durres, Albania.

The Office of Personal Data Protection Inspector actively participated in plenary meetings of the Consultative Committee of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data; during these plenary meetings, the issues of modernization of Convention 108, the so called large databases, personal data protection in police sector, air transport passenger information, protection of health data, collection of data for the purpose of combating terrorism and automatic data transfer mechanism for taxation purposes have been discussed.

Bilateral cooperation with Data Protection Authorities from different countries has significantly increased in 2015; this includes independent monitoring authorities of Romania, Macedonia, Albania, and Poland. Memorandum of Mutual Cooperation has been signed with the Bureau of Inspector General for the Protection of Personal Data of Poland in Warsaw; this Memorandum aims to deepen the cooperation between the Data Protection Authorities of Poland and Georgia and to carry out joint activities.

During 2015, donor organizations provided increased support to the Inspector's Office. With financial assistance of the Council of Europe, legal expertise of the draft legislative amendments prepared by the Office of Personal Data Protection Inspector is being conducted by the Council of Europe experts. With support of the International Centre for Migration Policy Development (ICMPD) project "ENIGMA", a working meeting dedicated to the issues of personal data protection in court system was held; also, training was delivered to the representatives of media outlets. In order to enhance capacity of the Office of Personal Data Protection Inspector, United Nations Development Program (UNDP) is launching a project funded by the European Union; within the scope of this project the following activities are planned: institutional capacity building of the Office of Personal Data Protection Inspector; elaboration of strategy and action plan; development of technical infrastructure; survey of public awareness about personal data protection and etc.

2015 was the year of recognition of the Office of Personal Data Inspector in many different directions. The Inspector's Office received an award of the Gender Equality Council of the Parliament of Georgia and UNDP for gender balance at executive level; award of the Institute for Development of Freedom of Information for ensuring accessibility to public information; non-government organization "Young Barristers" nominated the Office of Personal Data Inspector as the most open public institution.

OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

7 Vachnadze Str. Tbilisi, Georgia
(+995 32) 242 1000
office@pdp.ge
www.personaldata.ge
FB/DPAGeorgiaOfficial