



**REPORT ON THE STATE OF
PERSONAL DATA PROTECTION
AND ACTIVITIES OF THE INSPECTOR**

2016

**REPORT ON THE STATE
OF PERSONAL DATA
PROTECTION AND ACTIVITIES
OF THE INSPECTOR**

2016



Office of the Personal Data
Protection Inspector

CONTENTS

INTRODUCTION	5
LEGAL GROUNDS AND PRINCIPLES OF DATA PROCESSING	11
DISCLOSURE OF PERSONAL DATA AND ACCESS IN INTERNET	33
OVERSIGHT OVER COVERT INVESTIGATIONAL ACTIVITIES AND PERSONAL DATA PROCESSING BY LAW ENFORCEMENT AGENCIES	49
VIDEO SURVEILLANCE	63
DIRECT MARKETING	71
THE RIGHTS OF DATA SUBJECTS AND ACCESS TO INFORMATION	79
THE INSPECTOR'S PARTICIPATION IN THE LAW-MAKING PROCESS, EDUCATIONAL AND OTHER ACTIVITIES	87

INTRODUCTION

Annual report of the Personal Data Protection Inspector on the state of personal data protection and activities of the Inspector is overview of current trends of personal data protection in Georgia, main courses and challenges of work of the Office of Personal Data Protection Inspector, revealed violations, results of measures taken to respond these violations and other problematic matters.

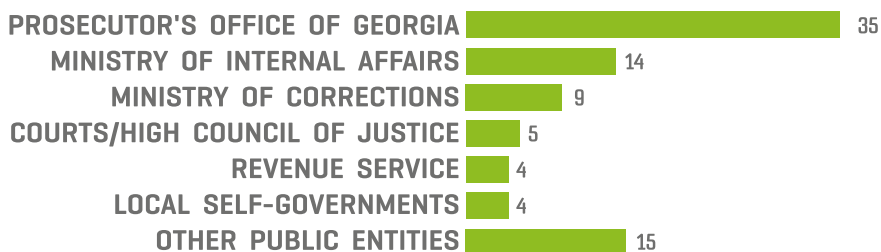
2016 is important in the light of institutional development and strengthening of the Office of Personal Data Protection Inspector, carried out inspections, dealt complaints and increased number of revealed violations.

Comparing to previous years in 2016 the number of consultations provided to citizens, public and private organizations increased three times; the number of citizens' complaints and inspections was also increased two times; 221 facts of violations were revealed; fine was imposed on 63 organizations; while 35 organizations were warned; Several public and private organizations were requested to apply appropriate organizational and technical measures in order to ensure data protection, 202 recommendations were issued for this purpose; in 47 cases the liability was not imposed due to expiration of statute of limitation determined by the law for the administrative liability and 6 cases were transferred to authorized law-enforcement institution due to presence of elements of a crime.

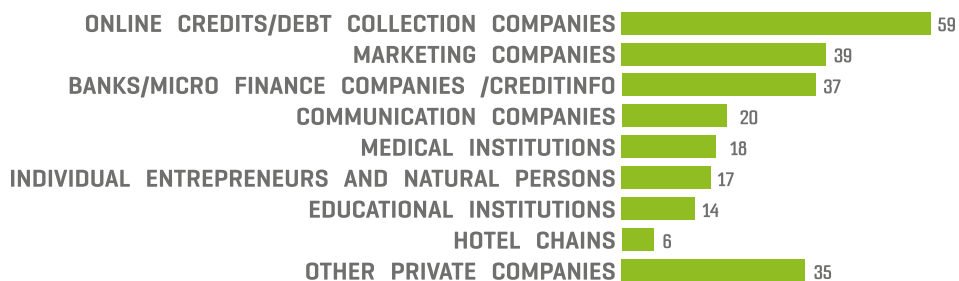
The data processing in the following institutions was examined as a result of submitted complaints and conducted inspection




PUBLIC INSTITUTIONS



PRIVATE INSTITUTIONS





The Institutional Development Strategy of the Inspector's Office for 2017-2021 was prepared with the support of the United Nations Development Program (UNDP) and the European Union; the values, mission, vision, main objectives and two-year action plan were drafted; numerous information and education campaigns and meetings were conducted in order to raise public awareness regarding personal data protection issues.

The Inspector's Office started working on legislative amendments in order to implement the National Action Plan of the Association Agenda between the European Union and Georgia and to bring the national laws in compliance with European standards. Cooperation with the European Police Office (Europol) was strengthened with the involvement of the Inspector's Office. The Office of Personal Data Protection Inspector in cooperation with the Council of Europe started elaboration of the guidelines for media. Main goal of these guidelines is to encourage striking balance while private life of a citizens is covered by media. The Inspector's Office hosted the first conference of the Eastern Partnership Data Protection Authorities. The bilateral cooperation with the data protection authorities of other countries expanded; Furthermore, the interest towards data protection reforms in Georgia is increasing.





LEGAL GROUNDS AND PRINCIPLES OF DATA PROCESSING

LEGAL GROUNDS AND PRINCIPLES OF DATA PROCESSING

In order to strike a fair balance between the right of any person to protect personal data and interests of private or public organizations processing personal data it is necessary to respect the principles determined by the law as well as to ensure existence of legal ground for data processing.

Violation of the principles of data processing still remains one of the most common problems with regard to personal data protection. The majority of organizations inspected in 2016 process inadequate and disproportionate amount of personal data.. The practice of data retention for indefinite period or for inadequately long time is very common. This creates certain obstacles for the citizens in the course of obtaining different services. The facts of negative pressure on children and their family members due to disclosure of incorrect information regarding state of health were revealed.

121 citizens' complaints from 216 complaints dealt by the Inspector in 2016, were related to legal grounds and principles of data processing. Most of these complaints were about the access to financial data and disclosure of loan obligations to the third parties, as well as accessibility of information related to health.

As a result of dealt complaints and conducted inspections 121 cases of processing data without the sufficient legal ground and violation of principles were revealed. Some of organizations were assigned administrative liability, they were either warned or fined and in some cases the liability was not imposed due to expiration of two month statute of limitation from the moment of commission of violation determined



by the law. Notwithstanding to this, organizations were given mandatory recommendations in order to eliminate deficiencies related to the data processing.

Present report represents main violations revealed by the Inspector in 2016; Moreover, concrete examples are given. Analysis and generalization of these examples underlines the importance of data protection.

CREDITINFO DATABASE

The access to credit information was still important in 2016, which is proved by the increased number of consultations and complaints regarding the processing of credit information.

JSC “Creditinfo Georgia” is the organization established by the commercial banks that receives information permanently regarding the financial obligations of natural and legal persons from the entities operating in Georgia and issuing loans. . The database is established based on the received information and access to this database is ensured through the relevant contract and payment of certain fee.

The information regarding the solvency of a person and predicting analysis of future credit behavior is very important for the organizations issuing loans. Monthly, around 3 million searches are made in the database of JSC “**Creditinfo Georgia**” by banks, microfinance organizations, online credit organizations, leasing and insurance companies, aesthetic service providers, construction and distribution companies. Inspector indicated the necessity to introduce legal regulation of work of JSC “**Creditinfo Georgia**” in annual report of 2015 and this issue is still acute in 2016. The importance of legitimacy of data processing in this database is underlined by its volume, database includes information about almost 2 300 000 natural persons.



Citizens in their complaints submitted to the Inspector's Office were mainly doubted legitimacy of access to data stored in the JSC "**Creditinfo Georgia**"; in some cases the subject of investigation was the accuracy of data in the database and the opportunity to delete information regarding the illegal access to data.

The use of database of JSC "**Creditinfo Georgia**" means to receive information not only on the financial obligations of a person, but also access to rating score calculated by the statistical analysis of data (so called "individual blended score"). "Individual blended score" is a scoring model, which predicts future credit behavior, probability of due fulfillment of financial obligation and the risk of default based on complex analysis of person's individual payment behavior, information available on individuals and business linked to them. Almost all organizations examine and take into consideration credit score created by JSC "Creditinfo Georgia."

During reporting period the facts of use of above mentioned database by organizations that are not directly linked to loan services were revealed. Among them were for instance organizations providing cosmetic and aesthetic services. These organizations explain the necessity to access the database by the objective to examine the solvency of a customer. According to their explanation the goods were sold by the "installment payment plan" and it was important to know the credit history of a customer in order to determine relevant financial risks.

The transfer of information regarding the financial obligations by the organization issuing loans to JSC "Creditinfo Georgia" or/and access to credit data by organization is only allowed on the basis of data subject's consent as it is determined by the standard agreement between the parties. Despite this, from the cases investigated by the Inspector facts of checking data without the consent were revealed. It is important to notice, that there is no preliminary determined list of organizations/persons autho-



ized to have access to the database of JSC “Creditinfo Georgia” only in special circumstances. JSC “Creditinfo Georgia” has no ability to double check the existence of legal ground for data processing in each case prior the transfer of data stored in the database. This fact significantly increases the risk of illegal access to data.

It is noteworthy to mentioned that JSC “Creditinfo Georgia” stores not only information about persons with financial debts (“negative history”), but also data of those who fully and properly fulfilled their financial obligations. Number of searches made in their credit history and facts of access to their data make impact on calculating their rating score.

During reporting period citizens applied to the Inspector’s Office in order to prevent negative impact on their credit history and they requested to delete illegally processed data from the database of JSC “Creditinfo Georgia”. After examination of the issue, Inspector concluded that information regarding the access to applicants’ data by different clients were identified and stored in the system of database of JSC “Creditinfo Georgia”. Because of the facts, that illegal access to data were revealed during the examination of complaints, JSC “Creditinfo Georgia”, on the basis of the decision of the Inspector, was requested to delete information regarding the illegal access to data. In addition, JSC “Creditinfo Georgia” was requested to develop and adopt rules on deleting information on illegal access to data on credit history from the database and to ensure the application of appropriate organizational and technical measures for this purpose.

During the reporting period the use of username of certain organization by an unauthorized person was also revealed. In one of the cases examined by the Inspector JSC “Creditinfo Georgia” was requested to determine clearly terms for storage of data and its deletion from database.



In order to protect person from the unauthorized access to credit information it is important:

- *To ensure, that credit issuing organizations access database only in case of existence of legal grounds and appropriate legitimate purpose;*
- *To elaborate appropriate organizational and technical measures in order to minimize risks of unauthorized access to the database by JSC “Creditinfo Georgia”;*
- *To determine the rules of use of database, categories of data and the timeframe of data storage in the legislation; to limit number of persons authorized to have access to database based on necessity and etc.*

DATA PROCESSING BY ONLINE CREDIT ORGANIZATIONS AND PROBLEM LOAN COMPANIES

Such characteristics as the simplicity, accessibility and speed of the process of issuing loans online makes online credits attractable and it is used by more and more people which significantly increases the volume of personal data processing by the online loan companies. Companies mainly collect information about debtors online from the data subjects themselves. Typically, person who wants to take a loan online shall register on the website of a company, fill out electronic application form, provide personal data.(for instance: name, last name, personal ID number, address, contact information and etc.) and shall agree (by ticking the button “I agree”) to terms and conditions of loan agreement determined by the company. In the majority of cases the mandatory and voluntary columns are not identified in the electronic application form; In addition, in a most cases debtor does not get familiar in details with the contract terms and as a result he/she does



not have sufficient information regarding the purpose and volume of use of his/her personal data by a company and what type of problems can be caused with regard to personal data in case of failure to fulfill obligation (contacting employer or family of debtor, disclosure of information regarding the debt without any necessity and etc.)

The vast majority of complaints dealt by the Personal Data Protection Inspector in 2016 are related to the legitimacy of data processing by the online credit organizations and problem loan collection companies. Applicants in the most cases refer to the illegal disclosure of information regarding the financial debts to the third persons (family members, neighbors, friends or/and colleagues) as well as to the compliance of content of loan agreement regulating personal data processing with law.

DISCLOSURE OF INFORMATION ON FINANCIAL DEBTS

Information regarding the financial debt of a natural person (debt, the amount of debt, deadline of payment and etc.) represents personal data and disclosure of these information to a third party is permitted only in a case of existence of legal grounds for disclosure (for instance: consent of a data subject; prevailing legal interests of a third person or data processor and etc.), disclosure of data is necessary for the achievement of concrete legitimate purpose and the volume of disclosed data is in accordance with the condition of legitimate interests. Data processor and especially organizations working in financial sector that possess information related to the financial condition of an individual are obliged to strike a fair balance between their legitimate interests and the right to protect personal data of a debtor. Disclosure of personal data of data subject (including the information regarding the financial debt) shall be directly linked to the protection of legiti-



mate interest of data controller and shall be necessary measure for the achievement of legitimate purpose of the processing.

A citizen applied to the Personal Data Protection Inspector and indicated that one of the online credit companies disclosed the information regarding his/her financial debt to his/her colleagues. It is important to note, that these persons were not indicated by an applicant in the loan agreement as contact persons. In addition the loan agreement determined concrete forms of communication between the parties (telephone number, e-mail and contact to the address) and did not determine the opportunity to transfer the information regarding the financial obligations to the third persons. Notwithstanding to this fact, the company decided to contact with an applicant through third persons and disclosed the information regarding the financial debt to them. Company failed to use any other means of direct communication with an applicant; Furthermore, sharing the information with third persons regarding the financial debt of an applicant was not necessary; Company failed to inform an applicant without disclosing the detailed information regarding his/her financial condition to a third person. The company did not have legal ground for disclosure of information. Violation of article 5 of the Law of Georgia on Personal Data Protection was established by disclosing of data to a third person and administrative liability was imposed on a company in the form of a fine.

The cases of transfer of problem loans by the online credit companies to other companies working on debt collection are very common. In such situations, the personal data of a debtor is transferred to the com-



panies working on debt collection, which is given the authority to act on behalf and for the purpose of organization that issued loan. In such case for the purpose of the Law of Georgia on Personal Data Protection such companies represent the data processor. . In 2016 there were revealed cases when data processors used methods for debt collection and were processing personal data without legal ground, legitimate purpose and necessity. Among them are: visit to the house and work place of debtor and discussion of financial obligations in presence of other persons; attempt to find a debtor by contacting his/her possible acquaintances; direct or indirect sharing of information regarding the financial obligations to the acquaintances of debtor and etc.

Both loan issuing as well as problem loan collection companies are obliged to take into account rules and prohibitions established by the law for the data processing when disclosing personal data. Otherwise the issue of imposition of administrative liability is raised. The facts of unlawful processing of personal data not only violate the rights of data subject but also damage the name and reputation of a company.

As a rule, the loan agreements include standard terms and conditions for processing of debtor's personal data by this terms debtor provides consent for the processing. However, in the majority of cases the terms and conditions of agreement are not clear and are vague for citizens due to general wording of concrete provisions of an agreement. According to the law consent of data subject represents clearly established will of the person after receipt of the respective information, on his/her personal data processing for specific purposes expressed orally, through telecommunication or other appropriate means. ; When drafting the regulatory provisions on processing of personal data of the contract the requirements of the Law of Georgia on Personal Data Protection shall be taken into account not just nominally but in its full content. The con-




tract shall state clearly and obviously the possible volume and extent of data processing, including the cases and forms of transferring information regarding the financial condition to the third persons.

In 2016 in some of the cases examined by the Inspector the terms of the agreement could not be considered to be clearly established will of a debtor to process data for certain purpose and through certain form, due to its incomplete, general or/and broad character. In all such circumstances the companies were given recommendation to determine clearly the concrete purpose and forms of processing of personal data in the contract terms.

In 2016 a citizen applied to the Personal Data Protection Inspector who indicated in application that one of the conditions of loan agreement between him/her and one of the online companies related to the processing of personal data of debtor was violating the requirements of Georgian law on Personal Data Protection. The wording of the provision of the agreement was following: “by signing this contract consumer gives unconditional authority to the company to transfer information about a debtor (including, information containing personal data) to a third party without the additional agreement of a consumer, including: contact persons identified by a consumer, family members and other persons residing on the address of a consumer, debt collection companies, companies ensuring money transfer services and other persons. Transfer of personal data to a third person shall be ensured in order to implement authority established by this contract and Georgian legislation and enforcement of existing obligations, including for the purpose to search for a debtor and make him/her pay debt and fulfil obligations determined by this contract.”





The Inspector considered that this provision of the agreement was general and very broad; it did not provide information to an applicant regarding the possible purpose of transferring his/her personal data to a third person, including family members. Terms and conditions of an agreement, without the reasons and grounds of concrete necessity, shall not be considered as expressing voluntary consent to disclose information regarding the financial obligations of an applicant to a third person.

In described situation Inspector decided to demand from data controller to clarify the provisions of an agreement regulating personal data processing, by determining of purpose of the processing and to decide volume of the processing taking into account real needs.

For the loan issuing companies and debt collection companies it is important to consider following, during data processing:

- *To give clear information to data subject about processing of their data, including, cases of possible disclosure (to whom the information can be disclosed, when, in which cases and volume of disclosed information);*
- *The information regarding the financial obligation of a person might be disclosed to third parties only in case if it is necessary and if it is measure of last resort to achieve the legitimate purpose of a company, minimum amount of personal data shall be disclosed in such cases.*




ISSUES RELATED TO PROCESSING OF PERSONAL DATA BY DATA PROCESSOR

Frequently data controllers use the services of different entities and make the personal data possessed by them available to such entities. In such circumstances these entities are processing personal data on behalf of organization giving the assignment and for the purpose of the Law of Georgia on Personal Data Protection represent data processors who has contractual relations with data controller. This contract shall be signed according to the rule and in a form established by the law.

In 2016 during the inspection of legitimacy of data processing by the Personal Data Protection Inspector by data processors there were revealed cases where contract between data processor and data controller was covering several issues of providing service and also included the assignment of processing personal data. In some cases such assignment was not in compliance with the rule established by the law. For instance, the contract was not made in writing; the relevant mechanisms of data security were not identified; There were revealed cases when data processor exceeded authority envisaged in contract and etc.

In 2016 while dealing with one of complaints, Inspector examined the service contract between online credit organization and debt collection company with regard to personal data processing. It was revealed that contract did not include prohibitions determined by the law and rules of data processing, concrete mechanisms of ensuring data security and prevention mechanisms for exceeding of powers were not identified either. In addition, companies determined that data controllers failed to monitor data processor, when according to the law “a data controller is obliged to monitor





data processing by data processor, to cover rules, prohibitions and obligation of an authorized person to take measures determined by the law in relevant contract in order to minimize unlawful or accidental disclosure of data or other risks related to processing”.

Companies were requested to bring a contract on data processing in compliance with the requirement of Law of Georgia on Personal Data Protection.

Several facts of absence of written contract on data processing and failure to regulate process of data protection by data processor were revealed during the process of reviewing complaints . It was not clear what was assignment, how should it be fulfilled and how the security and good faith of data processing shall be ensured.

According to the Law of Georgia on Personal Data Protection data processor shall process personal data within the scope of authority determined by the data controller, in order to prevent unlawful processing which is will not be incompliance with the original purpose of data processing. Furthermore, it is very important for data controller to assign the data processing to a qualified, trustworthy and honest person, because dishonesty of data processor can cause unlawful use of personal data.

In 2016 a citizen reported to the Personal Data Protection Inspector that lender disclosed amount of debt and related information to the family members through the telephone conversation. As it was revealed an applicant strictly wanted to keep information about the financial debt confidential and after the information was disclosed the serious conflict arose between applicant and his/her family members. In this case data was processed by data processor. In particular, data processor on its own initiative, without the consent



of data controller, found out names and contact information of family members of the applicant and communicated to them information related to debt of an applicant.. According to the contract data processor was obliged to perform assignments honestly and had to be lawful, enforceable and concrete; moreover, an authorized person was prohibited to share personal data of debtor to a third party. It has been established that data controller did not give the power to data processor to disclose information regarding the financial debt to the family members of the applicant. It was not necessary to disclose information regarding the financial debt of an applicant. Due to the fact that data processor exceeded power assigned by data controller and unlawfully disclosed personal data to a third party administrative liability in a form of fine was imposed to it.

The following shall be taken into consideration by organizations when they assign data processing to data processor:

- ***The service contract shall be concluded in writing and shall include special rules and prohibitions of data processing for data processor;***
- ***Contract with data processor on data processing shall not be concluded if due to the activities and/or aims of data processor there is a risk of inappropriate data processing.***
- ***Any further data processing by data processor for any other purposes shall be inadmissible. Data processor may not transfer the right to process personal data to any other person without the consent of a data controller.***
- ***Data controller shall be obliged to monitor data processing by data processor.***



PROCESSING OF PERSONAL DATA OF EMPLOYEES


The personal data of employees by the public or private organizations are processed based on legislation regulating labor relationships and consent of an employee. In certain cases organizations have legitimate interest to process certain volume of information of employees for the purpose to control the service quality, although the protection of organizational interests shall not take place on account of disproportional limitation of rights of employed persons.

As a result of inspections of several big companies it was revealed that organizations keep different categories of personal data for indefinite period of time even when there is no legitimate purpose of processing such data. For instance, it has been revealed that organizations were keeping the data of those candidates who failed job competition. Among stored data were: CVs of a job candidates, submitted documents, data of their family members and the results of tests. Organizations failed to provide reasons for storing personal data of possible candidates for indefinite period of time.

The issue of lawfulness of monitoring of communication during the working hours is very important when discussing personal data processing of employees. The legislation does not provide separate regulation related to monitoring of work related communication but in order to ensure the right to privacy of employees it is necessary to protect the principles of data processing and monitoring the communication only in cases determined by the law.

During the reporting period two citizens applied to Inspector's Office and indicated that employer monitored the means of electric communication and acquired the content of personal correspondence. It has been revealed during the





inspection of the fact that means of electronic communication were registered in the name of a company and were used by the employees to communicate with the customers of a company. In addition, employees were warned about the monitoring of electronic means of communication in their use for the purpose of quality control of customer service, though a company allowed employees to use electronic means of communication transferred to them by a company for the personal correspondence as well. It has been revealed that employer did not define scope and purpose of monitoring of electronic means of communication in the use of employees, this fact created threat of disproportional processing of personal data of employees. The recommendations were given to the data controller.

During the monitoring of the employees' correspondence organizations are obliged :

- *To give clear instructions to employees whether they are allowed to use work e-mail, telephone and other means of communication for personal purpose;*
- *Preliminary inform employee about the monitoring of work correspondence, as well as cases and forms of monitoring;*
- *To conduct monitoring only in case of existence relevant legal grounds and to get familiar with only necessary information in minimum volume.*

The decision of the European Court of Human Rights on the case of **Barbulescu v. Romania** regarding processing of employees' personal data



dated January 12, 2016 is very important. According to the facts of the case, one of the private companies terminated employment contract due to the use of “Yahoo Messenger” for personal correspondence during the working hours. “Yahoo Messenger” was created for the work related purposes. Moreover, factual circumstances proved that the internal regulation of the company strictly prohibited usage of organization’s communication means for personal purposes and employees were informed about this in writing.

Based on the circumstance the European Court of Human Rights concluded that a fair balance was struck between the applicant’s right to privacy and correspondence and his employer’s interests, because employee was prohibited to use “Yahoo Messenger” for personal correspondence and it therefore found that the employer acted within the scope of its authority and the monitoring was limited in scope and proportionate. It is important to note that according to the Court’s assessment making telephone call or sending electronic correspondence from the work environment is protected by Article 8 of the European Convention on Human Rights. In case employee is not informed about the monitoring he/she has legitimate expectation that his/her personal communication and use of internet is protected from interference. The decision of the European Court of Human Rights on this case was different from other decisions made on issue of employees’ data processing (see the cases of *Halford v. United Kingdom* (1997) and *Copland v. United Kingdom* (2007)), because in instant case the internal regulation strictly prohibited use of company’s computer and resources for personal purpose.

MONITORING OF HOTELS

Three hotel chains were inspected in 2016 due to the volume and content of processed personal data in the hotel management process, the number



of personnel involved in the processing and other related risks. The scope of inspection was lawfulness of processing of guests' personal data.

The hotels possess following information about the guests: name and last name; passport number; credit card information; information about all transactions made in electronic program regarding the guest (including room reservation; canceling the reservation, placement of a guest at the hotel, special requests made by a guest, history of staying at the hotel in the past, telephone calls made from the hotel room, as well as goods and services purchased during the stay at the hotel and etc.).

None of the inspected hotels depersonalize or delete above mentioned personal data the guests' data was stored since the moment of establishment of a hotel for indefinite period of time, even when there was no need, necessity and lawful interest to process these data.

Article 4, paragraph "e" of the Georgian Law on Personal Data Protection clearly envisages certain criteria for data retention; In particular, according to this provision "data may be kept only for the period necessary to achieve the purpose of data processing. After the purpose of data processing is achieved, data must be blocked, deleted or destroyed, or stored in a form that excludes identification of a person, unless otherwise determined by Law".

According to the information provided by the companies data was stored for statistical purposes, which cannot be considered to be adequate for lawful interest, because it is sufficient to use depersonalized data for this reason. Based on above mentioned, companies were requested to apply appropriate organizational and technical measures to make possible to delete, destroy or keep data in depersonalized form. This absolutely excludes the risk of unlawful use of personal data and so that hotels' pur-



pose to analyze statistical information will be still achieved and will be more effective to increase the quality of services provided by the company. It is important to take into account that deletion/destroy of old personal data serves not only the interests envisaged by the Georgian Law on Personal Data Protection but also the financial interests of a company, because storage of information and documents containing personal data is linked to certain expenses.

Hotels shall take into account the following when serving the clients:

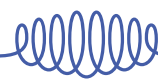
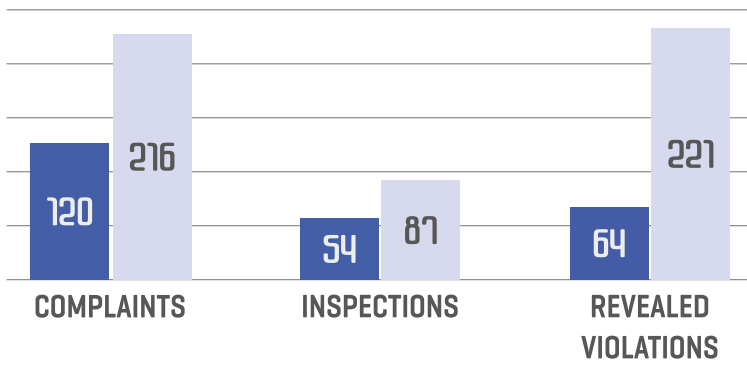
- *Identify precisely needs based on which they will request concrete information from clients for the further processing;*
- *Determine strictly the timeframe of storage of received information as well as group of those people who can have access to data about the guests stored by the hotels;*
- *Delete/destroy information containing personal data as soon as commercial purpose is achieved or shall be kept in depersonalized form for statistical purposes.*





2015

2016





DISCLOSURE OF PERSONAL DATA AND ACCESS IN INTERNET

DISCLOSURE OF PERSONAL DATA AND ACCESS IN INTERNET

Legislation allowed data subject (natural person) to decide personally whom to allow processing of his/her personal data, for which purpose and in which volume. The exceptions from this rule are permitted only in cases determined by law when private and public interests prevail over the interests of a citizen. The principles of data processing determined under article 4 of the Law of Georgia on Personal Data Protection in conjunction with the legal grounds of data processing create guarantees for the protection of right of data subject.

Violation of principles of data processing can be especially damaging for data subject in case his/her personal data becomes public in internet. In the internet data is accessible for any person and indefinite number of people has opportunity to use disclosed personal data for personal interests. Frequently disclosure of data can be considered to be necessary to achieve the respective legitimate purpose, but evaluation shall always be done - whether the information can be disclosed so that the interests of data subject are protected.


In 2016 three juveniles applied to the Inspector. They indicated that the decision of Tbilisi City Court about the limitation of representation right to a parent of one of the applicants' was public in internet. When entering the name and last name of an applicant in search engine of internet the information with personal data of an applicant was available on the webpage of LEPL Department of Common Courts; in particular, decision of Tbilisi City Court on public notification issued in 2014.

It has been revealed that based on the procedural legislation the court decision on public notification were permanently published on the webpage of LEPL Department of Common Courts, and the date for removal of this information from internet was not identified. As procedural legislation requires publication of public notification, Inspector concluded that her competence did not apply to the data processing for the purpose of case proceedings in the courts, including making public notifications. In this case the fact, that the exclusion from the authority determined by the Law of Georgia on Personal Data Protection is present until there is need to process data for the purpose of legal proceedings and personal data processing is necessary to ensure justice, shall be taken into the account. After the mentioned purpose is achieved the regulations determined under the Law of Georgia on Personal Data Protection apply to the personal data processing by the courts, including the publication of court decisions with personal data on the webpage of common courts. According to the procedural legislation after 7 days pass from the publication of decision on public notification it shall be considered to be delivered to a party and after the passage of this term there was no longer legitimate purpose for further availability of decision on webpage. Court was requested to evaluate and determine the timeframe and scope of public availability of decision on public notification including personal data on the webpage and to apply appropriate organizational and technical measures which will allow deletion of data from the webpage after the passage of term mentioned above. Based on a decision of the Inspector the High Council of Justice of Georgia on September 12, 2016 adopted decision №1/250, according to which public

notification published on webpage is not available after the expiration of 7 days from the moment of publication.


The similar evaluation was given to the LEPL National Bureau of Enforcement procedure for publishing notification/proposal for indefinite period of time on webpage. Within the scope of dealing with one of the complaints the Bureau was requested to determine for the achievement of relevant legitimate purpose the term and volume of publication on webpage of notification/proposal containing personal data and to delete the document with personal information from webpage after the expiration of term.

The decision of the Inspector regarding the publication of personal data by the LEPL Georgian Bar Association in respect of disclosure of data in internet is very important. Lawyer applied to the Inspector and indicated that decisions made against him/her in 2014 and 2015 by LEPL Georgian Bar Association was published on official webpage. He/she requested from the Georgian Bar Association to depersonalize data but his/her request was rejected. Within the scope of examination of complaint it has been revealed that according to the Georgian Law on Advocates of Georgia a person may get rid of the status of disciplined lawyer by nullification of the sanction. Warning of a lawyer shall be considered cleared in six (6) months after the date of its imposition. In the case of suspension of membership of the Georgian Bar Association, mentioned disciplinary sanction shall be considered cleared after the expiry of one (1) year from the date of restoration of membership. It was ascertained that the above-mentioned circumstances were not considered when publishing decisions of the Ethics Com-



mission at the webpage and the decision remained public even after the clearance of sanction which was considered to be against the requirements of Law of Georgia on Personal Data Protection. Based on a decision of the Inspector LEPL Georgian Bar Association was assigned to evaluate the term and volume of publication of a decision on their webpage and to remove it after the expiration of set term. The decision of the Inspector was appealed to the court but Tbilisi City Court did not share the position of an applicant.

In majority of cases the legislation does not determine the term for data processing/publication and organizations do not have specific and clear goal for the data processing. Accordingly data processor does not delete, block or depersonalize unnecessary personal data after the goal of data processing has been achieved. The most problematic with this regard is the terms for the data processing published in internet, because in such circumstances publicity of data for any additional day significantly increases the risk of damaging lawful interests of data subject. Such cases were mainly revealed in the law enforcement field when investigative agencies disseminated information containing personal data for the purpose of informing citizens so that the relevant evaluation of protection of interests of data subject by the data processor did not take place.



A representative of a citizen applied to the Personal Data Protection Inspector and indicated that the Ministry of Internal Affairs in its official webpage and through different means of media disseminated the video footage of arrest of a person where direct identification of a person was possible. The Office of Personal Data Protection Inspector studied the case and did not agree with the explanation of the Ministry of Internal Affairs stating that the dissemination of video footage of arrest served the purpose of protection

of public security, avoiding threatening circumstances and possible negative impact by disclosing identity of arrested person. The Personal Data Protection Inspector determined in her decision that possible negative impact in the given case was neutralized, there was not state interest to disclose threatening circumstances and identity of a person in order to protect public security. In addition the fact that the Ministry usually disseminated the video footage of arrest in a form excluding the identification of a person was taken into consideration, which is acknowledged international practice. Taking into account the factual circumstances of present and other cases it has been established that the Ministry violated the principles of data processing and there were no legal grounds to do so.

During the inspection it has been revealed that the Ministry of Internal Affairs publicized through its official webpage information regarding the past criminal record of a person but it has been revealed that the criminal records were cleared for the crimes committed in the past. Accordingly the information disseminated by the Ministry was not correct and precise. According to the legislation a person with cleared criminal record is a person without any criminal past. The public entity is obliged to establish not only the fact of indictment but also the issue of clearance of criminal record when the case is about the disclosure of very sensitive, special category personal data, information about the past criminal record and to process special category data only in cases determined by the law.

The lawfulness of data processing by the Investigative Unit of the Ministry of Finance of Georgia through the official website (www.is.ge) was inspected during the reporting period. In particular, disclosure and publicity of special cate-

gory data such as citizenship, employer, arrest, defendant's status, commencement of criminal case and other type of information about different natural persons without the legal grounds determined under article 6 and article 5 of the law of Georgia on Personal Data Protection (information regarding the production-sale of counterfeited money and arrest of a person for similar crime in the past). The Ministry identified the legal grounds for such actions to be public awareness for the purpose of prevention regarding the success of the investigative unit in crime combating, especially about the revealed and suppressed crimes; as well as grounds determined under article 5, paragraph "g" and "e", prevention of crime, significant public interest and protection of legitimate interests of a third person.

Personal Data Protection Inspector determined in her decision that in order to achieve the goal of crime prevention it was important to inform public about the achievement in combating the crime by the Investigative Unit, especially regarding the revealed and suppressed crimes. Although, in a given case identification of possible criminal and disclosure of information about them does not represent mandatory condition for the crime prevention and it shall not have impact on the formation of public opinion, and it will not be able to avoid the crime and protect the public order. Therefore, the goal of protection of important public interests was achievable by placing information on the official website of the Investigative Unit in a form that will not allow full identification of data subject.

In addition to administrative measure the Ministry was requested to remove or depersonalize information containing

personal data published on the official website of the Investigative Unit and examined by the Inspector.

The cases of publication of personal data for indefinite period of time have been revealed during the reporting period by the different educational institutions as well as by the LEPL National Assessment and Examination Center. It has been established based on the applications and notifications submitted by the citizens that the website of organization kept public without the legitimate purpose, for indefinite period of time, personal data of students and entrants, in particular, the results of different exams conducted in the past, with the personal data of students/entrants. Despite the fact that the institution had the legitimate purpose to publish the personal data initially the Inspector decided that there is no purpose or necessity of publicity of personal data after the legitimate purpose has been achieved. Data controller was requested to remove personal data from website after the achievement of legitimate purpose.

During assessment of the issue of publicity of personal data, data controllers shall define:

- *Concrete, legitimate purpose of making data publicly available;*
- *Whether it is possible to achieve legitimate purpose without the public availability of personal information;*
- *Whether publicized personal data is proportional to the legitimate purpose of the processing and ensure that it is removed from the website after achievement of legitimate purpose.*

AUDIO-VIDEO RECORDS PUBLISHED IN INTERNET

While discussing the problem of accessibility of data in internet it is very important to mention dissemination of several video or audio recordings of private life through social networks and media, as well as disturbing facts of threatening to disseminate video recording portraying private life.

In several cases, as a result of the efforts of public agencies, access to the resource where video files were made public has been immediately restricted., but even short period of time was enough to save videos and there was threat of repeated dissemination of videos and increased risk of violation of interests of those shown on the video and their family members. Unlike previous years in 2016 the users of TV media and social networks showed strong sense of responsibility and the videos have not been disseminated further. The society was also unified when requesting the necessity of quick and effective investigation of this crime, including the origin and authenticity of video records.

The Inspector, despite the fact that all exposed cases contained crime attributes and were beyond competency of Personal Data protection authority, underlined several times through her public statements about the necessity of effective and immediate preventive mechanisms and investigation, need to involve foreign experts, high public interest towards the outcome of investigation and negative impact of dissemination of audio-video recordings not only on the right to privacy of concrete persons but also the public perception and approach.

During the reporting period through the webpage of one of the newspapers the video called "prison video footage" was disseminated. The footage allowed full identification of persons, which was infringing for their dignity and honor, harmed their interests and interests of their family members. Despite the fact that the scope and mandate of Inspector's

Office does not cover data processing by media outlets for the purposes of providing information to public, the Inspector identified in her public statements the obligation of media to strike a fair balance between informing public and protecting human dignity and honor, especially when it comes to the high number of victims of inhuman and degrading treatment and torture and when the form of dissemination of such information allows unlimited access to it.

DATA PROCESSING REGARDING THE HEALTH CONDITION OF JUVENILES

Especially high standard of protection of child's rights is established not only by the national laws but also by international documents. The special attention and care is necessary when the case refers to the special category of data regarding the juveniles. During the reporting period the Office of Personal Data Protection Inspector received several notifications related to processing of pupils' special categories of data by the public schools.

Based on the notification received from the Ministry of Education and Science of Georgia the Office of Personal Data Protection Inspector inspected the lawfulness of processing of special category personal data of two pupils by the public school in one of the regions of Georgia. As a result of inspection of case circumstances, it has been revealed that pupils several years ago students were treated for airborne transmissible disease and after the treatment they were moved to another public school. It is important to note that they had closed form of disease that was not harmful for others. The information regarding the state of health became known to the school management and parents of classmates. This was followed by the protest by one of the

teachers and parents of other pupil. Director of the school contacted the parents of pupils and asked them not to allow children to come to school until their full recovery. One of the teachers withdrawn documents on the state of health of children from director of school and in order to examine the correctness of disseminated information provided them to one of the doctors of a hospital. It is important to note that parents were not informed about this fact. Soon after this fact the issue was discussed at the meeting of parents'. The school informed parents that based on the documents on state of health pupils were allowed to come back to school and attend classes because their health condition was not dangerous for others any more.

According to the legislation, school is obliged to create the safe and secure school environment for health and life at the school building as well as its surrounding territory. In addition, director of school s personally responsible for creation of safe environment for health and life of teachers and pupils. The interest of a director of school– to receive information on the form of disease and to protect the health condition of persons at school through the special measures is the obligation of director and represents legal ground, determined by law for collecting data. But communication of data, especially with teachers, parents of other childrens and doctor, according to the Law of Georgia on Personal Data Protection represents the disclosure of special category data to a third person. When the case refers to the special category data the protection standard established by the Law of Georgia on Personal Data Protection of Georgia is very high. According to article 6, paragraph 3 with-

out the written consent of the data subject making publicly available and disclosing of special category data to a third person is prohibited. As a result of inspection it has been revealed that school did not have such consent. The fact that the addressee (for instance: school teacher) was informed about the disease of a student did not release school from the obligation determined by the law. In addition, school officially verified the diagnosis regarding the disease of students (complete diagnosis) to third persons in addition to teachers.

This example once more proves how large scaled can be possible harm caused by processing of personal data in violation of rules envisaged by law. The special care and caution shall be taken into the account when processing the information regarding the health condition. It is also important to note, that this is not single fact related to the processing of personal data of pupils by the schools; It is important to develop systemic approach towards the problem which requires development of concrete steps for establishment of high standards for personal data protection which will help to raise public awareness regarding the importance of data protection. The Inspector's Office started cooperation with the Ministry of Education and Science of Georgia to develop special recommendations for this purpose.

INFORMATION BUREAUS

According to established practice any interested person was able to obtain information from the information companies regarding any fixed telephone subscriber. Therefore, during the reporting period the lawfulness of data processing by two biggest information bureaus were investigated, taking into account that they process personal data of subscribers in big volume and risks related to that.

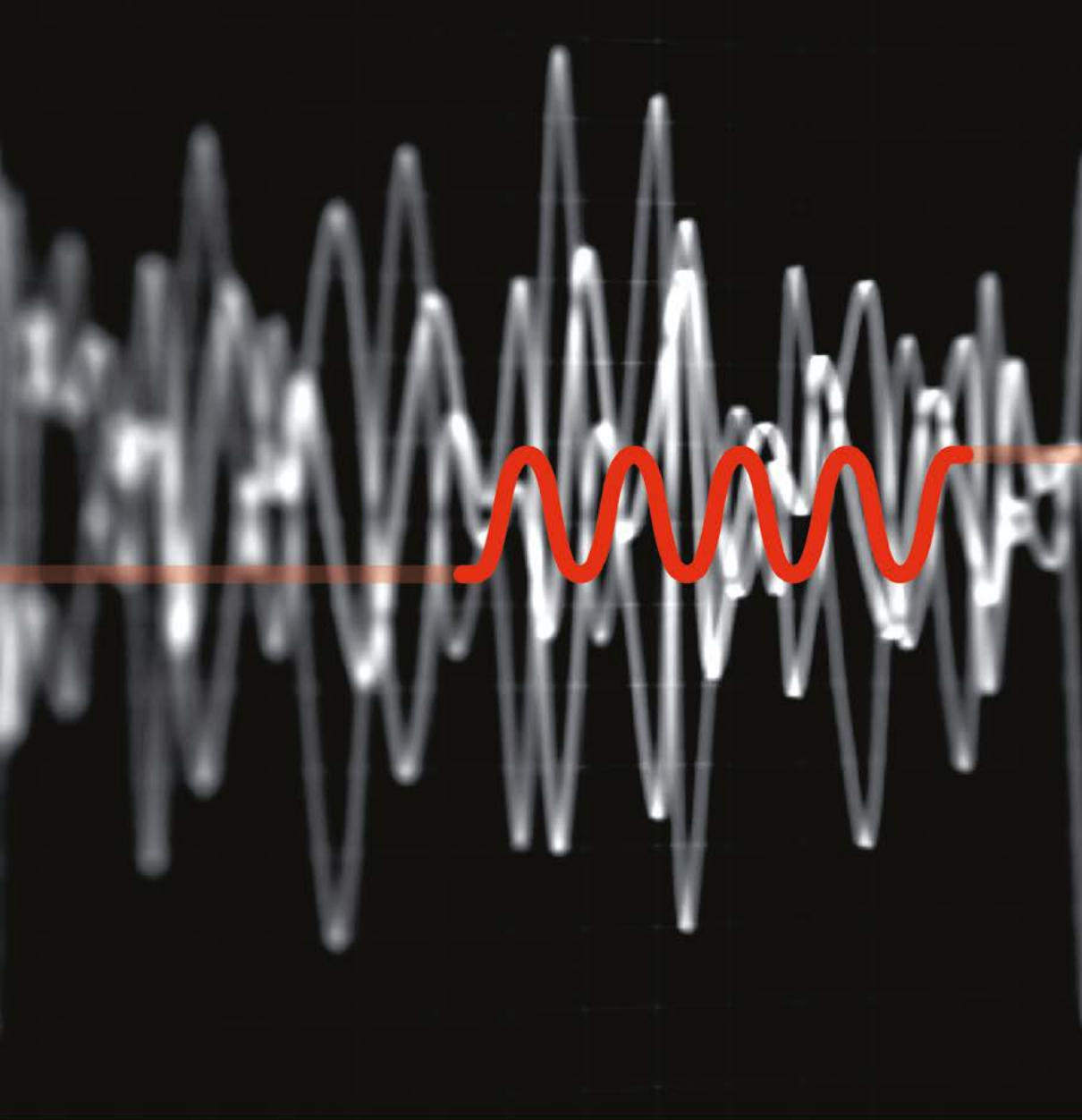
Th companies own electronic data base, were the fixed telephone numbers of subscribers are kept, database includes the name and last name, address, telephone number of an individual. During providing information services the companies were providing data to any interested person in case of request, without informing and obtaining consent from subscriber.

According to the explanation provided by the company, personal data processing of personal data, in particular collection, storage and disclosure to third parties was performed based on consent of subscribers. According to the law of Georgia on Personal Data Protection consent is determined as a voluntary consent of a data subject, after receipt of the respective information, on his/her personal data processing for specific purposes expressed orally, through telecommunication or other appropriate means, which enables clearly establishing the will of the data subject. Therefore law determines that the mandatory condition for data subject consent on processing of his/her data (including disclosure) is receiving of the respective information and expression of will for processing data for special purpose. Companies failed to present any information/documentation proving that they have obtained the consent for collection, storage and disclosure of data to interested persons.. In addition, it has been established during the monitoring that conversation between the operators and customers was audio recorded and companies were keeping these records for indefinite period of time.

Based on all above mentioned and decision of Inspector companies were requested: to determine the grounds for personal data processing, establish accuracy of data, to update data, to delete and remove data collected without legal grounds and irrelevant to the processing purpose and to determine reasonable period of time for keeping the audio recording of conversation between the operator and customer and delete/remove them after the expiration of this time.

During data processing it is necessary for any organization operating in information providing services and anybody rendering information about them, including any authorized person to take into account following:

- *To process data, including disclosure of information about the subscriber, only in case of existence of legal ground, including consent of subscriber, determined by law.;*
- *Consent of subscriber shall be identified as voluntarily expressed will and not condition. Refusal to data access data shall not cause limiting the communication services.*



**OVERSIGHT OVER COVERT
INVESTIGATIONAL ACTIVITIES AND
PERSONAL DATA PROCESSING BY
LAW ENFORCEMENT AGENCIES**

OVERSIGHT OVER COVERT INVESTIGATIONAL ACTIVITIES AND PERSONAL DATA PROCESSING BY LAW ENFORCEMENT AGENCIES

The law enforcement agencies have a special role in protecting human rights, including the right to privacy. The law enforcement agencies usually adequately react to the Personal Data Protection Inspector's decisions and recommendations. However, the cases considered by the Data Protection Inspector's Office demonstrate that while implementing their responsibilities the law enforcement agencies mainly face challenges with upholding the principles of data processing and the existence of legal grounds necessary for data processing. Also, it needs to be noted that in 2016 one fact of criminal nature was detected and transferred to the law enforcement agency for reaction.

OVERSIGHT OVER COVERT INVESTIGATIONAL ACTIVITIES

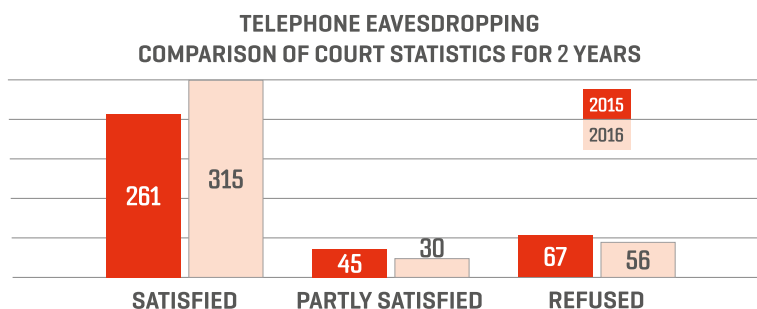
The public is particularly interested in the issues of personal data processing during covert investigational activities and oversight of this process. According to the legislative amendments adopted on March 31, 2015 Personal Data Inspector was authorized to oversee investigational activities envisaged in Articles 136-138 and "a" and "b" sub-paragraphs of Article 143¹ of the Criminal Procedure Code of Georgia.

According to these legislative amendments the Inspector's Office regularly studies statistics and content of the court decisions and decrees of the Prosecutor's Office. The Office also compares these data with the statistics published by the Supreme Court. According to the 2016 data, among co-



vert investigational activities the most frequent action was submission of a motion to receive a document or information in accordance with the Article 136 of the Criminal Procedure Code. Compared to the previous year the secret telephone eavesdropping statistics have slightly increased. The least number of decisions have been made in favor of controlling postal and telegraph communications.

Compared to the previous year the number of covert investigative activities has generally increased. As for the secret telephone eavesdropping and recording, compared to the previous year the number of court decisions submitted to the Inspector's Office has increased by 28 while the number of motions requesting an extension of the term for such actions has decreased by 6 in 2016. In 2016 the Inspector did not give consent in 47 cases by means of the two-stage electronic system of covert investigative activities. The reasons of refusal were technical errors detected during examination of legality of grounds for data processing or inaccuracies/ambiguities in the resolution part of the decision. Approvals were provided after these inaccuracies were addressed.



TERM EXTENSION COMPARISON OF COURT STATISTICS FOR 2 YEARS



During the reporting period the inspection of the Operative-technical Unit of the State Security Service was completed to check legality of covert investigations and activities concerning data banks, which are envisioned in Sub-paragraphs “a” and “b” of the Article 143¹ of the Criminal Procedure Code. It needs to be noted that the activities of the Operative-technical Department of State Security Service are regulated by sub-statutory normative acts, which are undisclosed or fully secret. The inspection revealed various flaws related to the procedural, technical and legal issues in covert investigative activities and actions related to data banks. The Inspector decided to issue special recommendations/orders to the State Security Service of Georgia and set a deadline for implementing these orders. The Operative-Technical Department of the State Security Service of Georgia provided information on how these recommendations/orders were considered in due time.

OBLIGATION TO NOTIFY THE PERSONAL DATA PROTECTION INSPECTOR


In 2016 the law enforcement agencies and electronic communication companies failed to fulfill properly obligation to notify the Personal Data Protection Inspector in ten cases. This number is smaller compared to the previous years, that shows tendency of reducing of violations.

The Article 143³, Part 6² of the Criminal Procedure Code envisages an obligation to send one copy of the prosecutor's decree with the justification of investigative activities to the Personal Data Protection Inspector. In the reporting period the Office of the Personal Data Protection Inspector inspected the Prosecutor's Office due to the failure to fulfill this obligation in 9 cases.

As a result of inspection it became clear that in 6 cases a copy of the decision was not sent to the Personal Data Protection Inspector. The Prosecutor's Office provided an explanation according to which the decision was not provided due to the need to achieve specific legal outcomes in a short period of time by starting several urgent and simultaneous investigative/procedural activities concerning criminal cases, including planning and implementation of these activities. The Inspector did not accept this explanation and pointed out that an investigative activity provided in Article 136 of the Criminal Procedure Code unconditionally and imperatively obliges the Prosecutor's Office of Georgia to send the Inspector a decree issued by the Prosecutor's Office in response to urgent needs in a specified period of time.


Three cases examined as a part of the inspection of the Prosecutor's Office concerned delays in the provision of decrees issued by the Prosecutor's Office. The inspection established that the Prosecutor issued a







decree and sent its copy to the Personal Data Protection Inspector only after the covert investigation was practically implemented and the court acknowledged its lawfulness, more specifically the submission was late by five days. A five-day delay in providing the Office of the Personal Data Protection Inspector a decree issued in response to urgent needs was not considered to be an immediate delivery for the purposes of the Georgian law. In all of the nine cases the statute of limitations for this violation did not enable the Personal Data Protection Inspector to impose a liability envisioned in the Law of Georgia on the Protection of Personal Data on the Prosecutor's Office.

The obligation for notification is also imposed on those electronic communication companies, which are authorized persons and sphere of their activity includes telephone or/and internet network provision or/and services. According to the legislation in force, these companies are obliged to make a record of the facts of transfer of electronic communication identification data to relevant state bodies and provide this information to the Personal Data Protection Inspector in a specified period of time.



In the reporting period the Personal Data Protection Inspector examined seven electronic communication companies. During inspection the companies were asked to provide documentation related to the transfer of electronic identification data to law enforcement agencies. The examination of these documents showed that there was inconsistency between the time when the documents were transferred to a law enforcement agency and preparation of these documents. Company representatives explained that they drafted the response letters immediately after having received the decision concerning investigative activities. However, an authorized representative of the law enforcement agency





came to take the document after some time. In the decisions on such cases the Personal Data Protection Inspector noted that electronic communication companies are obliged to act in accordance with the Article 20, paragraph 4 of Georgian Law on Personal Data Protection.. This is important for the effective fulfillment of supervisory functions by the Personal Data Protection Inspector as well as for ensuring protection of human rights and freedoms, including the right to privacy. The Personal Data Protection Inspector also pointed out that for the purposes of Article 20, Paragraph 4, the time of transfer of electronic communication identification data is the moment when this document is actually delivered to the law enforcement agency and the latter has access to the content of the document. Correspondingly, the time of transfer is not the time of preparation of the document containing electronic identification data, but the moment when this document is provided to the law enforcement agency.

The inspection of electronic communication companies revealed a violation in one case. This, compared to the previous years, is an indicator of improvement of the electronic communication companies' practice of notifying the Inspector.

According to the legislation in force, in order to properly fulfill the obligation to notify the Inspector the data controllers have to consider the following:

- *It is advisable to develop internal procedures, which will describe specific job-related duties;*




- *The Agencies are advised to monitor the delivery of notifications by the courier service;*
- *In specific cases it is advisable to develop electronic registers of notifications to be submitted in order to avoid technical or human errors.*

PROCESSING OF VIDEO SURVEILLANCE RECORDINGS FOR INVESTIGATIVE PURPOSES

In 2016 the Personal Data Protection Inspector completed 14 inspections of the Prosecutor's Office to study legitimacy of requesting recordings of surveillance cameras from private legal persons and processing these data. The requests were made to meet urgent needs in criminal cases and were based on prosecutor's decrees.

The inspections demonstrated that in view of the fact that the Prosecutor's Office decided not to use the retrieved material as an evidence and applied to the court with a request not to consider a motion for acknowledging legality of the video recordings, there was no reason to keep the retrieved personal data and the Prosecutor's Office was obliged immediately destroy this material according to the rules envisaged in law. The Prosecutor's Office of Georgia violated the requirements of Article 4, Sub-paragraph "e" of the Law on Personal Data Protection by keeping the computer files with the personal data afterwards. The Inspector's Decision also discussed the issue of consent given by a data controller conducting video surveillance. A consent given by a data controller is not legal ground for providing a recording retrieved from the system of video surveillance to third parties. The consent to transfer these recordings to the law en-





forcement agency should be given by the data subjects – *“it is true that the data subjects are notified by the video surveillance signs and to some extent are aware of the fact that their images are captured in the video recordings. However, warning an individual about video monitoring is not equivalent to informing of data subject that the recording will be transferred to third parties or that he/she consents to such action.* The inspection established a violation of the law by the Prosecutor’s Office in 13 out of 14 cases and imposed a fine according to the Code of Administrative Violations.

In the reporting period the Ministry of Internal Affairs of Georgia and Tbilisi Mayor’s Office were also inspected. The purpose of inspection was to study whether recordings of one of the video monitoring systems in the city of Tbilisi were requested and transferred lawfully. The transfer was done by City Transport Service at Tbilisi Mayor’s Office. In this case the Personal Data Protection Inspector revealed that the Ministry of Internal Affairs processed the computer files with personal data based on a letter without providing a legal document envisioned in Article 5 of the Law on Personal Data Protection – a court decision/prosecutor’s decree. The law in force sets a high standard for retrieving recordings (computer files) from the video surveillance systems. On the one hand, both public and private users of video surveillance systems have an understanding that the recordings can be retrieved from the security and protection systems for only investigative purposes. On the other hand, personal data of those persons who are not subjects of interest of investigative agencies are processed for purposes strictly defined in the law and these data are destroyed practically automatically – when the overloaded system overwrites old recordings with new ones. In 2016 the Inspector consulted many organizations/entrepreneurs about the statutory rules.

While processing of the video monitoring it is necessary:


- *To take necessary organizational and technical measures to protect the data kept in their video surveillance systems from unsanctioned access and disclosure by all data controllers*
- *To disclose and transfer data kept in the video surveillance system to the representatives of the law enforcement agencies only according to the rule established in the Criminal Procedure Code;*
- *To delete/destroy data processed in the video surveillance system after the expiration of data retention term.*

PROCESSING OF COMMUNICATION IDENTIFICATION DATA


According to the legislation in force, an electronic communication company shall register the facts of transfer of communication identification data to the state bodies and inform the Personal Data Protection Inspector about these facts according to the rules established in Articles 112 and 136 of the Criminal Procedure Code of Georgia.

The statistics provided by the electronic communication companies reveal annually growing number of requests for the submission of electronic communication identification data made by the investigative bodies for operative-investigative purposes. As an example, according to the information provided by one of the companies, in 2015 the company received 373 (three hundred thirty-seven) court decisions concerning information requests, in 2016 the information was disclosed based on 683 (six hundred eighty-three) decisions.







The data processing by communication companies for investigative purposes has revealed a number of problems. However, it needs to be noted that the scale and nature of these flaws and violations has been substantially reduced compared to the previous year. The electronic communication companies pay greater attention to and examine grounds for disclosing information. For example, according to the information provided by one of the companies, in 2016, 300 requests made by investigative bodies were declined and the latter were asked to submit copies of court decisions/prosecutor's decrees.



One of the inspections revealed that the electronic communication company disclosed the information despite the lack of legal grounds envisaged in the Article 5 of Georgian Law on Personal Data Protection. The information was disclosed at the time when the court decisions was not valid any more according to the requirements set in the Article 143³, Part 12 of the Criminal Procedure Code and could not be applied as a legal ground for disclosing computer data. There were also cases where the volume of disclosed information exceeded the data that was requested.

In the reporting period the inspection of the Ministry of Internal Affairs revealed that it requested and received information from an electronic communication company without legal grounds. The electronic communication company, on the other hand, submitted demographic information for the person whose IP address was different from the address indicated in the court decision. In this decision an error was made in the IP address. The error was not corrected in accordance with the rule indicated in the Criminal Procedure Code of Georgia.





In addition to the above mentioned, the Inspector revealed that the Prosecutor's Office also violated the law while requesting information based on the court decision. In this case personal data files were requested and were delivered by the electronic communication company while the court decision was not valid any more according to the requirements set in Article 143³, Part 12 of the Criminal Procedure Code of Georgia and could not serve as a legal ground for disclosing and receiving computer data.

Despite these cases there was a positive trend towards systemic solution of the above problems by the law enforcement bodies. In particular, in 2016 the Prosecutor's Office developed special internal recommendations for prosecutors and investigators with an aim to properly fulfill requirements provided in the Criminal Procedure Code of Georgia and the Law of Georgia on Personal Data Protection during collection of evidences in criminal cases. It is expected that implementation of these recommendations will significantly reduce the number of certain types of errors. Also, in 2016 the Prosecutor's Office of Georgia arranged five training courses to raise qualification of the staff. The training covered several topics in the context of the Article 8 of the European Convention on Human Rights, including the issues of personal data protection, telephone eavesdropping and secret recording of telephone conversations, and accessing computer data. In this reporting period the Ministry's initiative to develop the code of conduct and other work-specific legal acts for its structural units for the personal data protection purposes should be positively assessed. It also needs to be noted that as a part of inter-agency cooperation the **memorandums/agreements** were concluded. These documents outlined and adjusted practical aspects of data processing to ensure their conformity with the law.



In order to ensure full compliance of evidence collection process by law enforcement agencies with the law:

- *Each agency should develop and introduce internal recommendations/ procedures for this purpose. They should also conduct regular trainings for the employees of the agency;*
- *The statistics related to the evidence collection issues have to be systematically and regularly analyzed. The analysis will reveal problems of evidence collection processes.*





VIDEO SURVEILLANCE


VIDEO SURVEILLANCE

The law strictly defines purposes of video surveillance: crime prevention, protection of public order, protection of an individual's security and property, protection of a minor from negative influences, protection of secret information.


Video surveillance shall be conducted out of necessity and not as an additional mechanism for controlling citizens' behavior. Also, according to the law, all data processors shall display a warning sign in a visible place while installing a video surveillance system. The purpose is to respect and protect citizens' rights by informing them.

Despite the fact that the Inspector's Office carried out numerous activities related to video surveillance, including awareness raising activities, development of special recommendations, inspection of lawfulness of processed data, video surveillance was still problematic in 2016. The problems included the lack of video surveillance signs in places where video monitoring was conducted, surveillance of employees without informing them, video surveillance of neighbors' apartment entrances in residential buildings without neighbors' consent.


During the year eleven violations were detected based on the citizens' complaints and inspections. Most often citizens applied to the Inspector because of the lack of video surveillance signs in places monitored by private organizations. The video surveillance systems are most commonly used in places where customers are served (sales and restaurants). The data collected as a result of video-audio surveillance was used for improving the quality of services and controlling employees in addition to serving the purposes envisaged in the law.



The inspections carried out in 2016 revealed the cases where a company had installed a video surveillance system in its property, but did not actually conduct video monitoring. Also, there were cases where video surveillance signs were displayed in places where no video surveillance system was installed. Correspondingly, no video recording of the perimeter was conducted. In 2016 two of such cases were studied based on the citizens' applications. One concerned the surveillance signs in the fitting rooms in a clothes store, the other concerned video control warning signs in the toilets of the trade center. The Law on Personal Data Protection strictly prohibits video surveillance in fitting rooms and restrooms. Thus, the accounts of such violations led to inspections. The inspection revealed that the surveillance warning signs were displayed to prevent theft while no surveillance was actually conducted. Display of warning signs without actually conducting surveillance, particularly in places where video recording would be offending for citizens, can mislead a data subject into believing that the data related to him/her is being processed; Correspondingly, the organizations were advised to remove video surveillance warning signs.



In one case a company was conducting video surveillance within the internal perimeter of a shop without displaying a video surveillance warning sign. According to the explanations provided by a company representative, the company was engaged in commerce, including cash transactions. Correspondingly, the shop kept cash and products. Thus, the video surveillance aimed to protect the company's property and the money and other belongings owned by the employees, also, the purpose was to ensure security of the company's numerous customers and employees. The Inspector decided that these objectives served the company's important interests and correspondingly were legitimate according



to the law. However, the law On Personal Data Protection establishes special rules concerning video surveillance. The rules include an obligation to display a video surveillance sign if video monitoring is conducted. The reason for this rule is that video surveillance affects or may affect different individuals. In this case data processing does not depend on the subject's will. That is why the law establishes an obligation to inform individuals about the fact that their data is being processed, thereby respecting and protecting the rights of citizens. During inspection the company addressed this violation and prominently displayed a video surveillance sign.

VIDEO SURVEILLANCE OF RESIDENTIAL BUILDINGS CONDUCTED BY OWNERS

Among other issues the Law on Personal Data Protection regulates video surveillance in residential buildings. Very often citizens conduct video surveillance in private houses or apartment buildings with an aim to protect their property. However, the law attributes great importance to the balance between the protection of the owner's interests and the neighbors' right to privacy.


The study of different cases has revealed that quite often a video surveillance system installed for the purposes of property protection may violate the other individuals' right to privacy, for example, the rights of the neighbors in apartment buildings. It is necessary to carry out public awareness activities that would inform the citizens that they should firstly assess their needs and then select the means of property protection, including the video surveillance systems. Any person can protect oneself and his/her property at minimal costs, without using high power video

surveillance cameras (with high resolution, a zoom function etc.) It needs to be noted that in such cases the scale of data processing is lower thereby decreasing the risks of illegal processing of personal data.

In one of the cases studied in 2016 the owner of a private house installed a video surveillance system in the nearby apartment building to identify dishonest residents littering his property. In this particular case the Levan Samkharauli Bureau, a Legal Entity of Public Law examined recordings and established that the images were not good enough for identifying individuals. Only silhouettes were visible. Correspondingly, in this case the personal data were not processed.

VIDEO SURVEILLANCE OF WORK PLACES

According to the legislation in force, the owners of certain places are required to install video surveillance systems with parameters defined in a specific normative act. Such places include petrol stations, there are obligatory rules towards them to install video surveillance systems. In 2016, an inspection of one of the petrol retailers revealed that in addition to security and property protection purposes and other aims provided in the law video surveillance of petrol stations intended to control quality of the customer service and also to impose disciplinary sanctions (fines) on employees. The Inspector decided that this kind of data processing violated the rules of video surveillance, because a data controller is obliged to install and use a video surveillance system in the cases strictly defined in the law – for personal and property security, and protection of secret information purposes, if these objectives cannot be attained through other means. Also, in such exceptional cases, all employees of a private or a public enterprise have to be informed in writing about the ongoing vid-



eo surveillance and their rights. In this particular case, the petrol station employees whose workplace was monitored were not properly informed about the fact that in addition to the property protection and security purposes, the monitoring was conducted to control quality of the service.

Data controllers using video surveillance systems shall consider the following issues:

- *Video surveillance systems have to be used only in exceptional cases;*
- *A video surveillance system should have technical specifications consistent with the objectives of its use;*
- *The rights of individuals who are monitored have to be protected by prominently displaying warning signs, also in some cases, by properly informing the neighbors and receiving their consent for installing a system.*



DIRECT MARKETING

DIRECT MARKETING


In 2016 a big number of complaints of citizens, recommendations and consultations provided by the Inspector's Office still concerned undesirable promotional notifications. In comparison to the previous years, marketing conducted through phone calls was particularly problematic in the reporting period.

In 2016 forty-eight citizens applied to the Inspector with a request to examine violations of the direct marketing rules. Violations of the direct marketing rules established in the law were found in 30 cases. In 27 cases the Inspector imposed a fine, in 3 cases a sanction was not used because of the expiration of the statute of limitations provided in the law. The majority of violations concerned the lack of a mechanism which would allow a person to opt-out from offers made through telephone calls or SMSs. In some cases such mechanism existed but was functioning with problems. Companies which offer goods and services by telephone do not inform citizens on their right to require termination of processing of their personal data for marketing purposes. In some cases, citizens were still contacted in 10 days from the moment of submission of such a request. Sometimes citizens were not informed about the source of data concerning them, etc.

TELEPHONE MARKETING

In 2016 a citizen applied to the Personal Data Protection Inspector and reported that one of the companies called his telephone number for direct marketing purposes by offering books for sale. The applicant noted that he had asked the company to stop processing his personal data for direct marketing purposes several times, but these requests were ignored.





The application review revealed that the applicant asked the company to stop using his personal data for the purposes of direct marketing by an e-mail. In 10 days from the receipt of the request the company still contacted the applicant on the phone to offer its products thereby violating the obligations established in Article 8, Sub-paragraph 5 of the Law of Georgia on Personal Data Protection.

The company asserted that it did not manage to read the applicant's request on time due to a big number of letters received by e-mail and hence did not stop processing the applicant's data.

The practice shows that while offering services/products in telephone conversations, the majority of companies do not inform citizens that they have a right to request termination of using their data for direct marketing purposes. The companies also fail to make a note of refusals made orally. In the reporting period the Inspector imposed an obligation on several companies to inform data subjects about their rights during telephone marketing.

DIRECT MARKETING BY COMPANIES PROVIDING LOANS


The examination of complaints submitted in the reporting period revealed that companies providing loans (banks, microfinance organizations, on-line credit companies) often sent out messages notifying citizens that loans had been approved for them. Such notifications were sent on the initiative of company providing loans without application to the loan. The notifications concerning loan approvals did not indicate how recipients could turn off such notifications in the future.



In 2016 the Personal Data Protection Inspector received a complaint from a citizen calling for reaction to the violation of the rule for use of personal data by the bank for direct marketing purposes. During the review of the complaint, a representative of the bank asserted that the absence of the refusal mechanism in the messages concerning loan approvals was not a problem, because these messages were sent out to the bank customers, who had agreed to receive notifications by signing an agreement with the bank. According to the legislation in force, the bank is a financial institution providing financial services, and for commercial banks provision of loans and related services are authorized activities. The Personal Data Protection Inspector considered the loan offers as direct marketing, because according to the law, direct marketing is defined as an offer of goods, services, employment or temporary jobs by post, telephone calls, e-mail or other means of telecommunication. Correspondingly, such messages are subjected to the rules established in the Article 8 of the Law of Georgia on Personal Data Protection.

According to the Inspector's decision, a bank service contract cannot establish a rule different from the obligations defined in the law. Despite the fact that the client consented to receiving notifications as a part of the contractual relationship, the data subject should still have an opportunity to refuse processing of his/her personal data for direct marketing purposes at any time. Correspondingly, the bank should have been guided by the rules established in the Law of Georgia on Personal Data Protection and have provided information on the rights of the data subject as well the mechanism that would allow the client to turn off further





notifications. The Inspector's decision establishing a violation by the bank was fully upheld by the court.


It needs to be noted that following the Inspector's decision, the bank included instructions about the refusal mechanism in the sent messages thereby allowing them to refuse the use of their personal data for direct marketing purposes by sending a message to a specific number.

Despite the fact that many organizations engaged in marketing introduced the refusal mechanism, and the Personal Data Protection Inspector's Office, in addition to reacting to citizens' applications, proactively works with companies to address this problem, citizens still have to refuse the use of their data by individual companies. This is caused by the abundance of direct marketing companies and the number of offers that they make. This practice is both inconvenient and time-consuming and costly. Correspondingly, considering the best practices of the European countries, it is advisable to develop a mechanism at the statutory level which would allow citizens to decide from whom, when and how to receive promotional messages.

INFORMATIONAL NOTIFICATIONS

Many citizens approached the Personal Data Protection Inspector in the pre-election period concerning text messages received from municipalities and other election subjects after September 19, 2016. The study of the factual circumstances revealed that one of the mobile telephone companies offered the bulk SMS service to any person. This service allowed the clients to send text messages via the corporate SMS portal not only to the numbers that they themselves obtained, but also to the above companies' data bases of unidentified individuals grouped into specific segments.





In 2016 the Inspector explored legitimacy of sending SMSs through the above portal. The examination established that municipalities and election subjects had concluded contracts with the mobile operators. According to this contract, the mobile operators had an obligation to send text messages drafted by the clients through the special SMS portal to its electronic communication network. It needs to be noted that municipalities and election subjects did not collect and process the subscribers' data. Also, in the case of municipalities, the purpose of text messages was to inform citizens about infrastructural works taking place in the region. The text messages indicated a mechanism for turning off further notifications (SMS OFF). As for the election subjects, the SMSs sent on their behalf called for supporting specific subjects during the elections.

In view of the fact that municipalities and election subjects did not process the subscribers' data themselves, while text messages were sent out via an SMS portal to the bases of unidentified data, no violation of the Law of Georgia on Personal Data Protection was revealed.

Despite this it is advisable for any client, whether this is an organization or an individual, to clearly specify the purpose and the segment (subscriber selection criteria) for using such services. Also, it is advisable to allow recipients of text messages to preliminary decide whether they want to receive messages of this sort and if so, what kind of information and from whom. This should be done in a way that would not make the recipients' personal data accessible to the users of the SMS portal.



All persons engaged in direct marketing shall consider the following:

- *In all promotional offers (despite the form of an offer), the recipients shall be informed about the right to avoid marketing affecting him/her;*
- *A subscriber should have an opportunity to turn off direct marketing notifications through the same means that an offer is made by or/and some other easily accessible means.*






THE RIGHTS OF DATA SUBJECTS AND ACCESS TO INFORMATION

THE RIGHTS OF DATA SUBJECTS AND ACCESS TO INFORMATION

The Constitution of Georgia allows a citizen to acquaint himself/herself with the information and documents related to him/her, which are kept at state institutions according to the rules established in the law, unless these documents include state, professional or commercial secrets. The Article 21 of the Law of Georgia on Personal Data Protection guarantees a data subject's right to request this information. A citizen has a right to request information relating to the processing of his/her data from public and private data controllers. A data controller has an obligation to provide this information immediately upon request, or in 10 days from the moment of request, if a response to the request requires search for information, processing of voluminous documents or consulting other institutions. The citizen also has a right to request correction, update, addition, blocking or destruction of information, which is incomplete, incorrect, outdated or obtained through illegal means. The organization has an obligation to take these actions within 15 days, or inform the data subject about the reasons for refusal.

In 2016 the Inspector's Office considered applications submitted by 17 citizens concerning lawfulness of collection of information related to them, the failure to timely submit requested information or to submit it all. Eleven facts of violation of the rules for informing citizens were revealed. The majority of complaints concerned violations of the rules related to access to information by private organizations, although one of the complaints involved a public institution.




The inspector received a complaint by a former prisoner according to which the Ministry of Corrections of Georgia not only illegally processed his personal data, but also violated the rule on the access to information. The review of the application established that the personal data had been processed in accordance with the law. However, it revealed a violation of the rule for informing data subjects. More specifically, the information was provided in violation of the 10-day term.

The Inspector also received a complaint from a citizen who was asking to study whether one of the commercial banks lawfully transferred his data to the data bank of the joint stock company Creditinfo Georgia. The applicant noted that he had timely and properly fulfilled his obligations in accordance with the contract with the bank. However, the bank did not timely reflect this information in the data bank where he was still noted under the debtors' status. The bank did not properly inform the applicant thereby violating the Article 21, paragraph 1 rule for the provision of information to a data subject.

The law provides a citizen with a right to choose a form for provision of information to him/her, verbally and electronically. However, in practice there are cases where organizations did not adequately react to the requests made orally or electronically.

The Inspector received an application from a citizen who noted that he had sent the company an electronic message requesting information about the sources of data related to him. The company responded two months later, after




the Inspector started an inquiry into this case based on the citizen's complaint. The company confirmed receipt of the e-mail, but also noted that it had not studied the content of this letter.

Review of the complaint revealed that the e-mail address to which the data subject had sent the message was the company's official contact address. The company had an employee authorized to check this e-mail. The fulfillment of the citizen's right shall not be prevented by an employee's negligence or technical problems. According to the law, the applicant was supposed to receive information about the data sources immediately upon request, or in cases strictly defined in the law, no later than 10 days.

Provision of information to a data subject is also relevant to the problem of cyber threats. Increasing number of illegal hacking of personal data, more frequent attacks against computer systems, suspicious online service offers, fraudulent schemes, so called phishing, etc. become increasingly problematic in Georgia and globally. Quite often such crimes are supported by the low level of awareness of potential victims on the risks and security measures.

During the reporting period the Personal Data Protection Inspector's Office carried out several activities in this direction aiming to prevent threats and rise citizens' awareness. The activities generated tangible results.



An online credit company offered a seemingly simple service to customers: they had to enter their internet banking user name and password in the special fields on the company's website to receive a notification that their loan was



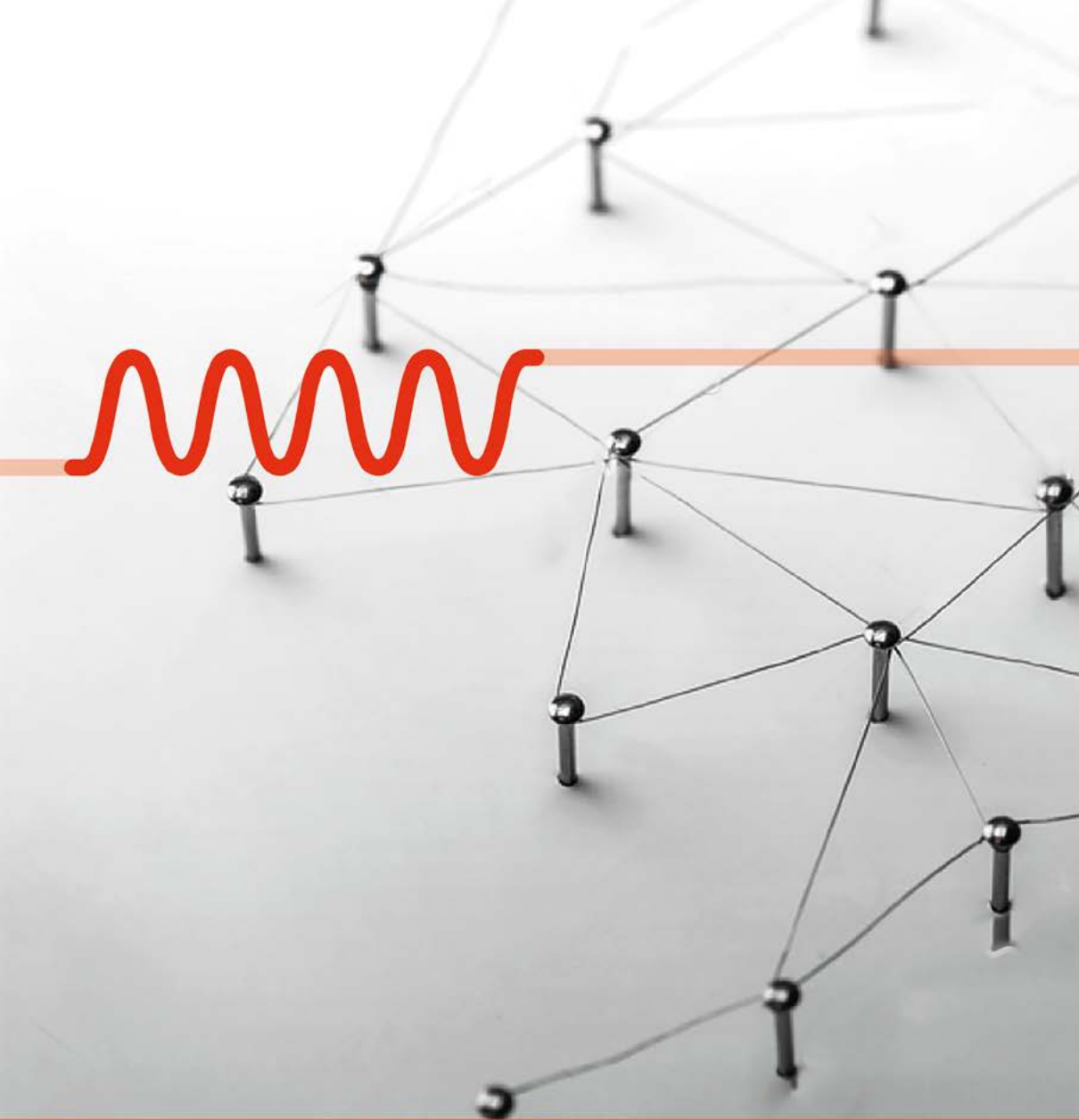
approved in a couple of minutes. This service, which was provided on the Georgian company's website, turned out to be a property of an organization registered abroad. By using the internet banking user name and data, the company prepared a report about the customer's state of finances and shared this report with the online credit company. This fact was found alarming by the banking sector because it implied an illegal access to the customers' data.

The Inspector decided that such scale of data processing was not proportional to the individual's identification purposes, while the fact that the company was getting hold of the persons' internet banking user name and password raised risks to the personal data security. The online credit company was ordered to cancel this service, which is not currently used by other organizations.

In 2016 two suspicious websites appeared on the internet. One of the sites offered to check out the customers' data on the so called black lists, the other offered to determine how safe their bank cards were. For these purposes the websites asked the customers to enter their bank information, including the card number, expiration date, and CVC code. The websites were not registered in Georgia. This complicated identification of persons running these sites. The Personal Data Protection Inspector published several statements warning citizens. The Ministry of Internal Affairs has also started an inquiry into this issue. Consequently, the suspicious service collecting citizens' banking information disappeared from the websites.



In 2016 several suspicious applications were circulated in Facebook. These applications offered customers different services in exchange of personal data, including provision of information on the visitors of their Facebook profiles. In view of the high risks of the so called phishing, the Personal Data Protection called on the internet users to take caution. These statements attracted high interest from the public and media. Consequently, several citizens contacted the Inspector's Office for consultations and additional information concerning their internet security.



**THE INSPECTOR'S PARTICIPATION
IN THE LAW-MAKING PROCESS,
EDUCATIONAL AND OTHER ACTIVITIES**

THE INSPECTOR'S PARTICIPATION IN THE LAW-MAKING PROCESS, EDUCATIONAL AND OTHER ACTIVITIES


PARTICIPATION IN THE LAW-MAKING PROCESS

In the reporting period opinions and recommendations concerning draft laws and sub-statutory acts were sent to several bodies based on the requests of the latter. The aim of the recommendations was to ensure conformity of the drafts with the legislation on personal data protection. These included the following acts:

The Minister of Labor, Health and Social Protection draft order on “the rule for writing a prescription for the second group pharmaceutical products (medication products) and approving the form #3 – the prescription form”. The electronic prescription form includes an individual's personal data, in some cases, it is possible to retrieve information about the state of the person's health; Correspondingly, it was important to ensure that the data processing rules were clearly and precisely defined in the draft order. The Ministry was advised to refine the registration rule for individuals authorized to access the data kept in the electronic system, to specify the volume of data to be processed, to delete/archive invalid prescriptions, to conduct so called data logging, to take security measures, also to create a so called “patient's page”, through which citizens would be able to check whether their data were accessed.

Based on the request of the Ministry of Internally Displaced Persons from the Occupied Territories of Georgia, Accommodation, and Refugees the Inspector's Office studied the draft law on International Protection and as-





sociated drafts. The Ministry was provided with the opinion on processing the special category and biometric data, audio recording, and regulations concerning the terms for data retention.

In addition, consultations were provided to the Ministry of Economy and Sustainable Development on the draft law on Electronic Commerce; to the LEPL Data Exchange Agency on the amendments to the Administrative Code of Georgia; to the Ministry of Justice on draft amendments to the Law on Prevention of Legalization of Illegal Income; to the Public Defender on draft amendments to the Organic Law of Georgia on the Public Defender, draft amendments to the Law of Georgia on International Treaties, draft amendments to the Code of Imprisonment, draft amendments to the Criminal Code of Georgia, and draft amendments to the Parliament Rules of Procedure.

Recommendations were also provided to the Supreme Court of Georgia and the High Council of Justice on the High Council of Justice Rule for Publication and Access to the Court Acts; to the Ministry of Internal Affairs on the issue of regulation of DNA data; to Tbilisi Mayor's Office on the instructions concerning video monitoring of public preschools and retaining, processing, and destroying recordings by means of electronic equipment; to the Administration of the Government of Georgia on the Government Decree approving the rule for placing video surveillance cameras in public places for the security and protection of order purposes; to the Ministry of Corrections on the joint draft order of the Ministry of Internal Affairs of Georgia and the Ministry of Corrections of Georgia concerning instructions for the provision of medical information related to an accused/convicted person by Ministry of Internal Affairs' isolators of temporary retention to the Ministry of Corrections penitential institutions.



As a result of the above work the procedures for data processing envisaged in various laws or sub-statutory acts were refined; the objectives of data processing envisaged in these acts were clarified; the data security guarantees were introduced. In some cases it was decided that a particular way of data processing was not reasonable due to the associated risks.


Introduction or/and revision of regulations concerning data processing requires the Inspector's involvement in the law-making to ensure technical and material conformity of the regulations to the Law of Georgia on Personal Data Protection. This is particularly important for the areas where data processing should be approached particularly carefully, e.g. in health care, education, financial activities. Consideration of the data processing principles at the early stage of law-making will reinforce the high standards of data processing in the Georgian legislation.

TRANS-BORDER DATA FLOWS


Transfer of data to other state or an international organization is allowed according to international treaties and agreements signed by Georgia and also in cases established in the Law of Georgia on Personal Data Protection. In the reporting period the Inspector's Office studied several drafts of international treaties and agreements. For this purpose of data security relevant agencies were provided with recommendations and suggestions to include specific provisions in the documents.

In 2016 the Personal Data Protection Inspector's Office received 6 applications requesting permission to transfer data to another state according to the rules established in the law. The applications mainly concerned the transfer of the personal data related to customers of organization or






employees abroad. From submitted applications only two requests were partially satisfied by granting a permission to transfer specific categories of data.



One of the applicants asked a permission to transfer data related to the employees and job candidates to the founding organization, which was located in Turkey. According to the application, a decision to appoint a candidate was made jointly, both by the organization issuing data and the founding organization (data recipient). Correspondingly, it was necessary to transfer data concerning the candidates for positions. As for the transfer of data concerning the organization's employees, their data was automatically accessible to the foundation organization as the information was stored in the human resources management system. The organization intended to transfer different types of information, including the date of marriage, knowledge of native and foreign languages, work experience, and disability status. Despite the fact that according to the application and attached documents it was clear that the data security guarantees and the consent were in place, the organization did not manage to justify what kind of legitimate and clearly defined objectives were served by transferring certain types of data (e.g. data concerning the employee's health, marital status, date of marriage). Correspondingly, the application was satisfied partially and the organization was allowed to transfer only specific categories of data.





In several cases the organizations were refused to transfer personal data, because submitted documentation did not include information about the measures taken for data security during data transfer. In some case the submitted information and documents were not sufficient to assess advisability of transferring data abroad.


EDUCATIONAL AND AWARENESS-RAISING ACTIVITIES

For three years of existence the Office of the Personal Data Protection Inspector acquired citizens' and partners' trust and certain visibility in the society. At the beginning of the next three-year cycle the Office is planning to further intensify its work aimed at public awareness-rising. In the 2017-2021 institutional development strategy developed by the Inspector with the support of the European Union and the United Nations Development Program, public awareness-raising is one of the four strategic goals, while developing the culture of respect to privacy in the society is a part of the Office's mission.

The Office has planned and implemented several projects, events, and activities aimed at raise public awareness about the importance of personal data and data protection mechanisms. For this purpose the Office applied alternative, diverse, and modern channels of communication, digital and interactive forms, traditional and new media, multimedia platforms, and educational activities.

The awareness-raising campaign specifically targeted students and university professors to raise their interest in the topic of personal data protection. In 2016 the Inspector's Office regularly held public lectures at various universities, attracting more than 350 students.






The Office also carried out data protection weekends for lecturers and academic staff to support introduction of the academic discipline of personal data protection within the framework of the UN and EU joint program Human Rights for All. Fifty professors and teachers from Georgian Universities took part in the weekends. “The Personal Data Protection Hour”, including a public lecture, discussion, and a quiz was held at the state and private universities. The event was accompanied by posting an information poster and photo shooting. Informational materials were distributed among citizens at Rustavi, Tbilisi, Kutaisi, Gori, Telavi, and Batumi Service Agencies.

In 2016 the Inspector’s Office carried out 31 trainings for more than 800 employees of public and private organizations with an aim to support implementation of the legislation and practice and high standards of personal data protection. The trainings were carried out for the representatives of the Central Election Commission, Tbilisi Mayor’s Office, Ministry of Internal Affairs, Georgian Bar Association, Ministry of Internally Displaced Persons From Occupied Territories, Accommodation and Refugees, and other agencies, the court staff, principals of Tbilisi-based kindergartens etc. Also, the Office of the Personal Data Protection Inspector organized trainings for the representatives of small and medium businesses and other interested citizens on the monthly basis.

In 2016 the Office of the Personal Data Protection Inspector still prioritized provision of comprehensive information to media on the topic of personal data protection and activities of the Inspector’s Office. This time regional media outlets were targeted. Thirty journalists from regional media outlets were trained.

In partnership with the European Council the Office has started developing the guiding principles for media the primary purpose of which is to






encourage balanced while reporting on citizens' personal lives. The guidelines are developed with the engagement of the European Council experts and representatives of local media.

The Inspector's Office closely partnered with the judiciary; a memorandum was signed between the Office and the High Council of Justice to develop a curriculum on the topic of personal data protection. The Office was also engaged in the Supreme Court of Georgia Working Group, the purpose of which was to develop a uniform standard on publishing court decisions.

In 2016 in addition to meetings and educational activities the Inspector's Office actively used traditional and new media and multimedia platforms of communication for public awareness-raising purposes. A new column "It is interesting" was added to the website where multimedia materials on the importance of personal data protection provided in easily comprehensible and simple way are uploaded. The Facebook page got more active too, the number of likes increased by 30% compared to 2015 and total access exceeded half a million. The Facebook page was actively used to provide consultations to citizens. In the reporting period more than 1000 consultations were provided.

For the public awareness-raising purposes the Inspector's Office regularly updated the news section of the website; published monthly statistics. At the end of 2016 the Office developed a video summary of annual statistics and circulated it in social media. The Personal Data Protection Inspector's work was covered on television, internet and print media. From September to January the program Radio City had a weekly insert on the topic of personal data protection.





In 2016 the Inspector's Office actively issued sectoral and thematic recommendations on the issues of personal data protection. In 2016 the Office developed and published recommendations for schools and parents concerning protection of student's personal data, as well as recommendations concerning online shopping security, data processing in health sector, and protection from fraudulent internet applications. Videos were created on the topic of personal data protection in pre-election period and direct marketing. An interactive test was developed to assess internet security.

The mobile application "inspect 2" is working in the testing mode. The purpose of the application is to allow citizens easily and quickly notify the Inspector on violation by mobile phone.

In 2016 the Inspector's Office actively participated in various events dedicated to the personal data protection and organized by public or private institutions. The Inspector took part in Tbilisi Internet Forum in discussion titled "Internet and Personal Data Protection". The Deputy Inspector was engaged in the training of media representatives organized by the Charter of Journalist Ethics. The representative of Inspector's Office participated in the conference on the topic of personal data protection organized by the Mgalobslishvili, Kipiani, and Dzidziguri Law Firm.

On July 7 2016 the Personal Data Protection Inspector organized a roundtable discussion involving representatives of civil society and international organizations with the support of the European Union and the United Nations Development Program. The meeting summed up the work of the Inspector's Office over the period of three years, future plans were also discussed. For this event the Inspector's Office developed a document - fact sheet - reflecting results of the three-year work.



On April 14, 2016 the Inspector's Office presented the draft amendments to the Law of Georgia on Personal Data Protection and the opinion of the European Council experts concerning this draft to the partner public institutions, nongovernmental organizations, representatives of media and international organizations. The presentation aimed to provide information and receive feedback from the partner organizations.


The Office of Personal Data Protection inspector hosted reception dedicated to the International Day of Personal Data Protection. The reception was organized with the support of the European Union and the International Centre for Migration Policy Development Office in Georgia. Representatives of the legislative and executive authorities of Georgia, public and private sector organizations, NGOs and international organizations, as well as diplomatic missions in Georgia were invited to the reception. The event included an award ceremony for winners of the competition of photos/videos/posters concurs organized by the Personal Data Protection Inspector's Office.

INTERNATIONAL RELATIONS

One of the important directions of the Inspector's work is the interaction with international organizations and supervisory bodies of other states in the area of personal data protection. Establishing high standards of personal data protection requires sharing of international practices, observing global events in the area of data protection and participation in international processes.

In 2016 the Office of the Personal Data Protection Inspector still actively managed international relations. It was engaged in international networks and regularly updated foreign colleagues about the Office's progress and achievements.





The Personal Data Protection Inspector was actively engaged in modernization of the text of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). In 2016 the Inspector was elected as a member of the Convention 108 Consulting Bureau (T-PD).

The Inspector's Office is a member of numerous international networks and conferences related to the personal data protection. The Office representatives took part in the International Conference of Data Protection and Privacy Commissioners, the 18th Meeting of Central and Eastern Europe Data Protection Authorities, Spring Conference of European Data Protection Authorities, and the Berlin Group meetings. The representatives of the Inspector's Office presented information on the state and specifics of data protection in Georgia, as well as on practice and achievements of the Inspector's Office at the international level

In 2016 representatives of the The United Kingdom's Information Commissioner's Office (ICO) visited the Office of the Personal Data Protection Inspector within the framework of the UK-Georgia Reform Assistance program supported by PMCG and PwC. The Personal Data Protection Inspector actively participated in the National Internet Governance Forum held on December 2016 as a co-organizer. The office representatives also took part in the regional conference concerning access to public information organized by the European Council.

On December 14-15, 2016 the Inspector's Office hosted the first regional conference on personal data protection in Eastern Partnership countries. The conference was held within the framework of the European Council and the European Union joint project. Representatives of the personal data protection supervisory bodies and other responsible authorities,



as well as the European Council experts participated in the Conference. During the conference the experience of different states was shared, participants exchanged views on personal data protection issues and set plans for future partnership with the European Council.

In 2016 bilateral partnerships with supervisory bodies of other states were initiated and developed. The Office of the Personal Data Protection Inspector hosted colleagues from Moldova and Armenia within the scope of the study visit. The guests received information about the Office's practice, Georgian data protection legislation and system. A partnership memorandum was signed with the National Center for Personal Data Protection of Moldova. In addition, the Inspector was invited to Armenia for experience-sharing purposes. Inspector presented to the colleagues the reforms taking place in Georgia, major directions of the work of the Inspector's Office, and the role of the Office in Georgia's EU integration process.

STRATEGY AND ACTION PLAN OF THE INSPECTOR'S OFFICE

As a part of the UN and European Union joint program Human Rights for All, consulting company "GEPRA", developed the 2017-2021 institutional development strategy and the 2017-2018 action plan for the Office of the Personal Data Protection Inspector. In this process the mission, vision, values, strategic goals and respective objectives were defined. According to the strategy, in 2017-2020 the main goals of the Office is to activate work in major areas and increase effectiveness of the Agency through organizational development, also to promote public awareness and further develop strategic partnerships. The finalized strategy and action plan were introduced to the public and partner organizations at a public presentation.



REGISTER OF THE FILING SYSTEM CATALOGUES

The Article 19 of the Law of Georgia on Personal Data Protection obliges data controllers to keep a filing system catalogue for each filing system (data base, where data are organized and accessible according to specific criteria); establishes the types of information to be included in the catalogue and requires a data processing organization to notify the Inspector before creating a new filing system, adding new data categories or/and amending the information. The Inspector maintains a register of filing system catalogues. The information included in the register is public and the Inspector ensures its publication according to the appropriate rules.

In 2015 the Office of the Personal Data Protection Inspector developed an electronic register of the filing system catalogues. In 2014-2015 the Office digitalized about 5000 filing system catalogues provided by private or public data controllers.

In addition, in 2016 the Personal Data Protection Inspector issued the Order Approving the Rule for Notification of the Personal Data Protection Inspector about Maintenance of Filing System Catalogues and Publication of Filing System Catalogues, according to which filing system catalogues can be submitted only in electronic form through the electronic register of filing system catalogues. The Order simplified provision of electronic system catalogues to the Inspector, as well as the update of submitted filing system catalogues by data controllers. The electronic register of filing system catalogues also allows interested individuals to receive information about the categories of data processed by public and private organizations.





**TBILISI, N.VACHNADZE STR .7
[+995 32] 2 42 1000**

**office@pdp.ge
www.personaldata.ge
FB/DPAGeorgiaOfficial**



**Office of the Personal Data
Protection Inspector**