

# **REPORT ON THE STATE OF PERSONAL DATA PROTECTION AND ACTIVITIES OF THE INSPECTOR 2017**





# CONTENTS

4

INTRODUCTION

7

DATA PROCESSING IN PUBLIC SECTOR

29

DATA PROCESSING BY LAW ENFORCEMENT AGENCIES

51

DATA PROCESSING IN PRIVATE SECTOR

73

VIDEO SURVEILLANCE

89

DIRECT MARKETING

97

RAISING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES



## INTRODUCTION

Detected violations and the results of subsequent measures, problematic issues and the ways of addressing them, positive dynamics and existing challenges – the fifth Annual Report of the Office of the Personal Data Protection Inspector of Georgia summarises the state of personal data protection in the country and the activities carried out by the Inspector’s Office in 2017. The statistical data and the cases presented in the document reflect the ongoing changes and current tendencies not only throughout 2017, but also highlight the trends of the last 5 years.

In comparison with 2016, in 2017 the number of inspections and detected violations, as well as the number of citizens’ complaints and delivered consultations, increased. As a result of 240 complaints from citizens and 114 conducted inspections, the Office studied 385 cases of data processing in public and private organisations. In 2017, 274 administrative offences were revealed, in 145 cases, organisations were fined; 53 warnings were issued, in 76 cases the sanctions were not imposed due to expiration of the statutory limitation period of two months. In addition, 270 mandatory instructions and recommendations were issued. 11 cases were referred to relevant agencies for response and investigation, including, due to the presence of elements of crime.

Compared to the previous years, organisations improved identification of legal grounds for data processing and progress is notable in terms of determining



the period of data retention. The awareness of organizations in public sector as well as in large businesses regarding personal data protection has also increased. The decrease of the number of violations by the public entities is also noteworthy while the same number increased in private sector. Importantly, citizens were more active: half of the overall number of consultations, which amounted to more than 4800, were delivered to citizens.

The Inspector continued cooperation with the Parliament of Georgia, the Government of Georgia, ministries and Legal Entities of Public Law, the National Bank of Georgia and other regulatory bodies to enhance the standards of data protection in legislation and day-to-day activities. During 2017, the Inspector's Office examined more than 30 drafts of international agreements and treaties, prepared opinions and recommendations on various legislative acts.

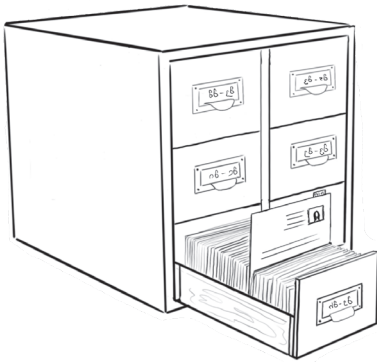
The Inspector's Office worked actively to raise public awareness through a wide variety of modern channels of communication, interactive multimedia platforms and educational activities. The Office carried out numerous informational meetings, events and campaigns, new online platform was created; with the assistance of the European Union and the United Nations Development Programme, public relations strategy was also elaborated and the Office started working on a new website, which will be accessible for the persons with disabilities.

The Inspector's Office was actively engaged in sharing the best international practices, as well as sharing Georgian experience and successful projects with international data protection community. In 2017 the Inspector's Office hosted the 19th Meeting of the Central and Eastern European Data Protection Authorities (CEEDPA), marking the first high-level meeting on personal data protection in Georgia.

The Inspector's Office is still actively involved in fulfilling Georgia's international obligations, including the Association Agenda between Georgia and the European Union. The Progress Report of the European Commission on Implementation of the EU-Georgia Association Action Plan, published by the end of 2017, underlined that "the Independent Data Protection Supervisory Authority continues to function effectively".



# DATA PROCESSING IN PUBLIC SECTOR



In order to achieve their statutory objectives or to provide services to citizens, public entities process large amounts of personal data. A wide variety of databases are created and the information is regularly exchanged among the public bodies. In certain cases, private organisations have access to the data held by public bodies. Generally, public bodies process data based on law or for the purposes of fulfilling their obligations prescribed by legislation. In some cases, the law explicitly prescribes the legal grounds for accessing and transmission of data while in certain cases, data are processed, based on data subjects' consent or request to receive services.

Together with having the legal grounds for processing of data, public bodies should ensure that principles and safeguards of data processing are adequately protected: the bodies should identify legitimate purpose, volume of data and period of retention, ensure security of data, adequately inform public, let data subjects exercise their rights, etc. These principles altogether set the main safeguards to strike a fair balance between the right to privacy of citizens and the interests of organisations, promotes accessibility of public services, improvement of the quality of services and reliability of public institutions.



Within the reporting period, through inspections and citizens' complaints, the Inspector's Office studied 115 cases of data processing in public entities including collection, usage, disclosure and transmission of data to the third parties. In the process of review of citizens' complaints and inspections, 38 cases of data processing by the ministries and legal entities of public law (except law-enforcement institutions), as well as courts, election administration, local self-government were studied. In 2017, the Inspector's Office delivered more than 900 written and verbal consultations to the public institutions, that led to adequate compliance with personal data protection legislation and prevention of potential violations.

As a result of complaints and inspections, the Inspector examined 115 cases of data processing by public bodies. More than 900 written and verbal consultations were delivered to public entities.

AS A RESULT OF COMPLAINTS AND INSPECTIONS, THE INSPECTOR EXAMINED

**115** CASES OF DATA PROCESSING BY PUBLIC BODIES.

**900+**

WRITTEN AND VERBAL CONSULTATIONS WERE DELIVERED TO PUBLIC ENTITIES.

It is important to underline that compared to previous years, the practice of determining the grounds for processing personal data by the public entities has improved and the progress is visible with regard to determination of the extent of data to be processed, as well as the period of data retention. The awareness regarding the protection of personal data of public entities has been raised, although some problems and violations were still revealed. The Report exposes the violations, the problems and the specific examples identified in the activities of public institutions throughout 2017, the analysis of which proves the importance of enhancement of data protection standards in public institutions.

## **DATABASES**

Public entities process large volumes of personal data of natural persons that are gathered in different databases for various purposes, such as administering the unified registry of citizens, administrative penalties, social assistance programs, healthcare system, education system. Due to the volume of data stored in databases, there may arise the necessity to use the data for the purpose other than the initial purpose of their collection, that is why, other public institutions or private entities may be granted access to these databases.

Frequently, employees of these entities have access to these databases and information about the citizens. That is why, each employee with the access to the database, should be registered in the system as an individual user with individual login and password/digital pass. The access levels must be pre-determined and each activity in the system should be recorded. Due to the risks of unauthorized use of the data or abuse of access to the databases, organisations must pay special attention to securing the information stored in the databases and effectively monitor their use.






## DATABASE OF ADMINISTRATIVE OFFENCES

Within the reporting period, a citizen lodged a complaint to the Personal Data Protection Inspector and indicated that the information regarding the imposition of a fine for administrative offence (name, last name, ID number, vehicle registration number, date of imposition of a fine, amount of fine, location of a scene and other data related to the administrative violation) was unlawfully publicized through a news web-portal. The publicized documents enabled to assume that the data was collected through the program interface used by one of the financial organizations/ payment service providers.

Under the legislation, the Ministry of Internal Affairs of Georgia is in charge of maintaining the unified database of registration of administrative offences. The review of the complaint revealed the following:






various financial organisations have access to the data stored in the unified database of administrative offences (name and last name, ID number, vehicle registration number, type of offence, date of imposition of a fine, amount of fine, etc.) in order to allow citizens to pay imposed administrative fines through their services;

- 
-  Prior to 1 August 2017, the cases of access to the data stored in the database by the financial organisations 2017 were not recorded. Neither was the Ministry regularly monitoring the lawfulness of access to the database;
  -  While reviewing the complaint, the Ministry started to monitor and register each access by financial organisations to the data stored in the database.

The review of the complaint also demonstrated that information about the imposition of administrative fines was accessible through the websites of these financial organisations through personal ID number only. Considering that the ID number is often publicly available (for example through the website of Public Registry), the information about administrative offences was easily obtainable. Upon the Inspector's decision, the Ministry of Internal Affairs was instructed to adopt appropriate organisational and technical measures in order to secure the data stored in the unified information database and to determine the necessary requisites for the financial organizations to gain access to the database and to search data.

Data controllers, that need to operate a database or grant access to the database to third parties, are required to determine:

-  persons authorised to have access to database and their access levels;
-  necessary requisites for the access to database in order to minimise risks of unauthorised access to the database;
-  mechanism for evaluation of lawfulness of access to database and its continuous monitoring.

## **DATABASE OF BORDER CROSSING**

Within the reporting period, a citizen lodged a complaint to the Personal Data Protection Inspector and indicated that LEPL “Revenue Service” without any legitimate grounds collected and used the information about him/her crossing the state border of Georgia. The review of the case revealed that the applicant was a CEO of an enterprise, which was the subject of tax inspection. Within the framework of this inspection, an employee of Revenue Service checked the information about border crossing through the relevant database of the Ministry of Internal Affairs. The Revenue Service claimed that checking the data was necessary in order to detect the location of the applicant and to timely deliver the tax notice to him/her as a representative of the taxpayer.

The rule of delivering documentation to the taxpayer is established by the Tax Code of Georgia and this rule remains the same whether the taxpayer’s



representative is in Georgia or not. Besides, the taxpayer had another representative as well, who received the tax notice in the end. Therefore, Revenue Service failed to prove the necessity of collecting the information about border crossing.

In the above case, LEPL Revenue Service was assigned to eradicate the problem and to process the data of the border crossing only when it is necessary to exercise its statutory obligation.

Data controllers, who need access to various databases to fulfil their obligations stipulated by law, should determine the extent of data to be accessed for this purpose. Utilizing databases shall be the necessary measure to achieve legitimate purpose not an effortless solution. Otherwise, the risk of disclosure, obtaining or unlawful use of the data stored by various institutions, will remain.

## **ID CARD DATABASE**

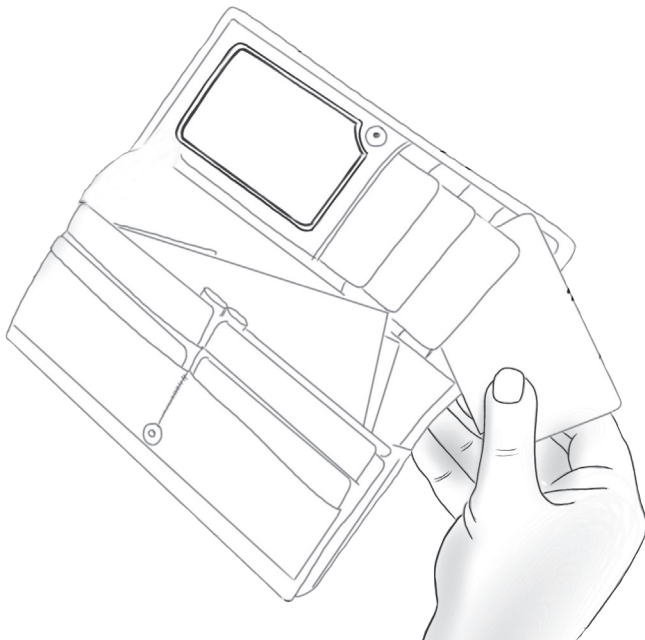
Identification of the purposes of access to database and determining the volume of accessed data still remains a challenge in public institutions.

Within the reporting period, one of the inspections revealed that a private company offered customers membership to the so-called loyalty system and the discount cards. A customer's consent to collect personal data from the database of LEPL Public Service


Development Agency was included in the agreement in order to provide this service and register the customers in the database.

After entering customers' ID numbers and the dates of birth into the system of the Agency, the company was able to access to the following data of a customer in real time: name and last name, father's name, place of birth, gender, citizenship, information about person's death, ID number, requisites of passport, registration address identifier, date of registration, the place of factual residence, photo, etc.

During the inspection, the company failed to prove the necessity to process customers' personal data of such volume and confirmed that only a part of the data was sufficient to issue a discount card. In addition, the Agency clarified that by the time of inspection technical means already made it possible to provide







only the necessary data to the company through applying relevant filters.

As a result, the Inspector's Office established that company received and the Agency disclosed the data to the extent that was inadequate and disproportionate to the purpose. Accordingly, the company was instructed to process customers' data to the extent deemed necessary to achieve legitimate purposes.

When it comes to processing the data stored in various databases, both the organisation that transfers the data and the recipient organisations, are required to determine the categories and the extent of data to prevent collection of larger volumes of data than necessary for achieving legitimate purposes. They are also required to ensure that these determined categories of data are adequate and proportionate of legitimate purposes.



## MAKING DATA PUBLIC AND ITS DISCLOSURE TO THIRD PARTIES

While sharing the personal data through the webpage or social networks of public entities, it is particularly important to respect the rules of data processing. The data become easily accessible for the unlimited group of people and the threat of the damages that may be inflicted on data subjects, increases significantly. At the same time, it is also important to strike a fair balance between the right to personal data protection and legitimate interests of public organizations.

In 2017 four citizens lodged a complaint to the Personal Data Protection Inspector. They claimed that their personal information was disclosed on the webpage of the Ministry of Environment and Natural Resources Protection of Georgia.

As a result of studying the case, it has been revealed that the photos of applicants, their names and information on illegal hunting was publicly available through the webpage and Facebook page of the Ministry, as well as the Facebook page of the Environmental Supervision Department of the Ministry.

In addition, it has been established that by the time of disclosure of the applicants' data, the court had not recognised the violation and nor had it ruled on imposition of administrative sanction. Therefore, the disclosed information contained inaccurate details as well.

The Inspector did not agree with the opinion of the Ministry and the Department that claimed that disclosing names and photos of applicants was necessary to prevent violation of environmental law, to fight against illegal hunting and to raise public awareness. In order to achieve these objectives, it was important to inform the society about the detected violations, though it could be done without revealing identities and disclosing photos of those involved in the incident.

PRIOR TO MAKING DATA PUBLIC, DATA CONTROLLERS ARE OBLIGED TO:



to make sure that there are relevant grounds for processing of data and data processing principles are protected;



to assess the necessity of disclosure of identification data and evaluate if it is possible to achieve the objectives through depersonalisation of data and by disseminating information without identifiers of a person;



To make sure the data is valid and accurate.

## **PROCESSING OF DATA BY A DATA PROCESSOR**

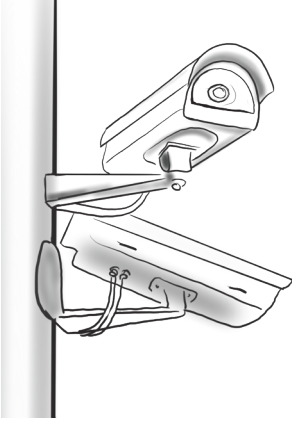
Oftentimes, on behalf of public entities or for their purposes, personal data are processed by data processors; for example, public entities designate postal service companies to deliver correspondence or conduct surveys through research companies. In these cases, public entities, as data controllers, are to a certain extent responsible for processing of data by a data processor.

As prescribed by law, while designating a data processor, organisations should elaborate an agreement or identify a legal act that will clarify regulations and limitations of processing. It is especially important to record all processing operations related to electronic data, including disclosure.



## **TBILISI CITY HALL**

Within the reporting period, the Office of the Inspector assessed the lawfulness of data processing through the street video surveillance system, carried out by Tbilisi City Hall and its data processor. The inspection revealed that the electronic system failed to register all the actions taken in relation to data. The system recorded only the information about login and logout of the users and the information about which camera had been accessed. However, the system failed to record by whom, through which camera, when and for what purpose the video recording was processed.

During the inspection, the data processor of Tbilisi City Hall activated the function of recording all processing activities in the system. According to the Inspector's decision, Tbilisi City Hall and the data processor were instructed to record all activities related to disclosure of personal data in compliance with legal provisions; also, a recommendation was issued to elaborate the written rules regarding the disclosure of video records containing personal data to the authorised third party(ies).



WHILE PROCESSING DATA THROUGH THE ELECTRONIC SYSTEMS, DATA CONTROLLER IS OBLIGED TO:




-  Ensure that all processing activities in relation to electronic personal data are recorded;
-  Assess risks and elaborate appropriate organisational and technical measures in order to safeguard data security.

## **NATIONAL BUREAU OF ENFORCEMENT**

In 2017, a citizen applied to the Personal Data Protection Inspector indicating that LEPL “National Bureau of Enforcement” sent him/her a letter regarding the loan taken from one of microfinance organisations. The letter was not sealed in an envelope enabling any person to read the content of the letter.

During the review of the complaint, it was revealed that LEPL “National Bureau of Enforcement” was delivering letters to recipients through a data processor – one of the postal service companies. The agreement between the Bureau and the company did not envisage the obligation of a postal service company to seal hybrid letters (a type of a letter that is received through the electronic means of communication and is printed as a hardcopy afterwards) in envelopes. After receiving a letter from the Personal Data Protection Inspectors’ Office, the LEPL ‘National Bureau of Enforcement” requested from a postal service company to seal letters in envelopes. In addition, the Bureau was assigned to clearly envisage in service contracts the obligations of data processor(s) with regard to personal data processing and to define tools to monitor fulfillment of these obligations.


WHILE PROCESSING THE DATA THROUGH DATA PROCESSORS, IT IS IMPORTANT THAT ORGANISATIONS:

-  Prior to processing, assess the risks of inappropriate data processing;
-  Specify the obligations of parties with regard to personal data processing through a written contract;
-  Monitor data processing by the data processor.



## DATA SUBJECT'S RIGHTS

In accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) the right of a data subject to know where, by whom and for which purpose his/her data are processed, the ways in which the data were collected, to whom his/her personal data were disclosed shall be fully realized. According to Georgian legislation, data subject can directly affect processing of his/her personal data; for instance, data subject is entitled to request an update, correction and deletion of personal data if they were inaccurate or processed unlawfully; he/she is entitled to request termination of processing of data obtained through consent.



The legislation establishes high standards for data controllers in public sector in order to ensure the protection of data subject's rights – a person has a right not only to request the information about the processing of his/her personal data, but also to consult his/her personal data kept at a public institution and obtain copies of the data free of charge.

Complaints reviewed and the consultations provided by the Inspector's Office throughout 2017, demonstrate that citizens' interest towards processing of their personal data has significantly increased. Cases when individuals request information from data controllers are frequent.

With respect to informing data subjects, it has been revealed within the reporting period that organisations fail to appropriately register the ways and means of collection of certain data; for instance, data subject failed to receive information regarding the collection of his/her telephone number despite the fact that he/she requested the information. In addition, it has been established that certain organisations do not register requests submitted by the citizens in verbal or electronic form. In such cases, exercising of a data subject's right depends on a good will of a relevant employee of the entity that increases the risk of disregarding citizen's request.

Along with the obligations of data controllers, the obligations of data subjects are also to be noted. The request of a data subject to receive information about him/her shall not be vague and shall objectively allow to seek appropriate information. For instance, in one case a citizen was requesting access to documents about him/her kept by a certain institution; however, the request did not contain information which would give the data controller a reasonable possibility to look for the documents.

In such circumstances it is important for data subjects to provide organisations with a clear request what information they are looking for specifically, in what form and to specify the documents they would like to receive. At the same time, data controllers should notify citizens about the circumstances obstructing access to data in due time and request clarification of information which is necessary to comply with a legitimate request of a data subject.

## **INTERNATIONAL TRANSFER**

Cooperation agreements in various fields between Georgia and other countries, investment projects implemented in Georgia, development of international trade relations increase the trans-border flow of personal data.

Within the reporting period the Inspector's Office reviewed more than 30 draft international treaties and agreements related to the fight against crime and cooperation with other states in different fields, that envisaged transfer of personal data. Based on the review of the drafts treaties, the Inspectors' office prepared a number of recommendations about the inclusion of conditions that will guarantee the protection of personal data transferred to another state.

The Agreement on Operational and Strategic Cooperation between the European Police Office and Georgia signed in April, 2017 facilitates the enhancement of sectorial cooperation with the European Union and its agencies in the process of Georgia's European integration, and is important with regard to transfer of data. The Office of the Personal Data Protection Inspector played a key role in the procedures to sign the treaty, especially with regard to evaluation of the state of personal data protection in



Georgia. Based on this agreement Georgia will be able to share crime-related information and personal data with Europol and law-enforcement authorities of the EU Member States through secure channels of communication.

In addition, in the reporting period the evaluation of the state of personal data protection in Georgia was carried out with the purpose of concluding an agreement with Eurojust (the European Union's Judicial Cooperation Unit). In May, 2017 the evaluation mission visited Georgia and the meetings were held in the Office of the Personal Data Protection Inspector as well. By the end of 2017, the protection of personal data in Georgia was evaluated positively and the steps were made to initiate the negotiation process for the agreement. Concluding cooperation agreement with Eurojust creates an important basis for the transfer/request of information, including personal data, between the relevant authorities in Georgia and in the EU Member States.



## LAW-MAKING ACTIVITIES

It is important to take into account the requirements of the personal data protection legislation when developing any regulations that are related to the processing of personal data in order to ensure protection of human rights and freedoms, including the right to privacy. In addition, it is necessary to regulate issues clearly, in order to prevent the risk of violating human rights due to ambiguity of provisions.

Within the reporting period comments and recommendations were provided on a number of laws and by-laws in order to bring them into compliance with the personal data protection legislation. Among them is the review, requested by LEPL Insurance State Supervision Service of Georgia, of the amendments made to the Resolution #36 of the Government of Georgia on “A Set of Measures to be taken for the Purpose of Transitioning to the Universal Healthcare System” issued on February 21, 2013. The regulation envisaged policies for requesting from insurance companies operating in Georgia relevant information about insured persons. The Service was recommended to determine the legitimate purpose of the collection and its extent.

Within the reporting period, upon the request of the Government of Georgia, relevant comments and recommendations were prepared with regard to the draft law of Georgia “on making amendments to the Law of Georgia on Protection of Personal Data”. The proposed amendments referred to the processing of special categories of data by the Ministry of Education and Science of Georgia and/or legal entities of public law under its umbrella. The Government was provided with suggestions regarding specifying

data controllers, forms and purposes of data processing, on extent of the data processing and measures to be taken in order to ensure data security.

At the request of the Parliament of Georgia and LEPL Revenue Service of Georgia comments and recommendation were prepared in relation to the draft laws introducing amendments to the following legislative acts: Law of Georgia on the Management of Lotteries, Gambling and other Prize Games; Law of Georgia on Gambling Taxation; Law of Georgia on Court Fees; Law of Georgia on Licence and Permit Fees; Code of Georgia on Administrative Offences and Administrative Procedure Code of Georgia. These amendments and changes were related to the creation of unified electronic registry containing personal data in the process of state regulation of lottery, gambling and prize gaming, defending legal interests of citizens and protection of customer's rights, as well as creation of database for the persons with gambling addiction and its future use.

Based on the request of the Ministry of Finance, comments and recommendations were prepared in relation to the draft law introducing amendments to the Law of Georgia on Accounting, Reporting and Auditing. The comments related to access of the Accounting, Reporting and Auditing Oversight Service to personal data stored in the central database of the Ministry of Internal Affairs of Georgia. The recommendation issued thereupon called for determining circumstances, form and frequency of collection of personal data from the central database of the Ministry of Internal Affairs in accordance with legitimate purpose of access to data.

In addition to these, the Inspector's Office reviewed draft laws on amendments and changes proposed by the Ministry of Internal Affairs in the following legislative acts: Law of Georgia on the Legal Status of Aliens and Stateless Persons; Law of Georgia on the Rules for Registering Citizens of Georgia and Aliens Residing in Georgia, for Issuing Identity (Residence) Cards and Passports of a Citizen of Georgia; Law of Georgia on Police; Code of Georgia on Administrative Offences; Administrative Procedure Code of Georgia; Law of Georgia on Labour Migration; Law of Georgia on Protection of Personal Data Protection; Law of Georgia on Higher Education. The Office issued recommendations regarding periodic update of data, on deletion of unnecessary data or/and storing it by means excluding identification of a person and on security matters (mechanisms of prevention of unauthorized access to data and indication of persons responsible for data security). Particular attention was paid to the forms of processing of foreigners' data by the police during immigration check, the issue of proportionality of data to be processed and the necessity of providing foreigners with all relevant information.

In consideration of the comments and recommendations of the Inspector's Office the levels of access to data and the volume of data to be processed were restricted. Appropriate organisational-technical mechanisms were created in order to ensure security of data and persons responsible for data security were defined. Legal provisions were specified in accordance with legitimate purposes of data processing, that significantly decreased the risks of disproportionate processing of data and arbitrary application of the regulation.



# DATA PROCESSING BY LAW ENFORCEMENT AGENCIES

**34**

**COMPLAINTS OF DEFENDANTS  
AND CONVICTS**

**28**

**REVIEWS OF LAWFULNESS OF DATA  
PROCESSING BY THE MINISTRY OF  
INTERNAL AFFAIRS**

**8**

**REVIEWS OF LAWFULNESS OF DATA  
PROCESSING BY THE PROSECUTOR'S  
OFFICE**

**5**

**REVIEWS OF LAWFULNESS OF DATA  
PROCESSING BY THE STATE SECURITY  
SERVICE OF GEORGIA AND  
OPERATIVE-TECHNICAL AGENCY**

**2**

**REVIEWS OF LAWFULNESS OF DATA  
PROCESSING BY THE INVESTIGATION  
SERVICE OF THE MINISTRY OF FINANCE**





Mostly, processing of personal data by the law enforcement agencies is carried out for the purposes of police and preventive measures, investigation of a crime, criminal prosecution and execution of criminal penalties. In order to exercise the functions vested upon it, law-enforcement agency is authorized to collect and process data from open as well as closed sources, directly from a data subject or from a third party. Accordingly, to strike a fair balance between the right to privacy and the interest of public security, a particular significance is assigned to thorough compliance with the requirements of law during data processing by the law enforcement authorities.

Throughout the reporting period, within the framework of complaints handling and inspections the Inspector's Office studied lawfulness of data processing by law-enforcement authorities for various purposes in 77 cases. Out of 77 cases 34 were complaints submitted by defendants and convicts. In addition, the inspection of juvenile rehabilitation centre was carried out. In 28 cases the Office reviewed lawfulness of data processing by the Ministry of Internal Affairs within the framework of complaints handling and inspections. In 8 cases the Office reviewed lawfulness of data processing by the Prosecutor's Office, in 5 cases by the State Security Service of Georgia and LEPL Operative-Technical Agency and in 2 cases - by the Investigation Service of the Ministry of Finance based on complaints.

In addition to addressing violations (the organisations were fined in 19 cases; warnings were issued in 4 cases and in 23 cases the liability was not imposed due to expiration of the statute of limitations) the law enforcement agencies were given relevant assignments and recommendations to eliminate shortcomings, that will ensure improve-

ment of quality of data protection in this sector. Furthermore, the Inspector's Office provided the law enforcement agencies with more than 130 written and verbal consultations for the purpose of advancing data processing standards. On the basis of requests submitted by various entities, the Office prepared conclusions and recommendations on drafts of a number of laws and normative acts.

Compared to the previous reporting period, in 2017 the number of facts of collecting computer data from private companies for investigation purposes without a prosecutor's resolution or a court ruling have decreased. In the second half of 2017 the number of complaints from defendants/convicts regarding the facts of data processing through video surveillance and while exercising the right to a phone call at the penitentiary institution have also decreased, which in turn highlights the positive effect of legislative changes and measures taken by the Ministry of Corrections of Georgia.

## **PROCESSING OF VIDEO SURVEILLANCE CAMERA RECORDINGS FOR INVESTIGATION PURPOSES**

Visual examination and collection of video recordings from video surveillance systems for investigation purposes without a ruling/resolution still remain to be outstanding issues. However, the number of violations related to unlawful collection of computer data has significantly decreased compared to the previous year. The Office has revealed a number of cases when data were processed to inadequate and disproportionate extent within the framework of investigative actions related to collection of video recordings.



Following the complaint of a certain citizen, it was established that at the beginning of 2017 the employees of the Ministry of Internal Affairs carried out a number of actions prior to the commencement of the investigative action related to the collection of video recordings from the video surveillance system envisaged by the prosecutor's resolution. In particular, they showed up at the home of a founder of a micro-finance organisation and requested to hand over recordings of the organisation's video surveillance system without presenting a court ruling or a prosecutor's resolution. The applicant requested relevant documents from the employees of the Ministry and clarified that the recordings would be handed over only after the relevant documents would be presented. The applicant was arrested due to the alleged failure to obey the legitimate request of a police officer and was transferred from his house to a police department.

In addition to this, the employees of the law-enforcement body visited the branch of the micro-finance organisation in question where they examined the recordings from company's video surveillance system stored in the computer database and took photos of certain sections with a cell phone.

As a result of one of the inspections conducted in 2017 it has been revealed that for the purpose of criminal case investigation investigator examined/seized the DVR device containing a video recording based solely on the written consent of the owner of the property. In the given case the DVR device transferred by the company to the law-enforcement agency contained more recordings than necessary to achieve the legitimate purpose.

Despite the fact that in given cases the collection of video recording served legitimate purpose and in one case even the appropriate resolution of a prosecutor was present, thorough adherence to the legislative requirements while conducting investigative activities and duly presenting a ruling/resolution on the collection of computer data, are of great importance.

## **PHOTO AND VIDEO RECORDING AS PART OF PREVENTIVE MEASURES**

Within the reporting period the Inspector's Office studied several facts of photo and video recording by the Ministry of Internal Affairs for the purposes of preventive measures.

Based on the information disseminated on social network, the Inspector studied the fact of video recording of a citizen by the employees of the Ministry of Internal Affairs during the process of preventive measures. The inspection revealed that the law enforcement officers stopped the citizen for a visual check-up and recorded the process on a personal cell phone. According to the clarifications of the Ministry, the purpose of video recording was an attempt to prevent unlawful conduct on behalf of the citizen, averting false accusations and discrediting the employees. However, the disseminated video footage depicted that the citizen clearly and repeatedly showed his readiness to cooperate



with the police, expressed consent to undergo a visual check-up and alcohol test and even the willingness to be transferred to the police office. It is important to underline that the disseminated video recording did not demonstrate any offence, failure to obey to the legitimate requests of the police, their verbal abuse or any other form of unlawful behaviour on behalf of the citizen. The video recording ended with its participants saying goodbyes to each other and the police returning the ID card to the citizen. The police officer did not delete the video from his personal phone and it was not transferred to the computer database of the Ministry. Accordingly, the video was not secured appropriately from accidental or unlawful disclosure, from any form of its illegal use or loss.

Based on a complaint of a citizen, the Inspector studied the fact of taking a photo of the citizen by the employees of the Ministry of Internal Affairs with a personal cell phone for the purpose of “identification”.



IT IS IMPORTANT TO UNDERLINE THAT THE PROCESS OF IDENTIFICATION OF A PERSON BY A PHOTO IS NOT PRECISELY REGULATED, WHICH ESTABLISHES INCOHERENT PRACTICE AND CREATES THE RISK FOR UNLAWFUL DATA PROCESSING IN VIOLATION OF THE PRINCIPLES ESTABLISHED BY THE LAW. THE USE OF VIDEO RECORDING AND DIFFERENT MEANS OF INFORMATION EXCHANGE AND THE USE OF PERSONAL CELL PHONE BY THE EMPLOYEES OF THE MINISTRY ARE RISKY WITH REGARDS TO ACCIDENTAL OR UNLAWFUL USE OF DATA.

In light of the aforesaid, the Ministry was given a recommendation to determine the rules of identification of a person by a photo as part of preventive measures and verifying the information in the database which will ensure the lawfulness of data processing. Herewith, in consideration of data security, it is necessary to evaluate appropriateness of the use of employees' personal telephones and means of information exchange for the enforcement of this measure. If necessary appropriate organisational–technical measures shall be taken to strengthen security measures in data processing.

## **ELECTRONIC SURVEILLANCE OF DEFENDANTS/CONVICTS**

Based on numerous complaints filed by convicts, within the reporting period the Inspector's Office studied the lawfulness of electronic surveillance of defendants/convicts in the cells of high risk prison facilities.

Article 54 of the Imprisonment Code of Georgia authorizes a penitentiary institution to conduct surveillance and control by electronic means in order to ensure security of defendants/convicts or other persons, to prevent suicide, self-injury, violence, property damage, and to avert other crimes and offences. At the same time, the administration of the penitentiary institution shall warn the defendant/convicts in writing and it shall specify electronic means and purposes of monitoring the defendant/convict.

While studying various issues throughout the reporting period it has been revealed that in some cases the defendants/convicts were informed by the administration of penitentiary institution regarding the electronic surveillance verbally only. Moreover, written warnings were drafted only several days after the commencement of surveillance. Apart from this, in majority of cases the document did not contain appropriate information regarding the grounds and purpose of electronic surveillance.

In order to ensure lawfulness of data processing as well as to provide appropriate information to the data subject it is necessary not only to inform data subject (convict) regarding the commencement of surveillance but also to clarify what type of electronic means are used and what is the purpose of surveillance. It is also important that the above mentioned warning is immediately attested by the document foreseen by Georgian legislation. On the one hand it will be relevant evidence in the monitoring of lawfulness of data processing, attesting that the Ministry warned the data subject, and on the other hand defendant/convict will have comprehensive information regarding the purpose and grounds of surveillance from the outset. Relevant instructions were issued to the Ministry of Corrections of Georgia.


It is important to note that by virtue of the amendments and changes to the Imprisonment Code, adopted on June 1, 2017, special rule of electronic monitoring of convicts in the cells of high risk prison facilities was approved. The Ministry of Corrections is working on establishing standardized procedures of informing convicts regarding the electronic monitoring at the special risk prison facilities.

## **ACCESS TO DATA OF THE CENTRAL INFORMATION BANK AND SECURITY OF DATA**

In order to perform the obligations vested upon it by the legislation, the Ministry of Internal Affairs of Georgia has a central information bank, where personal data (including special categories of data) is accessible. Accordingly, it is important to provide access to the information resources of the central information bank in each particular case based on the legal grounds and principles to avoid damaging legitimate interests of data subject with unauthorized access.

Despite the fact that compared to the previous years the number of unauthorized and unreasonable access by the Ministry's employees to data stored at the central information bank has decreased due to the work performed by the Inspector's Office and measures taken by the Ministry of Internal Affairs, in 2017 the Personal Data Protection Inspector revealed eight cases of unreasoned access to citizens' personal data in the information resources of the central information bank with the use of a digital pass (the so-called DIGIPASS).





It is important to underline that the logs of the central information bank of the Ministry do not include information regarding the data processed during the access to the system. Accordingly, it is important for the Ministry to ensure registering the data processed during the access to the central data banks, as well as to provide permanent and continuous control of the use of information databases.

It has been established during the inspection of the rehabilitation centre for juveniles that the case file containing individual plan that was kept in hard copies did not include actions related to the disclosure of personal data and/ or changes thereto. The Ministry of Corrections of Georgia was instructed to take appropriate measures to resolve this matter.



ACCORDING TO THE LAW, THE MEASURES TAKEN TO ENSURE SECURITY OF DATA SHOULD BE ADEQUATE AND PROPORTIONATE TO THE RISKS. THE CATEGORY AND CONTENT OF PROCESSED DATA, NUMBER OF EMPLOYEES AND QUALITY OF THEIR ACCESS TO DATA, THIRD PERSONS AUTHORIZED TO ACCESS DATABASE AND NUMBER OF SUCH PERSONS SHALL BE TAKEN INTO THE ACCOUNT WHEN EVALUATING RISKS.

## **ACCURACY AND VALIDITY OF DATA PROCESSING**

In order to ensure lawfulness of data processing it is necessary for the organisation to guarantee accuracy and validity of the processed data. Sources of personal data are important in this regard. Data controller should take all necessary measures to check the reliability of all collected information. The authenticity of data processed for the purpose of national security, public security and public order are especially significant, because processing of inaccurate data might cause irreversible damage to data subject and violate his/her rights.

Within the reporting period the Inspector established that a photo of one of the citizens included in the criminal case file was mistakenly regarded as the visual image of the defendant. The photo was transferred to the Prosecutor's Office which in turn requested Interpol National Bureau to issue a Red Notice for a wanted person by national authorities and submitted the photo as a visual image of the wanted person.



It is important to note that the Ministry of Internal Affairs corrected the mistake in the process of handling the complaint, removed the photo from the wanted person's file and submitted the information on the error to the Prosecutor's Office of Georgia. Finally, Interpol National Bureau made a change in the international search notice and Interpol General Secretariat ensured changes in a timely manner.

In order for a law-enforcement authority to transfer personal data internationally, it is required to carry out the transfer within the framework of an international treaty/agreement, to evaluate during the transfer the legitimate purpose of data processing, accuracy and validity of the data to be transferred and proportionality of its volume.

## INFORMING DATA SUBJECTS


The Constitution of Georgia and the Law of Georgia on Personal Data Protection guarantee the right of a citizen to request information regarding the processing of his/her personal data from any public organisation, including law enforcement authorities. In particular, the right to know what was the purpose and legal ground of data processing, how it was collected and to whom the data was disclosed.



THIS RIGHT OF A DATA SUBJECT IS NOT ABSOLUTE. IT CAN BE LIMITED FOR THE PURPOSES OF PUBLIC SECURITY, PROTECTION OF OTHERS' RIGHTS AND FREEDOMS, DETECTION, INVESTIGATION AND PREVENTION OF A CRIME. HOWEVER, IT NEEDS TO BE TAKEN INTO ACCOUNT THAT THE RIGHTS OF A DATA SUBJECT SHALL BE LIMITED ONLY TO THE EXTENT NECESSARY TO ACHIEVE THE PURPOSE AND IN A MANNER THAT IS NOT DAMAGING FOR THE PURPOSE OF RESTRICTION OF THE RIGHT.

In 2017 positive tendencies were revealed with regard to informing data subjects by law-enforcement agencies. In particular, in the majority of cases law enforcement agencies disclosed the information at the request of data subjects in accordance with the rules and timeframes established by the legislation. However, several cases of violation of deadlines and providing incomplete information were revealed based on the citizens' complaints.

Within the reporting period, based on the citizens' complaints, the Inspector



examined the lawfulness of informing data subject by the Prosecutor's Office of Georgia, State Security Service of Georgia and the Ministry of Internal Affairs of Georgia. In result, the fact of providing incomplete information or/and delay with submitting requested information to data subject were revealed.

In order for a data subject to exercise the right to receive information, it is necessary for institutions to take such organisational and technical measures that ensure complete and timely submission of requested information to data subject unless it threatens national security and the interests of public safety, detection, investigation and prevention of crime, protection of rights and freedoms of others. In case it is impossible to disclose requested information within the established timeframe due to a need to search for data in another institution or structural unit, its significant size, necessity to process unlinked documents or any other reason, the public entity is obliged to inform data subject regarding these reasons. Even if the law enforcement agency does not process data about the data subject or does not store the requested document, it shall inform data subject regarding the fact.

## **RIGHT OF DEFENDANTS AND CONVICTS TO A TELEPHONE CONVERSATION**

In 2017 the Personal Data Protection Inspector also examined the lawfulness of personal data processing during exercising by defendants and convicts of a right to a telephone conversation in the high risk prison facility.

While examining complaints, it has been revealed that telephone in the high




risk prison facility was installed in the duty room of the facility where the control of a defendant's and convicted person's telephone conversation was performed through a visual monitoring by an employee of the facility, who was present in the room during the call.

It was revealed that even though the purpose of an employee at the duty room was not eavesdropping phone conversations of a defendant and convicted person and processing of data in this manner, the room setting and space allowed the employees to listen to the content of defendants'/convicts' personal telephone conversation, which created a risk of violating confidentiality of phone conversations. Due to the reason that the presence of a prison employee during a phone conversation served the only purpose of ensuring security, the Ministry of Corrections agreed with the Inspector's standpoint and altered the setting of the room for phone conversations so that the intrusion into confidentiality of phone conversations will be avoided from now on.

## **OVERSIGHT OF COVERT INVESTIGATIVE ACTIVITIES**

During covert investigative activities it is essential to strike a fair balance between the interest to investigate a crime and inviolability of an individual's personal space. As a result of the amendments to the Criminal Procedure Code of Georgia, the regulation of technical infrastructure for covert electronic surveillance has been changed. Despite the fact that since March 30, 2017 there is no need to receive a prior consent of Inspector for the commencement of interception of telephone communication, LEPL Operative Technical



Agency receives the right to initiate the covert investigative activity only after the delivery of an electronic copy of a ruling or a resolution to the Inspector is confirmed.

In light of the above-mentioned changes, starting from April, 2017, Inspector's Office permanently monitors the ongoing process. Based on the analysis of revealed shortcomings and complaints submitted to the Inspector, the Office applies the measures determined by the legislation.

Within the reporting period, out of all investigative activities the majority of granted motions were related to requesting computer data, the investigative activity envisaged under Article 136 of the Criminal Procedure Code of Georgia. The least motioned investigative action was related to real time collection of internet traffic data. The number of motions on retrieval and recording of information from communication channels has decreased compared to the previous years.

In addition, the number of prosecutor's resolutions submitted to the Inspector requesting initiation of investigative activity to collect computer data due to urgent necessity has decreased and computer data is usually obtained based on a court ruling.

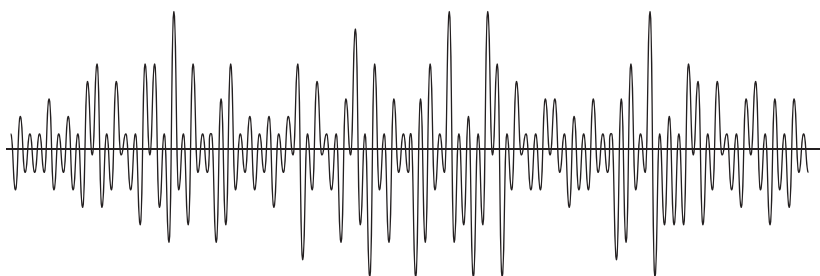
As for the statistical data regarding interception of telephone communications, the Inspector's Office received 699 court rulings on commencement, continuation, approval, partial granting and rejection of interception of telephone communications.


It is important to note that the number of documents received in 2017 regarding initiation of interception of telephone communications due to urgent necessity by the prosecutor's resolution brings us to the conclusion that the number of such covert investigative actions initiated/conducted in the absence

of a court ruling by the decision of a prosecutor has decreased compared to the previous years.

Up until March 31, 2017, the Personal Data Protection Inspector was authorized to supervise the covert investigative activity – interception of telephone communication by means of a two-stage electronic system through issuing electronic consent to conduct the covert investigative action.

In accordance with the legislation in force before March 31, 2017, the Inspector's Office did not issue consent for covert investigative action by means of a two-stage electronic system in 4 cases. After the legislative amendments of March 22, 2017, the Personal Data Protection Inspector was given the authority to suspend the process of interception of telephone communication in case of failure to submit to the Office a court ruling or a prosecutor's resolution either in electronic and/or tangible (documentary) form, or when the data included in electronic and hard copy of the prosecutor's resolution does not match





or/and they are vague/incorrect. Since April 2017 the suspension mechanism was used with regard to 21 rulings/resolutions. The covert investigative activities continued after the elimination of grounds of suspension.

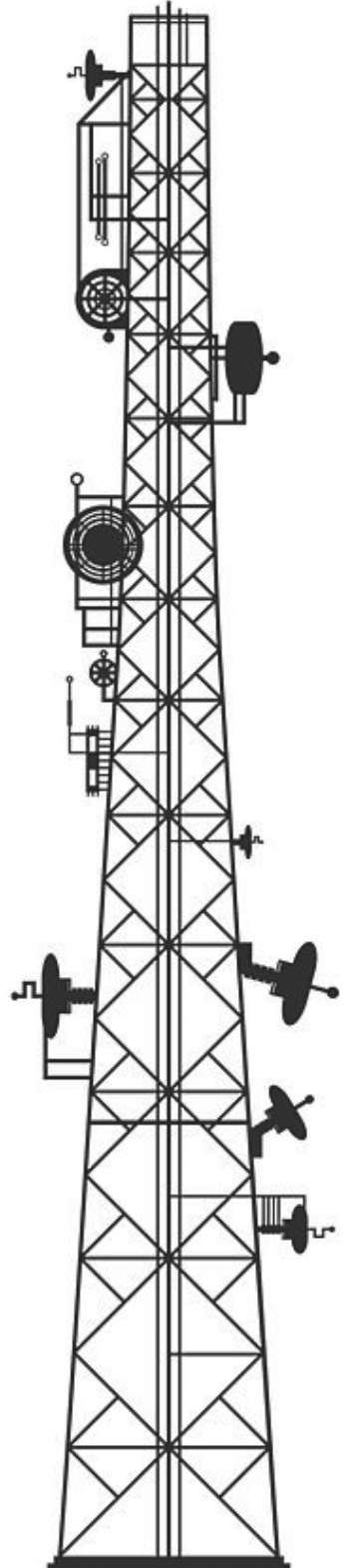
The Criminal Procedure Code of Georgia lays down a mechanism of special notification in case requisites and/or operative part of a judge's ruling on granting permission to carry out a covert investigative activity contains an ambiguity or irregularity. Since April 2017 the Office of Personal Data Protection Inspector notified authorized agency with regards to the ambiguity or irregularity in 10 rulings through an electronic control system. The shortcoming was addressed in accordance to the rules and timeframes established by the law.

Two inspections were carried out in 2017 with the purpose to examine lawfulness of data processing conducted by LEPL Operative-Technical Agency as a result of a covert investigative activity envisaged under Article 143<sup>1</sup>(1)(a) of the Criminal Procedure Code of Georgia. In addition, 2017 the Prosecutor's Office of Georgia and State Security Service of Georgia were jointly inspected. The purpose of the inspection was to examine lawfulness of processing data of several persons/data subjects through covert investigative activities. The inspection was conducted by means of the control mechanisms established under Article 35<sup>1</sup> of the Law of Georgia on Personal Data Protection. As a result of the inspection no violation of requirements of Law on Personal Data Protection has been revealed on the part of the Prosecutor's Office of Georgia, the State Security Service of Georgia or LEPL Operative-Technical Agency.

## **PROCESSING IDENTIFICATION DATA OF COMMUNICATIONS**

In 2017, the Office revealed five cases when electronic communication companies unduly fulfilled or breached their obligation under the Law of Georgia on Personal Data Protection of notifying the Personal Data Protection Inspector regarding the transfer of identification data of electronic communication to a law enforcement agency.

Within the reporting period the Office of Personal Data Protection Inspector inspected three electronic communication companies. In result of reviewing the documents regarding the transfer of information to a law enforcement agency it was revealed, that the companies violated the deadline for notifying the Inspector.







AN ELECTRONIC COMMUNICATION COMPANY IS OBLIGED TO TAKE SUCH ORGANISATIONAL AND TECHNICAL MEASURES THAT WILL ENSURE PROPER ENFORCEMENT OF OBLIGATIONS DETERMINED BY THE LAW, INCLUDING DURING HOLIDAYS AND NON-BUSINESS DAYS AND EVEN UNDER UNFORESEEN CIRCUMSTANCES.

During the monitoring of data processing by an electronic communication company for investigation purposes, it has been revealed that one of the electronic communication companies transferred information to the law enforcement agency in the absence of legal grounds determined under Article 5 of the Law of Georgia on Personal Data Protection. In particular, due to the ambiguity in the ruling, the company assumed that the judge had made a technical mistake and decided to provide the information for a period longer than determined in the ruling. The Inspector pointed out that in

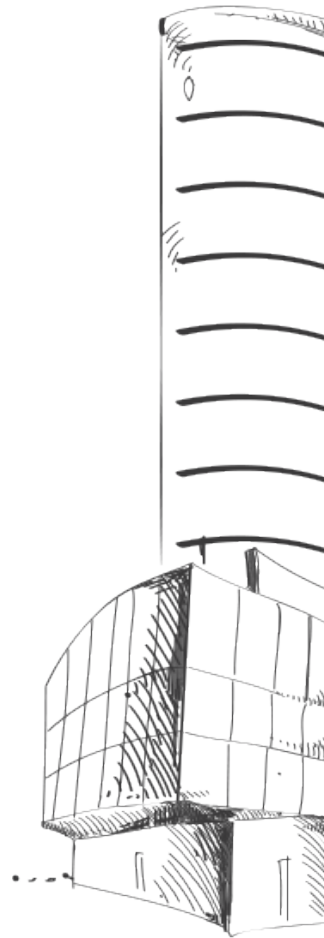
case of ambiguity in a ruling, the clarification shall be provided by the court. Only the court is authorized to decide on the ambiguity in a timeframe for which the information is requested and only the court is authorized to address shortcomings in a ruling. With regard to the same fact, a violation of principles of data processing foreseen by law was established in case of the Prosecutor's Office of Georgia as well.

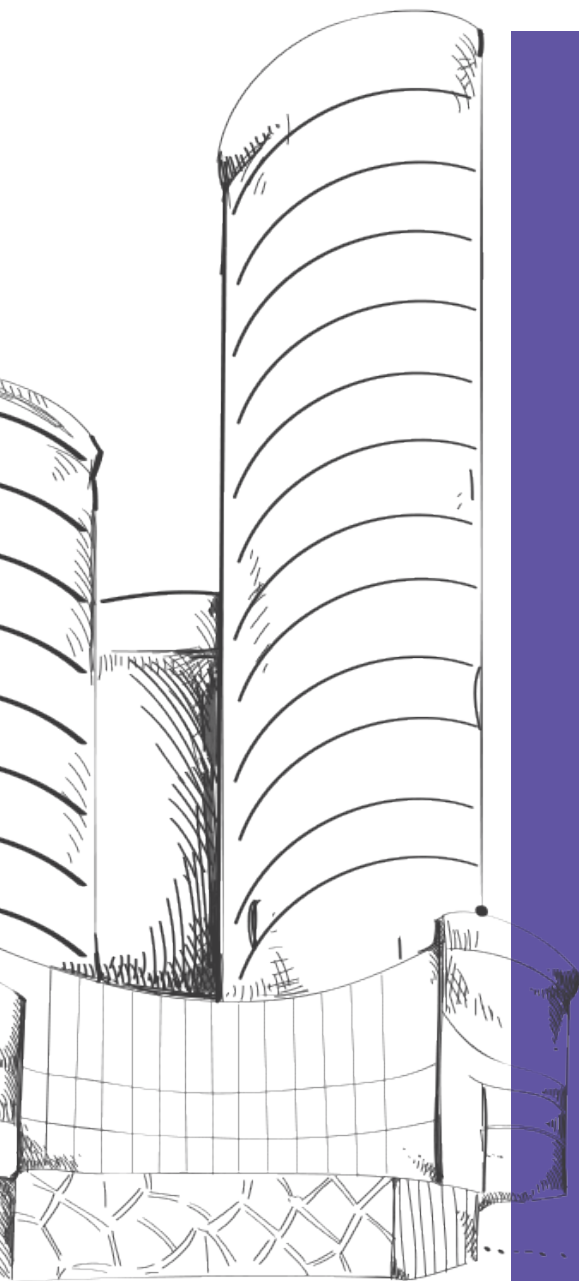


# DATA PROCESSING IN PRIVATE SECTOR

In Georgia majority of data controllers operate in the private sector. Usually, offering or providing different services to natural persons is connected to data processing. Notably, companies providing financial or healthcare services process large volumes of the personal data. Along with the development of technologies the creation and use of databases has been significantly increased and much more data is processed electronically and online by the private organisations.

THROUGHOUT THE REPORTING PERIOD, IN THE COURSE OF EXAMINING COMPLAINTS, CONDUCTING INSPECTIONS OR PROVIDING CONSULTATIONS THE INSPECTOR'S OFFICE STUDIED 270 DIFFERENT BUSINESS PROCESSES, INCLUDING IN THE FOLLOWING ORGANISATIONS OR SECTORS:





**51**

**RETAILERS**

**39**

**MICROFINANCE ORGANISATIONS  
AND ONLINE LOAN COMPANIES**

**32**

**COMMERCIAL BANKS**

**29**

**COMPANIES CONDUCTING  
DIRECT MARKETING**

**24**

**DEBT COLLECTING COMPANIES**

**24**

**PAWNBROKERS AND CURRENCY  
EXCHANGE BUREAUS**

**14**

**ELECTRONIC COMMUNICATION  
COMPANIES**

**11**

**HEALTHCARE AND INSURANCE  
COMPANIES**

**46**

**OTHER ENTITIES**

In addition, Inspector's Office provided more than 1500 verbal and written consultations to private organisations. As a result of these consultations, companies were able to fulfil their statutory obligations and prevent possible violations.

Unlike medium and small businesses, awareness regarding personal data protection has increased in large companies. Determination of grounds for data processing and the standards for data security have also improved. However, some shortcomings and violations are still revealed. Much more violations are revealed in medium and small businesses and, due to this, the Inspector's office regularly informs private companies about statutory regulations and practical advice in simplified form, which will help them protect customers' personal data.

The report describes violations and shortcomings revealed in 2017 while examining business processes of private companies and also gives some examples. As a result of the analysis of these violations and shortcomings it is possible to assess existing tendencies and challenges and to discuss measures that will facilitate the improvement of data protection in private sector.

## **DATA PROCESSING DURING THE MANAGEMENT OF PROBLEM LOANS**

Information regarding the financial indebtedness of an individual constitutes personal data and disclosure of this information to a third party is allowed only in cases explicitly determined by the law.

Within the reporting period the majority of cases studied by the Personal Data Protection Inspector related to the lawfulness of data processing in the debt collection process. In their complaints and requests for consultations citizens were referring to facts of debt collecting companies disclosing information regarding their financial obligations with family members, neighbours, friends on social network and/or co-workers. After studying the cases, it has been revealed that while collecting debts, the debt collecting companies are still often violating legislative requirements defined by the Law of Georgia on Personal Data Protection. Organisations (data processors) have lawful interest to negotiate with the debtor with the aim of ensuring payment and to communicate with third parties for this purpose, however, in this process it is important to follow data processing principles established by the law. The protection of company's interest shall not infringe the rights and dignity of an individual.

Throughout the reporting period it has been revealed that the credit companies process data of problem debtors to an extent which is not adequate and proportionate to the purpose. There were cases when companies were contacting persons who were not indicated in the contract as a contact person by the debtor. In addition, loan agreement included only several specific means of communication between the parties (telephone number, e-mail and address) and did not include the right to disclose information on financial indebtedness to third parties. Despite these restrictions, companies chose to communicate with the debtor through third parties. In several cases, there was no necessity to communicate with a third party, since the means of communication agreed with debtor under the contract were not completely exhausted.

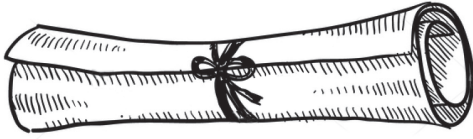






As a result of the review of a citizen's complaint, the Inspector established that loan agreement between a debtor and credit company included only specific means of communication (SMS; e-mail communication, etc.). However, the company used a communication tool which was not determined in the agreement and contacted the debtor's co-worker and family member for the purpose of reaching the debtor and disclosed the information regarding the indebtedness to them. At the same time, in the abovementioned case the company examined the debtor's personal profile on a social network, established the names of his/her friends and sent a standard message containing personal data of the applicant to some of them. In this case the data processor failed to substantiate the specific need and purpose for contacting third parties, especially considering that the company did not fully exhaust means of communication with debtor set forth in the contract.

According to the existing practice, the credit organisations use debt collecting companies for the management of problem loans. In such circumstances the latter receives data of the debtor and is also given the authority to act on behalf of and for the interests of a credit organ-



isation. Thus, debt collecting company becomes the data processor of the credit organisation. In 2017, several positive trends have been revealed as a result of the activities of the Inspector's Office. For instance, majority of credit organisations include the rules of communication with debtor in the agreement concluded with the debt collecting companies. Despite the above-mentioned, there were several cases when data processors used methods restricted by the credit organisation, such as disclosure of information on indebtedness with family members, neighbours, co-workers, persons connected on the social network, etc.

As a rule, loan contracts include standard terms for data processing and by signing the contract debtor gives his/her consent to processing his/her personal data for credit purposes, including data processing in case of problem debt collection. However, due to general wording of the contract provisions, the content of the conditions in the majority of cases is not clear to the debtor. In some cases, reviewed within the reporting period, the conditions of the loan agreement, due to its general or incomplete wording, were not considered as a debtor's consent for processing his/her data for a specific purpose and in a specific manner. In such cases, companies were given mandatory instructions.

#### DATA CONTROLLERS THAT POSSESS INFORMATION REGARDING THE FINANCIAL STANDING OF AN INDIVIDUAL SHALL:



strike a fair balance between their legitimate interests and debtors' right to the protection of personal data;



clearly and completely define the extent and scope of personal data processing in compliance with the purpose in the loan contract, as well as cases and forms of disclosure of information regarding the financial standing to third parties;



while managing problem debts themselves or through other companies, elaborate a unified standard for personal data processing and ensure its protection.

The previous reports on the state of personal data protection and the activities of the Inspector included information regarding the violations revealed during the data processing by credit bureau JSC “Creditinfo Georgia”. The reports also mentioned the need to regulate the activities of the bureau through legislation. Although the number of violations decreased compared to the previous years, in 2017 several problems were still revealed during data processing by JSC “Creditinfo Georgia”. Among the problems was the violation committed during the calculation of a credit score.

A citizen applied to the Personal Data Protection Inspector and stated that he used credit services from different credit organisations over the course of several years and, as prescribed under the contracts, certain information was stored in the database of JSC “Creditinfo Georgia”. JSC “Creditinfo Georgia” processed information received from credit organisations for the calculation of credit score (so-called “scoring”) and stored the score in its own database in a form accessible for the clients of JSG “Creditinfo Georgia”.

The Inspector's Office examined all contracts signed between the applicant and the credit organisations and established that the relevant conditions of the standard contract referred to by some organisations contained consent regarding the disclosure of certain data and the contract did not include consent on communicating data for the calculation of credit score and its results.

Informed and freely given consent by a data subject is very important, especially when calculating credit score and access to it by third parties may negatively affect the interests of a data subject and he/she might receive services with different conditions or might be refused services at all. As a result of the Inspector's decision, JSC "Creditinfo Georgia" was instructed to take measures to elaborate a unified consent form and periodically examine the presence of the consent for calculating a credit score.

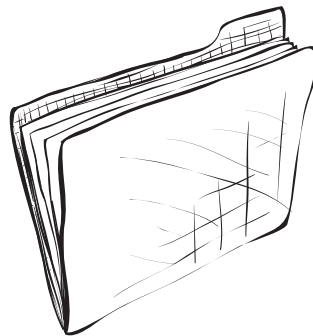


THIS CASE ONCE AGAIN PROVES THE NEED TO SPEED UP THE PROCESS OF ELABORATION OF LEGAL FRAMEWORK FOR REGULATING THE ACTIVITIES OF CREDIT BUREAU.

## PERSONAL DATA PROTECTION IN HEALTHCARE SECTOR

Under international and national regulations, health-related information falls under the special categories of personal data and higher standards are in place for its protection. Data processed in healthcare sector, for instance data disclosed to a doctor, may include information on previous diseases, genetic data, intimate issues, etc. Illegal disclosure of such information may result in the violation of a person's dignity, stigmatization or discrimination.

Protecting personal data is not only in the interests of a patient. If a person believes that his/her data will not be kept confidential, he/she may refrain from providing important information; this will create an obstacle to diagnose a disease, treat it effectively, and eventually properly administer the healthcare system. Therefore, high standards for protection of health-related data are essential for the healthcare system as well.



Due to sensitive nature of health-related data the Inspector's Office comprehensively examined lawfulness of data processing procedures in several healthcare provider companies throughout the reporting period. Despite several regulations in this field (laws on Patient's Rights and Healthcare and other relevant legal acts), a number of violations and challenges were revealed.

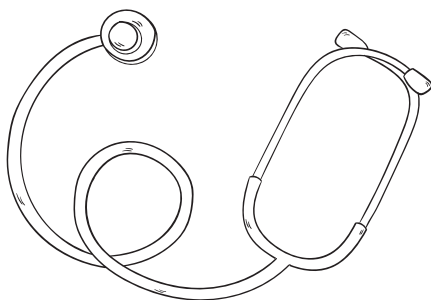
In 2017 the inspection of healthcare provider revealed that the organisation kept the register/journal where information on patients' laboratory tests was recorded. The register/journal of laboratory tests did not include either the information on to whom and when the test results were disclosed or the legal grounds for disclosure.

Within the reporting period a citizen applied to the Inspector claiming that his/her ex-spouse obtained documentation concerning his/her health from one of the healthcare providers and used it as evidence in the court proceedings.

The study of this case revealed that the healthcare institution released documentation concerning the applicant's health to his/her spouse without the consent of the data subject, based only on the identification document and certificate of church marriage. It was also established that as a practice this healthcare institution issued information concerning patients' health to family members who could provide documentation confirming that they were a particular patient's relative.

In 2017, during an inspection of one of the healthcare providers on the Inspector's initiative, the facts of disclosing personal data and health-related information to other organisations by telephone were also revealed. The healthcare provider did not keep a record of what data was disclosed, to whom, when and based on which legal grounds. It was also revealed that patients' medical information was provided to their relatives while there were no standards that would limit the circle of relevant persons.

The inspection of another healthcare provider conducted on the Inspector's initiative revealed that deceased patients' personal data were processed in violation of law. It was established that the organisation released medical information concerning the deceased patient to the person accompanying him/her and with whom the medical institution had concluded a standard agreement on the provision of healthcare/medical services. Mostly the person confirmed his/her relation to the deceased only verbally. In such cases authenticity of this relationship was not verified, since the healthcare provider considered him/her as the person accompanying the patient and the provider considered it possible to provide him/her with all types of medical documentation concerning the patient.



Any data controller and data processor shall keep a record of the types of information released, its recipients, the date and legal grounds based on which this information was disclosed. This obligation is particularly important when health-related information is released.

In 2017, the inspection of one of the healthcare institutions conducted on the Inspector's initiative revealed that this institution kept a registry in the form of a paper journal for the "incoming" and "outgoing" correspondence. There was no indication of who received this information and based on which legal grounds. The same inspection established that this healthcare provider did not record cases where documentation was provided based on a verbal request.

These cases were considered as violation of the legislation in force and all healthcare institutions were instructed to take relevant measures.

#### IN LIGHT OF THE ABOVE, IT IS NECESSARY THAT ALL HEALTHCARE PROVIDERS:



organise the processing of personal data well, define legal grounds for processing, and store the data for a specified period of time;



regularly monitor access of their staff to personal data and take adequate technical measures to ensure data security;



establish mechanisms for recording all actions related to the disclosure of information concerning patients (in particular, what data was disclosed to whom, when and on what legal ground) and develop



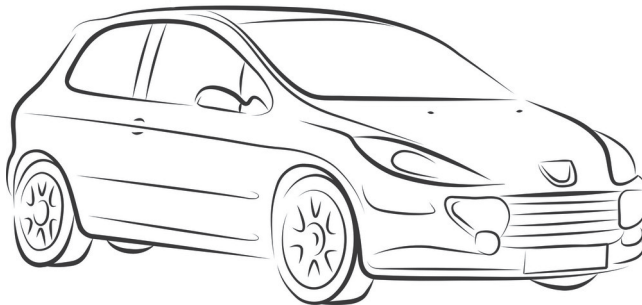
standard rules and procedures for providing documents containing patients' personal data to authorized third parties;



develop a standard rule/procedure to prevent disclosure of personal data to unauthorized persons and introduce an organisational mechanism for monitoring implementation of these rules.

## **INSPECTION OF “C.T. PARK”**

In Tbilisi municipality, “C.T. Park” LLC owns an exclusive right to manage parking. To this end the company uses a website - [www.ct-park.ge](http://www.ct-park.ge), where information on fined vehicles is placed to allow owners of these vehicles access to information on violations. Until the end of 2017, any interested person could receive information on the vehicle of their interest, including information on the fines and the places where violations were detected by simply entering the vehicle registration plate number on the website.



In 2017, Personal Data Protection Inspector received a citizen's request to delete information related to his fines from the web-site [www.ct-park.ge](http://www.ct-park.ge). In applicant's opinion, information on fines imposed on vehicle owners was published by the company in a way that would allow any interested person to easily discover the owners' personal information, including probable places of their residence and work.

After examining the case, the Inspector revealed that the web-site [www.ct-park.ge](http://www.ct-park.ge) included a large volume of information on thousands of individuals. This information was easily accessible for an indefinite period of time. The information placed on the web-site contained fine and vehicle registration plate numbers, photos reflecting the specific administrative offence, place and time of offence, the status of a fine, type of the offence, etc.



The purpose of publishing this information was to notify only the vehicle owner and a driver committing an offence. However, this information was accessible to all interested parties who know a particular vehicle registration plate number. Besides, in many cases a legitimate purpose for publishing data was already achieved or did not exist at all, for example, in cases where a fine receipt was annulled, was physically delivered to an addressee or the fine was paid. It was also revealed that the statute of limitation for executing and/or for cancelling the fine was not taken into account although the fact of violation was losing its legal importance after certain period of time.

As a result of examination, the company was fined for violating the data processing principles established under the law. The company was instructed to carry out specific measures which would ensure protection of the applicant's as well as thousands of other individuals' rights.

In response to the Inspector's instruction, the company established a specific time period during which the data are available on the website - [www.ct-park.ge](http://www.ct-park.ge) and restricted access to these data.

WHILE CARRYING OUT A PUBLIC AUTHORITY ONLINE, IT IS NECESSARY TO:



ensure a balance between the legitimate interests of data processing and the interests of a data subject;



determine the legal grounds for publishing data, uphold data processing principles by defining categories and volume of accessible data and the time period during which this information is accessible, among others.

## ONLINE PUBLICATION OF INFORMATION

Throughout the reporting period several cases were revealed where customers' data, recordings made by video surveillance cameras and personal telephones reflecting communication with them were published on social media and web pages. Any organisation communicating with the customers online has to protect personal information in its possession. A failure to fulfil this obligation in order to protect commercial interests may lead to violating the law.

Within the reporting period a citizen applied to the Personal Data Protection Inspector indicating that a company had published his personal data without a legal ground. After the examination of this case it was established that the applicant revealed his personal information to the company to receive a specific service. Later, he made a negative comment on the company's official Facebook page anonymously.

In response to this comment, the company published the applicant's personal data (name, surname, address) stating that his comment was impolite and misleading. The company stated that the customer's name was revealed to defend the company's business reputation and its legitimate interests and to prevent future assaults by publicly denouncing the applicant.

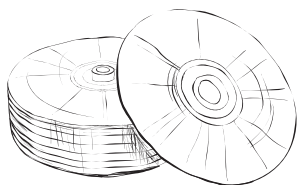
Inspector concluded that creating an anticipation among customers that their personal information will be published is not a legitimate way to defend a company's business reputation and prevent other actions endangering the company. Under the legislation in force, business reputation can be safeguarded through other means, including by applying to court. Hence, the company's explanations were not found substantiated.

## **DATA SECURITY**

Fulfilling obligations related to data security remains one of the major challenges in private sector. Within the reporting period, the Inspector studied several cases where data security obligations were not fulfilled by entities processing different types of data.

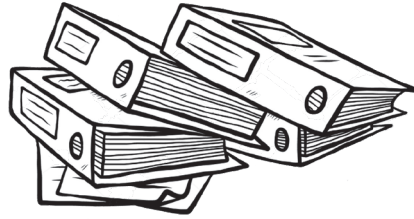
In 2017, a citizen applied to the Personal Data Protection Inspector indicating that a company checked his data in the database of JSC “Creditinfo Georgia” without his/her consent. It has been revealed that the company had access to the above-mentioned database under the contract concluded with JSC “Creditinfo Gorgia” and the data were accessible to two of the company’s employees with personalized usernames and passwords (the usernames were based on the first and last names of these individuals). The usernames and passwords enabled access to data from any computer. At the moment when the applicant’s data was accessed, the company had terminated employment relationship with the individuals possessing the usernames and passwords of the system. Despite termination of employment contracts, the former employees still maintained information necessary to access the database. They could access the database of JSC “Credinfo Georgia” from any computer even after termination of the contract as the company had not applied to the JSC “Creditinfo Georgia” to deactivate their usernames or/and change the passwords.

In the same case it was revealed that the company shared a working space with a partner organisation. The latter’s employees had unrestricted access to the JSC Creditinfo Georgia’s database by using the usernames and passwords registered under company’s name, even though there was no agreement between the company and the partner organisation regarding data processing.



The inspection of one of the microfinance organisations established that all the personal data of the clients was accessible to a large number of employees. Correspondingly, in relevant software there was no differentiation in the levels of access to clients' data.

In 2017 an inspection of a financial institution established that the organisation sent automated voice messages to debtors' telephone numbers (including, office numbers) in cases of payment delays. The voice messages contained information on the outstanding debt and measures to be taken by the company if a client failed to pay the debt. It should be noted that the loan agreement concluded between the company and a borrower did not include information on automated voice messages that were sent to debtors. Therefore, while concluding a contract data subjects could not reasonably expect that the company would send automated messages by unidentified speakers to the telephone numbers indicated in the application. If properly informed, the data subjects could have refrained from indicating a landline number and instead could have indicated only personal cell phone numbers.



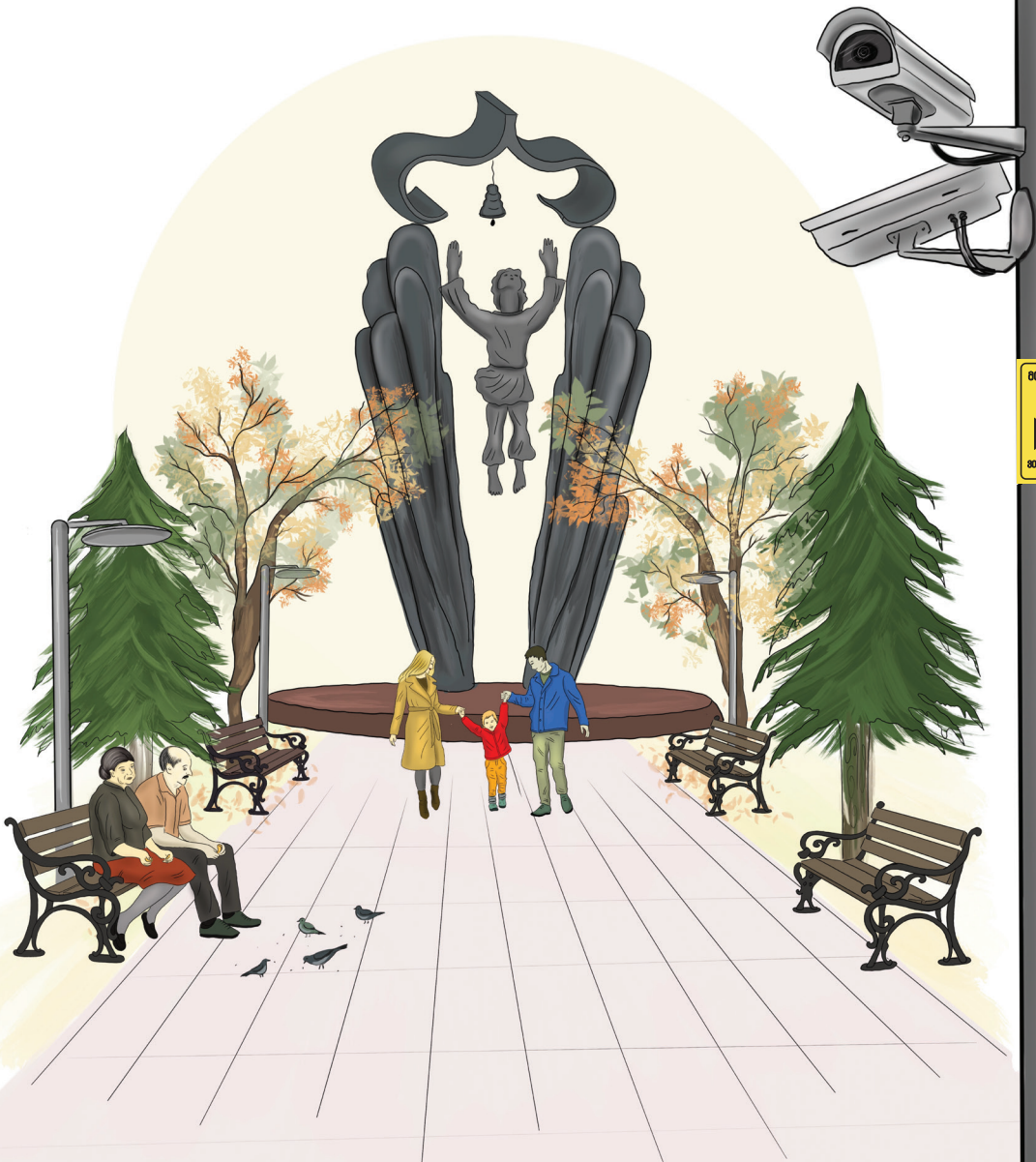
## FILING SYSTEM CATALOGUES

One of the accountability mechanisms for personal data processing is maintaining a filing system catalogue (compilation of data, filed and accessible according to specific criteria) and submitting it to the Inspector. In its turn, the Inspector operates a register of filing systems catalogues accessible to any interested individual and allowing them to receive information about the grounds, purpose and extent of information processed by organisations, persons responsible for data security etc.

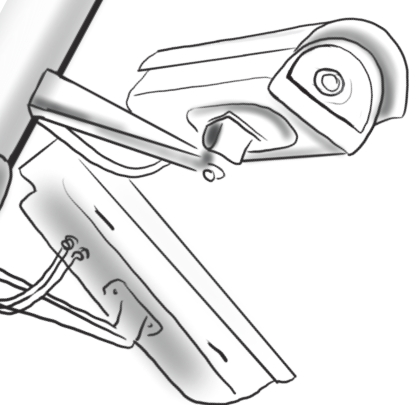
Within the reporting period the data controllers operating in Georgia submitted 1214 filing catalogues to the Inspector by means of the electronic register. From this overall number, 1108 catalogue were submitted by the data controllers in private sector, out of which 279 catalogues were submitted by health-care providers, 200 – by retailers, 192 – by financial organisations, 74 – by manufacturing companies, etc. Notably, in previous years filing catalogues were submitted mostly by so-called large data controllers; in 2017, many entities processing relatively small volumes of data submitted information about data processing through filing system catalogues.

After receiving filing system catalogues, the Personal Data Protection Inspector examines their compliance with the existing legal requirements. If any inconsistencies are revealed, the Inspector's Office provides relevant information and advice to ensure compliance of the data processing and filing catalogues with the requirements established by law.





# VIDEO SURVEILLANCE



Several violations were revealed as a result of inspection of 2400 video surveillance appliances.

Twenty-five organisations were fined or given a warning.

Video cameras in the streets and buildings, on the roads, in public transport and ongoing video surveillance have become a part of citizens' everyday life. In the case of *López Ribalda and Others v. Spain* the European Court of Human Rights explained that "a person's image constitutes one of the chief attributes of his or her personality, as it reveals unique characteristics and distinguishes him or her from his or her peers." Thus, the right to protect one's image is a part of a person's development.

Under Georgian legislation, video monitoring may be used to prevent crimes, protect a person's safety and property, defend public order and protect minors from harmful influences. It should not be used as an additional mechanism for controlling citizens' behaviour. While installing video surveillance appliances all data controllers are obliged to display a corresponding warning sign in a visible place in order to respect and protect citizens' rights through informing them.

The Inspector's Office carried out several activities regarding video surveillance, including awareness raising campaigns, inspection of lawfulness of data processing and review of citizens' complaints.

Throughout the reporting period the Inspector's Office examined more than 2400 video surveillance appliances owned by financial organisations, retailers, healthcare providers, hotels, pharmacy chains, petrol stations, municipalities and other public organisations. As a result of examination, several viola-

tions of video surveillance rules were discovered. Twenty-five organisations were sanctioned by a fine or a warning. Additionally, the organisations were assigned to display relevant warning signs, to inform employees about video monitoring, to store data for a specific period of time and to take organisational and technical measures ensure data security. The inspections carried out during the reporting period revealed that in addition to objectives strictly established under the law, such as crime prevention, protection of public order, person's safety, property, secret information, and protection of minors from harmful influences, private organizations used video surveillance for other purposes as well. More specifically, video monitoring of workplace was ongoing without informing employees; video surveillance was also used to control employees' behaviour, dress code and communication. In many cases companies did not take adequate organisational and technical measures to protect security of video recordings. The inspection also revealed facts of video monitoring in the changing rooms and places intended for hygiene.

#### THE FOLLOWING CIRCUMSTANCES HAVE TO BE TAKEN INTO ACCOUNT WHILE PROCESSING DATA BY MEANS OF VIDEO SURVEILLANCE:



Video surveillance systems can only be used to achieve objectives established by the law;



A video surveillance system should have technical characteristics corresponding the goals to be achieved;



The rights of individuals under video monitoring, have to be protected as much as possible, both by placing respective signs in visible places and by properly informing neighbours in residence buildings and receiving their consent for installing surveillance systems.

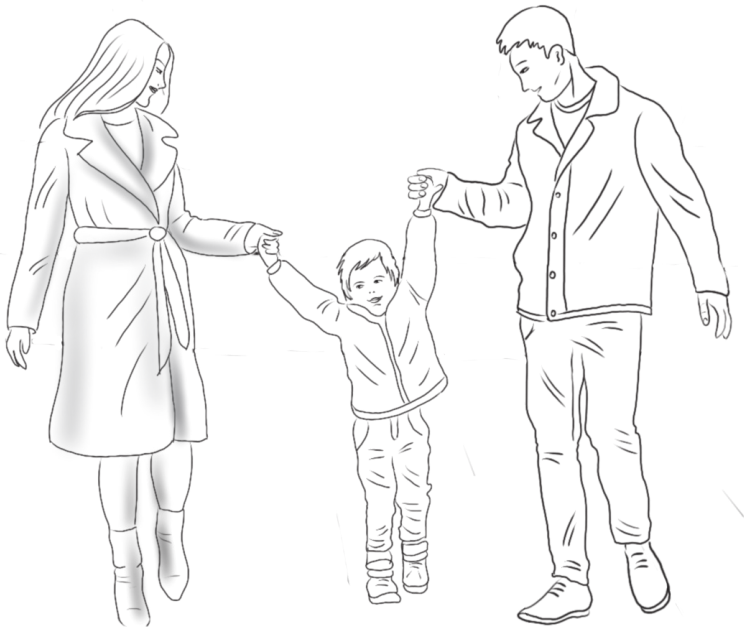
## **VIDEO MONITORING OF CHANGING ROOMS AND PLACES OF HYGIENE**

Video monitoring is prohibited in changing rooms and places of hygiene due to the form, extent, and sensitive nature of invasion of privacy. An individual has a reasonable and legitimate expectation that in such places video monitoring is not carried out.

Within the reporting period, media outlets disseminated information that a certain company was carrying out video surveillance of changing rooms and places of hygiene located in the shops owned by the company. The Personal Data Protection Inspector began studying the case as soon as this information was published. As a result of an inspection, it was established that video monitoring was carried out in changing rooms allocated for the shops' female employees. The company representative was explaining that video surveillance served the aim of protecting employees' safety and company's property. As a justification of video monitoring the company pointed out that it was initiated at the employees' written request (the company failed to present the written evidence of such a request).

The Inspector found the company responsible for an administrative offence, charged it with an administrative sanction and instructed it to terminate video monitoring of changing rooms located in shops and delete/destroy all the recordings.

The inspection of another company revealed that places of hygiene were subjected to video surveillance. The video cameras were installed in the hotel's two hygiene spaces allocated for children. The company explained that these spaces were used by children under the age of seven and video monitoring aimed to ensure their safety. The Inspector did not share the company's arguments, since it is clearly unlawful to monitor places for hygiene and all individuals, including children have the right to privacy. That is indeed why the law prohibits video surveillance of hygiene rooms.



## VIDEO SURVEILLANCE AT WORKPLACE

In many cases, public and private organisations use video surveillance at the workplace to control employees' punctuality and to protect internal standards, including employees' appearance/dress code.

Within the reporting period, the Personal Data Protection Inspector received a notification stating that a company was controlling its employees' dress code by means of a video surveillance system. There was a case where a disciplinary sanction in the form of a strict reprimand was imposed on the administrator of the company's branch office who did not wear a special uniform.

As a result of the inspection of one of the municipalities it was revealed that the chairman of municipality controlled the employees' punctuality by means of a video surveillance system and a mobile phone application despite the availability of a special system controlling entry and exit in the building (a so-called "tourniquet").

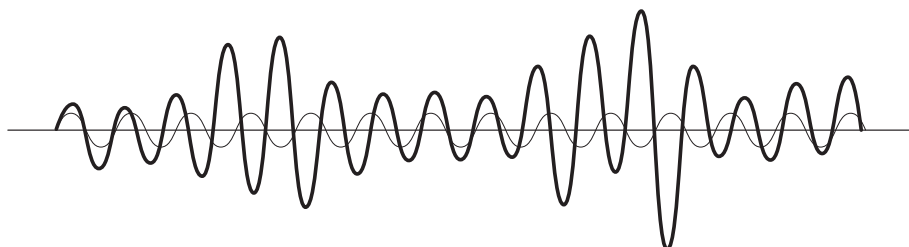
Within the reporting period an inspection of one of the public entities revealed that video monitoring and audio control were ongoing in the room of one of the structural units of the organisation which was located in the administrative building. Also, it was established that the majority of managers had access to video and audio recordings. The agency explained this fact by the managers' supervisory and controlling functions.

The Personal Data Protection Inspector explained that data security measures have to be adequate and proportionate to risks. The more people have access to data, the higher the risks that these data will be processed unlawfully. Thus, a data controller has to assess whether it is necessary for a specific employee to have access to data in order to fulfil his/her functions and duties.

In many cases organisations try to justify video monitoring of their employees' performance, communication practices, and dress code by the need to control the quality of services they provide. This may not be accepted as an acceptable aim for video surveillance; especially considering that organisations are using other means as well to this end. Also, even when there is a legitimate aim for video monitoring, all employees have to be informed about video surveillance and their rights in writing.


## AUDIO MONITORING

In previous years, inspections were conducted in several pharmacy chains where video and audio monitoring was used to control interaction between customers and employees with an aim to improve quality of provided services. As a result of the inspection, many pharmacy chains terminated audio monitoring and introduced alternative service quality control mechanisms.



In 2017, the Inspector's Office was notified that one of the pharmacies used audio and video monitoring to control employees. The inspection revealed that at the company's 22 retail points the employees and customers were monitored 24 hours a day by means of cameras and audio recorders placed on the pharmacists' desks. The inspection also uncovered that the company used alternative mechanisms for quality control purposes, which, unlike audio monitoring, did not require processing data that was disproportionate to the purpose.





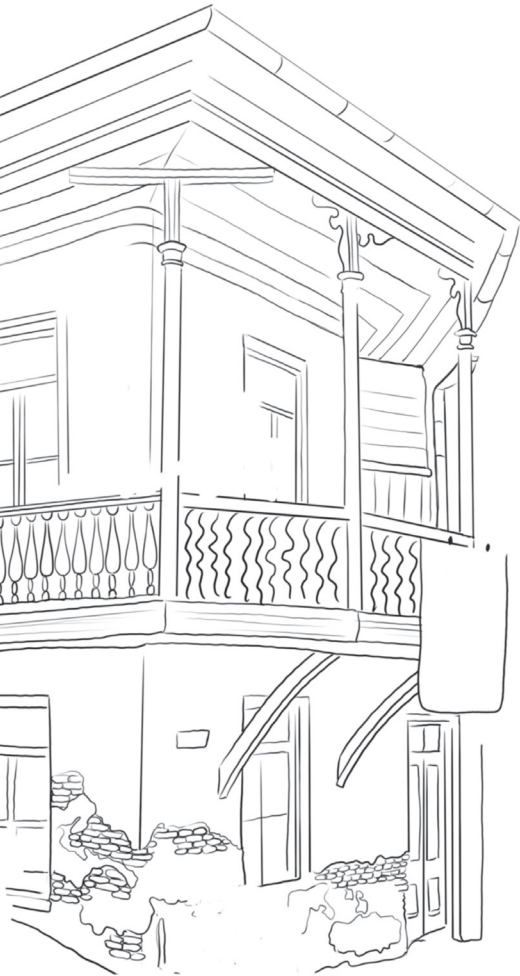
The data controller has a legitimate interest to control quality of its services. However, this can be achieved with less interference in employees' and consumers' privacy. Data controllers have to ensure a fair balance between their lawful interests and the subjects' right to personal data protection. The fact that audio monitoring appliances can be easily used for monitoring employees and customers, does not mean that they can be used at the expense of invasion into individuals' privacy. In addition, under the law, data should be processed to the extent necessary for the relevant legitimate objective. The data have to be adequate and proportionate to the objective for which they are processed.

Protecting the principle of proportionality becomes particularly important in cases where a video surveillance system allows for both video and audio monitoring. A data processor has an obligation to justify the need for audio monitoring. Audio monitoring is allowed if this is clearly envisaged in a normative act defining a data controller's or processor's functions and obligations, or if audio monitoring is necessary for the data controller to carry out its work and legitimate objectives may not be achieved by other means.



THE REVEALED VIOLATIONS INDICATE THE NEED FOR NORMATIVE REGULATION OF THIS ISSUE, IN ORDER TO CLEARLY DEFINE DATA CONTROLLERS' OBLIGATIONS AS WELL AS LEGITIMATE PURPOSES AND GROUNDS FOR AUDIO MONITORING WHEN AUDIO MONITORING SYSTEMS ARE INSTALLED.

## **VIDEO SURVEILLANCE OF RESIDENTIAL BUILDINGS CARRIED OUT BY INDIVIDUALS**



Citizens often use video monitoring of private houses and residential buildings to protect their property. Within the reporting period the Personal Data Protection Inspector studied several cases where individuals monitored residential buildings. As a result, it has been revealed that video surveillance systems installed for property protection purposes may violate other individuals' right to privacy, including the rights of neighbours or co-owners.


In one of the cases examined in 2017 the Inspector established that the video surveillance system was installed against the co-owners' will. One of the video surveillance cameras was installed on the door of the residential house to observe the entrance. The other was directed at the shared kitchen. The third camera was installed in the jointly owned corridor and was observing the claimant's facilities and rooms, including the bedroom entrance.

Citizens should precisely assess their needs and use video surveillance systems only for the property protection and security purposes. This can be achieved with minimal costs, without using technically advanced cameras (high resolution, zoom functions to magnify observed objects, etc.). In such cases the extent of data processing is less intrusive thereby reducing the risk of unlawful data processing. Notably, in a residential building more than half of the residents have to agree in writing to allow installation of a video surveillance system, and the residents of the building have to be informed accordingly.

## STORAGE OF VIDEO RECORDINGS

In practice there are cases where organisations do not assess their needs properly and keep data, including video recordings, for an indefinite period of time, even when there is no need or lawful reason for preserving the data.

The inspection of several companies revealed that they kept copies of recordings made in 2013 (including recordings handed over to law enforcement agencies) for an indefinite period of time. The companies failed to provide proper reasoning for keeping recordings passed to law enforcement agencies indefinitely. The legislation defines an obligation to provide video recordings to law enforcement agencies if there is a relevant legal basis, but does not call for keeping the recordings for an indefinite period of time. Any transfer of video recordings to the law enforcement agencies shall be registered in accordance with the requirements outlined in Article 18 of the Law of Georgia on Personal Data Protection, which provides for the registration of the following information: types of disclosed data, recipients, time and relevant legal grounds.



Under the current legislation, video surveillance systems shall be installed by the organisations engaged in the following types of activities: pharmacies, currency exchange bureaus, petrol stations, and organizers of gambling games. Notably, under the law these organisations are obliged to keep video recordings for not less than 30 days. However, the maximum term for keeping the archive is not established. It is advisable to regulate these issues and define a maximum term for keeping video recordings through normative acts.

Organisations shall keep video recordings for not less than 30 days. However, the maximum term for keeping recordings is not established. It is advisable to regulate these issues and establish a maximum term for preserving video recordings at the statutory level.



ORGANISATIONS SHALL KEEP VIDEO RECORDINGS FOR NOT LESS THAN 30 DAYS. HOWEVER, THE MAXIMUM TERM FOR KEEPING RECORDINGS IS NOT ESTABLISHED. IT IS ADVISABLE TO REGULATE THESE ISSUES AND ESTABLISH A MAXIMUM TERM FOR PRESERVING VIDEO RECORDINGS AT THE STATUTORY LEVEL.

## DISCLOSURE OF VIDEO RECORDINGS

There have been cases revealed where different organisations published information containing personal data on social networks. In most cases the companies justify such actions by the need to protect their business reputation and legal interests, to encourage positive behaviour in the society, etc.

The Inspector's Office inspected a company to study whether it lawfully published personal data on social network. This company published photos depicting a customer's visit to the shop. The photos were taken by means of the video surveillance system. The company claimed that this person was discrediting the company and was calling for boycotting the company despite being a frequent customer of the company's shops. The company used this argument to justify publication of the customer's photos.

It is possible to protect a company's business reputation without publishing personal data and identifying specific individuals. Individuals have a reasonable expectation that video recordings aim to protect a company's security and property and will not be published on social networks, especially in cases where publication of recordings is a disproportionate and unjustifiable invasion in a citizen's privacy.



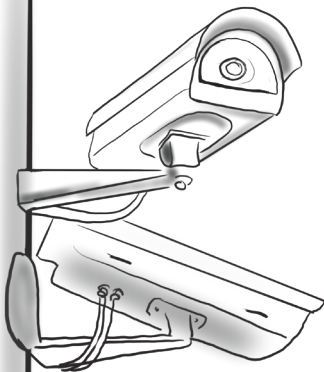
## **APPOINTING A DATA PROCESSOR TO CONDUCT VIDEO SURVEILLANCE**

Data controllers often use services of various companies thereby making the data at their disposal accessible for the companies. These companies are processing data for and on behalf of data controllers and they represent data processors. In 2017, the inspection of lawfulness of video surveillance practices revealed several cases where organisations used a shared video surveillance system to monitor a common space for safety and property protection purposes. Public and private entities often authorize other organisations to access the video surveillance system for providing technical services and protecting property and safety.

Data processor shall process data within the boundaries of the authority outlined in a written agreement concluded with the data controller. The agreement shall include requirements for data processing by the data processor, as well as statutory restrictions and rules. To avoid a risk of illegal use of data, the agreement shall define forms of data processing, security measures, etc.

## **ACCESS TO VIDEO SURVEILLANCE SYSTEM AND DATA SECURITY**

In 2017, the inspections conducted by the Inspector's Office revealed several violations of data security. Data controllers often did not take relevant organisational and technical measures necessary for data protection. In the reporting period there were cases where persons authorised to access a video monitoring system did not have individual usernames and passwords; instead they used shared username and password.



One of the retail stores did not register all actions related to data in an electronic register, whereas it is important to register all data-related actions, including views and exports of data to ensure data security and to prevent illegal access, data breach, use or destruction of data. The inspection also revealed that the video surveillance system was accessible to several persons who could create user profiles, define levels of access and authority, access data directly in the process of recording (in an uninterrupted regime), view and export video recordings. Authorized persons with access did not have individual usernames and passwords and jointly used common username (e.g. “admin”) and password. Thus, even if the software registered specific actions, it was impossible to identify a person who processed the data.

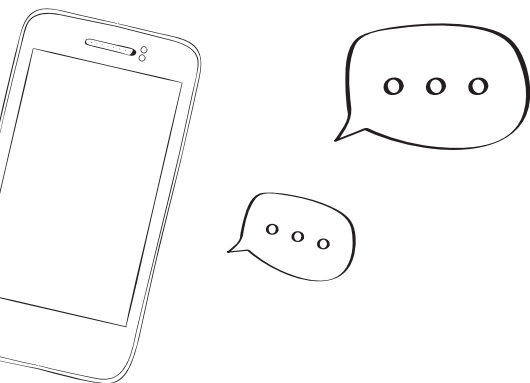
Organisations have to consider the needs and the authority of authorized individuals. Data security requires that each individual provided with access to personal data should have an individual username and password; otherwise risks of illegal data breach are created and it becomes impossible to identify persons who are responsible. In addition, it is advisable to develop adequate rules that will define issues of gaining access to a video surveillance system.





**HAIR TRANSPLANTATION**  
Conditions tailored to your needs!  
Visit the clinic "HairLocks" and pay in  
installments without interest.  
We guarantee the results!

# DIRECT MARKETING



In 2017, direct marketing continued to be an acute issue. However, it is to be noted that the number of violations decreased by 30% compared to 2016. Furthermore, while in previous years violations occurred mostly because of the absence of a refusal mechanism that would allow citizens to avoid marketing offers, within this reporting period violations were mainly caused by the flaws of this mechanism or its inadequate use.

In response to citizens' requests Inspector studied 29 cases of direct marketing. In 23 cases, violations of statutory rules were revealed and relevant fines were imposed on the organisations.

In the cases studied by the Inspector the organisations stated that the data for direct marketing purposes was mostly obtained from open sources as well as from the information that they received while providing different services to their clients. Most commonly, advertising text messages were sent out through so-called intermediary companies (including mobile phone operators). They usually used publicly available sources to create telephone number databases and the legislation in force allows use of such data for marketing purposes.

THE INSPECTOR'S  
OFFICE STUDIED

**29** CASES OF  
DIRECT MARKETING.

**23** IN CASES,  
VIOLATIONS OF  
STATUTORY RULES  
WERE REVEALED AND  
RELEVANT FINES WERE  
IMPOSED ON THE  
ORGANISATIONS.

Last year voters received messages from a candidate through an intermediary company. Although the sender did not have direct access to the data and text messages included information about the mechanism for refusing such messages, some citizens had doubts whether their data were obtained unlawfully.




Mobile operators often act as intermediary companies by providing special platforms for organisations. The platforms make it possible to send out advertising text messages without revealing telephone numbers to the client organisations. Mobile operators obtain subscribers' consent to having their data processed for direct marketing purposes. A subscriber unwilling to have his/her data processed by a mobile operator and/or some other intermediary company for direct marketing purposes, can apply to these companies with a relevant request and/or use a refusal mechanism indicated in text messages. The study of several cases revealed that organisations engaged in direct marketing via intermediary companies were unaware of so-called "black lists", i.e. lists of citizens who had refused to receive advertising messages. In certain cases, intermediary companies did not adequately register information about such individuals, in other cases - they refused to transfer this information to client companies. Thus, if client organisations decided to replace an intermediary company, they would face the risk of sending advertising text messages to individuals who by this time had refused to receive them.

Several citizens approached Personal Data Protection Inspector claiming that they had notified a specific organisation about their will not to have their data processed for direct marketing purposes in previous years. However, sometime later they received text advertisements on behalf of the same organisation again. As a result of examination of factual circumstances, it was revealed

that this was caused by replacing the data processor. At the time when applicants refused to receive advertising messages, the organisation was not keeping a record of so-called “black list” and neither was it receiving this information from the intermediary company. Thus, after the data processor changed and the organisation started sending out advertising messages through a different intermediary company, the organisation was unaware to whom not to send advertising text messages.

Within the reporting period there were cases when the addressees refused to receive certain categories of messages (e.g. offers related to gambling, medical services, various, etc.) instead of refusing to receive text messages from specific companies. These categories encompassed several organisations. Thus, it was impossible to identify which data controllers were requested by the addressees to stop processing their data for direct marketing purposes.

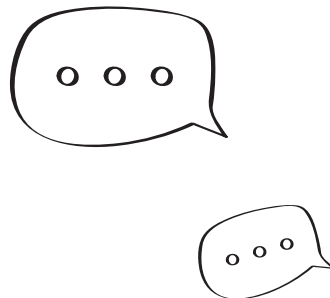
#### ORGANISATIONS ENGAGED IN DIRECT MARKETING THROUGH INTER-MEDIARY COMPANIES HAVE TO:

-  consider the issue of keeping and access to the so-called “black lists” in a contract concluded with an intermediary company;
-  offer recipients of text messages such a refusal mechanism that makes it possible to register the will of the recipients specifically towards this organisation;
-  avoid hiring a company that cannot verify lawfulness of obtaining personal data.

In the reporting period, there were still several cases where it was revealed that advertising text messages did not include a refusal mechanism. In one of the cases studied in 2017 the company offered through e-mail and text messages addressees presents in exchange for using certain services. The e-mail messages included neither the information about data subject's rights, nor a refusal mechanism.

The company indicated that an addressee could close his/her account on the company's web-page to avoid receiving messages. The Inspector did not find this to be an adequate refusal mechanism under the law because a data subject should be able to request termination of data processing without excessive efforts by using the same means which are used for carrying out direct marketing.

In the reporting period there was a case involving a public organisation carrying out direct marketing. A public organisation offering goods, services, employment and/or short-term work through text messages, e-mail or other means of telecommunication, is considered as an organisation carrying out direct marketing, similarly to private organisations. Thus, it is fully subject to direct marketing rules established by law.



In 2017 a citizen applied to the Personal Data Protection Inspector claiming that the LEPL Social Service Agency used his data for direct marketing purposes in violation of the rules. The study of the facts revealed that the Agency was required by law to carry out a program that promotes employment. To carry out this program, a website [www.worknet.gov.ge](http://www.worknet.gov.ge) was developed. Individuals looking for employment that had registered on the website received text messages containing information about vacancies. The messages did not include information about the refusal mechanism. During the examination of the complaint, the Agency explained that when a person was included in the program, by registering in the system he/she could choose means of communication and expressed readiness to receive relevant services. In addition, during registration or while editing data the user could delete the indicated telephone number and choose a different form of communication. The Agency also noted that text messages did not include a refusal mechanism because a contract between the parties was concluded voluntarily and a registered user was authorized to edit his/her profile information.

Despite the fact that individuals voluntarily provided their telephone numbers while registering on the website within the framework of the program and were allowed to delete these numbers from their profiles, they still should have had the possibility refuse receiving messages without additional efforts. It is also notable that a user of a telephone number may change easily. A new person acquiring a number may not be aware of the employment promotion program and the fact that his/her number is being processed by the Agency. Thus, the Inspector instructed the Agency to bring the process into conformity with legislation.





WHILE CARRYING OUT DIRECT MARKETING, BOTH PRIVATE AND PUBLIC ORGANISATIONS ARE OBLIGED TO INFORM DATA SUBJECTS ABOUT THE RIGHT TO REQUEST THE TERMINATION OF RECEIVING MESSAGES AND INCLUDE INFORMATION ABOUT THIS MECHANISM IN EVERY MESSAGE.



Notably, in addition to advertising messages, both public and private organisations often send information messages to citizens about terms of their services, changes in working hours, opening of new branch offices and other activities. It is advisable to include a refusal mechanism in these cases as well, thereby allowing citizens to refuse receiving unwanted information.

In 2017, there were cases when companies registered outside Georgia carried out direct marketing on the territory of Georgia.

For example, a citizen applied to the Inspector to examine whether his/her number was processed by a specific company lawfully. While studying the factual circumstances of this case, it was revealed that the applicant received advertising messages from a company registered outside Georgia. Furthermore, the messages were sent through three intermediary companies registered in different countries and finally reached Georgian customers registered on the company's web-page through one of the Georgian mobile operators.

Since direct marketing was carried out by a company registered abroad, it was impossible to establish the company's identification data while reviewing the application. However, it was found that the intermediary company sending out messages through a Georgian mobile operator was registered in Latvia.

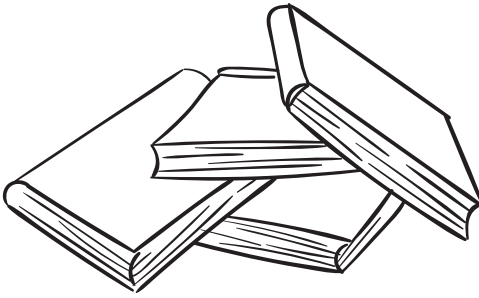
Therefore, the Inspector's Office informed the personal data protection supervisory authority in Latvia. The latter instructed the intermediary company to stop sending advertising messages to the applicant. The applicant confirmed that he has not received advertising messages from the company since then.

In the process of direct marketing, it is possible for several companies to be engaged together with the data controller organisation. These companies may be operating in different countries. Thus, the issue often needs to be addressed comprehensively. To protect citizens' rights, it might even become necessary to introduce stricter regulations.





# RAISING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES



Raising public awareness represents one of the key objectives of the institutional development strategy of the Inspector's Office, while promotion of the culture of the respect to privacy is an inherent part of the mission of the Office. Consequently, informing the public regarding the importance of personal data protection and related risks remained among the top priorities of the Office in 2017. Numerous projects, events and activities were carried out through a variety of modern communication channels, digital and interactive tools, multimedia platforms, and educational activities.

Within the reporting period, the Inspector's Office held 40 events, including trainings, public lectures, seminars and informational meetings that were attended by more than 1000 representatives of public bodies and private organisations. Trainings were held for the representatives of the Ministry of Internal Affairs of Georgia, MIA Border Police, the Ministry of Justice of Georgia, Medical Emergency Centre, Georgian National Energy and Water Supply Regulatory Commission, National Assessment and Examinations Centre, various political parties, and other organisations, in order to enhance personal data protection standards


THE INSPECTOR'S  
OFFICE HELD

40

EVENTS, INCLUDING  
TRAININGS, PUBLIC  
LECTURES, SEMINARS  
AND INFORMATIONAL  
MEETINGS, WHICH WERE  
ATTENDED BY

1000+

REPRESENTATIVES  
FROM PUBLIC  
BODIES AND PRIVATE  
ORGANISATIONS.



and apply the legal provisions in practice. At the same time, continuing the practice of previous years, the Inspector's Office held monthly trainings for individuals interested in personal data protection issues.

The representatives of the Inspector's Office conducted several thematic trainings, on the topic of information security and cyber security, among others. During the series of seminars held at the Caucasian House, University of Georgia, and Technopark Georgia, the staff of the Inspector's Office discussed the issues of data security and related risks with students, representatives of private companies, journalists and other interested individuals.

The Inspector's Office also took part in the Georgian Internet Governance Forum, where the representative of the Office spoke about the new General Data Protection Regulation of the European Union.

Among educational activities, the Personal Data Protection Winter School is especially noteworthy. The school took place from January 28 to February 3, 2017 on the occasion of the International Data Protection Day. Within the scope of a week-long program, the staff of the Inspector's Office together with leading international and Georgian experts, instructed the students of law and journalism on personal data protection, current trends and the importance of data protection in the era of technologies. The Winter School was held with the assistance of the European Union, the United Nations Development Programme and the Office of the United Nations High Commissioner for Human Rights, in partnership with the International Centre for Migration Policy Development (ICMPD) and Training Centre of Justice.



The Inspector's Office also continued cooperation with civil society. With the assistance of the European Union and the Office of the United Nations High Commissioner for Human Rights joint project "Human Rights for All", the Inspector's Office held working meetings with local non-governmental organisations in Batumi, Kutaisi, and Zugdidi. The participants acquired information about the Inspector's mandate, data protection legislation and practice. They also discussed topical issues related to personal data protection and prospects of cooperation.

Considering the importance of personal data protection in media activities, the Inspector's Office carried out trainings, workshops and seminars regarding personal data protection in the media. More than 100 representatives of television, radio, print and online media acquired information about the importance of personal data protection, the best practices and existing challenges.

In 2017 in cooperation with the Council of Europe and with active participation of the representatives of the media, the Guidelines for the Protection of Privacy in Media were being elaborated. The guidelines will be intended for journalists and other media professionals and will be aimed at promoting the balance between the right to privacy and the freedom of expression in media activities.

Additionally, academic personnel of faculties of journalism of various Georgian universities participated in Personal Data Protection Weekends aimed at promoting personal data protection as an academic subject in curriculum. The seminars were held with the assistance of the European Union and the United Nations Development Programme joint project “Human Rights for All” in partnership with the Training Centre of Justice.

In 2017, educational activities of the Inspector’s Office were aimed at the representatives of the private sector as well. The Inspector’s Office elaborated guidelines for start-ups that comprise the issues related to lawful processing of data and data security, etc. in simple terms and provide practical advice. The guide was presented within the framework of an international conference, DataFest Tbilisi, and was disseminated to 200 representatives of business start-ups within the framework of the Startup Market project as well. The electronic version of the guide is available on the website of the Inspector’s Office.

Considering the large volume of data processed by educational institutions and with the aim of advancing data protection standards, a special focus was made on data protection issues in the field of education. The Inspector’s Office elaborated and published recommendations for schools and higher education institutions.

In order to present the recommendations to the relevant audience, the Inspector’s Office held meetings with the representatives of universities in Tbilisi and the regions. The discussions with academic and administrative personnel and students addressed the importance of personal data protection, the Inspector’s role, and topical issues of personal data protection in the field

of education. During the meetings, recommendations and information materials were also disseminated.

Information materials were elaborated for the ethnic minorities living in Georgia. The brochure entitled “What we should know about personal data protection” was translated into Abkhazian, Ossetian, Azerbaijani, Armenian and Russian languages.

Within the reporting period, the Inspector’s Office carried out numerous awareness raising campaigns. On the occasion of January 28, the International Data Protection Day, the Inspector’s Office created the Personal Data Alphabet, a web platform that comprises a list of 33 individual examples of personal data and illustrates in simple terms the ways for their protection as well as potential risks. An online campaign, which was carried out to present the Alphabet to the public, Exceeded 600 000 reaches.


THE NUMBER OF REACHES  
OF ONLINE CAMPAIGNS:

600 000

MORE THAN

5000

VISIBILITY ITEMS WERE  
DISSEMINATED AT THE  
EVENT HELD IN RIKE PARK.



The Inspector's Office took part in the May 26 (Independence Day) celebrations with the online campaign titled "I am from the country of Rustaveli". A competition on the theme of "the Knight in the Panther's Skin" was held through the Office's Facebook page. Posters with the poem's heroes' personal data were created. As a result of this initiative, more than 70 000 individuals received information on personal data.

The Inspector's Office developed multimedia informational materials for the website and Facebook page, including video recommendations on how to protect personal data at schools and how to process voter-related data. The Office regularly publishes articles on Technology and Personal Data on its website. More than 20 000 individuals received advice and recommendations from these articles.

The Office of the Personal Data Protection Inspector actively engaged in the activities in celebration of the Europe Day 2017. On May 7, more than 5000 visibility items were disseminated. Consultations were delivered and a quiz was also held. The Inspector's Office took part in the event entitled "I Am an Active Citizen" during which more than 100 students living in the Pankisi Valley were informed about personal data protection.

Within the reporting period a new logo was created and a public relations strategy was elaborated with the assistance of the European Union and United Nations Development Programme. Currently a website accessible to persons with disabilities is being developed.


## INTERNATIONAL RELATIONS

Enhancing cooperation with international organisations and the personal data protection supervisory authorities of other states is one of the key aspects of the activities of the Inspector's Office. 2017 marked not only sharing the best international practices, but also sharing Georgian experience and successful projects to the international data protection community.

In 2017 the Inspector's Office continued its active participation in various international and multilateral platforms and processes taking place in the field of personal data protection. The Inspector's Office is involved in the process of modernization of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). The Inspector regularly participated in the meetings and activities of the Consultative Committee of the Convention 108 ("T-PD"), including elaboration of Committee's recommendations and guidelines for protection of data in various sectors.

The representatives of the Inspector's Office also participated in the meetings of the International Working Group on Data Protection in Telecommunications (Berlin Group).





In 2017, the Inspector's Office also joined the International Working Group on Digital Education that works on developing educational platforms and online services to raise public awareness on personal data protection issues. The Working Group consists of personal data protection supervisory authorities of more than 50 countries.

In addition, participation in international conferences and events is crucial in terms of sharing experience and enhancing international relations. The annual Spring Conference of European Data Protection Authorities, which was held in Cyprus in 2017, is a remarkable example. At the conference, the Inspector delivered a speech on awareness raising campaigns and shared Georgian experience with her foreign colleagues.

A highlight of 2017 was the 19th Meeting of the Central and Eastern European Data Protection Authorities (CEEDPA) hosted by Inspector's Office on behalf of Georgia. This was the first high-level event held in Georgia related to personal data protection. Within the framework of the meeting, discussions on the outstanding issues of data protection were held; awareness raising campaigns, oversight mechanisms over law enforcement sector, personal data protection on the internet were also discussed.

Representatives of the Inspector's Office took part in the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC), as well as the 29th European Case Handling Workshop and international conference organised by the Estonian Ministry of Justice in close cooperation with the University of Tartu School of Law.

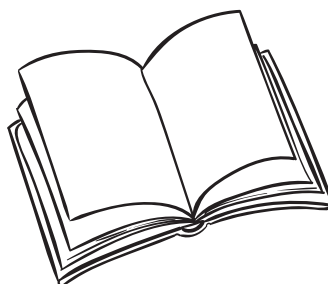
On the invitation of the Inspector General for the Protection of Personal Data of Poland, Personal Data Protection Inspector of Georgia also took part in the international conference held on the occasion of the 20th anniversary of the adoption of Personal Data Protection Law in Poland. The Inspector delivered a speech on current challenges related to personal data protection from the prospective of data protection supervisory authorities.

In addition to multilateral international relations, 2017 was important in terms of strengthening bilateral relations with other data protection supervisory authorities. The staff of the Inspector's Office participated in several study visits abroad. In January 2017, the representatives of the Office were hosted by the Italian Data Protection Authority and shared the best practices within the framework of the meetings. In December 2017, the staff of the Office visited Poland on the invitation of the Inspector General for Personal Data Protection of Poland; the objective of the visit was to share experience and best practices with regard to educational and awareness raising activities. The visits were conducted with the assistance of the European Union and the United Nations Development Programme.

The Inspector's Office also continuously contributed to fulfilling Georgia's international obligations, including the implementation of the EU-Georgia Association Agenda.



THE EUROPEAN COMMISSION IN ITS ASSOCIATION IMPLEMENTATION REPORT ON GEORGIA, PUBLISHED BY THE END OF 2017, UNDERSCORED THAT “THE INDEPENDENT DATA PROTECTION SUPERVISORY AUTHORITY CONTINUES TO FUNCTION EFFECTIVELY”.





The European Union  
for Georgia  
Human Rights 4All



The illustrations for this publication have been created with the assistance of the European Union and the United Nations Development Programme (UNDP). Its contents are the sole responsibility of the Office of the Personal Data Protection Inspector and do not necessarily reflect the views of the European Union and the United Nations Development Programme (UNDP).

Author of the illustrations - Tamar Kikoria