REPORT

THE STATE OF PERSONAL DATA PROTECTION AND ACTIVITIES OF THE INSPECTOR

2018

1

REPORT

THE STATE OF PERSONAL DATA PROTECTION AND ACTIVITIES OF THE INSPECTOR

2018

Office of the Personal Data
Protection Inspector

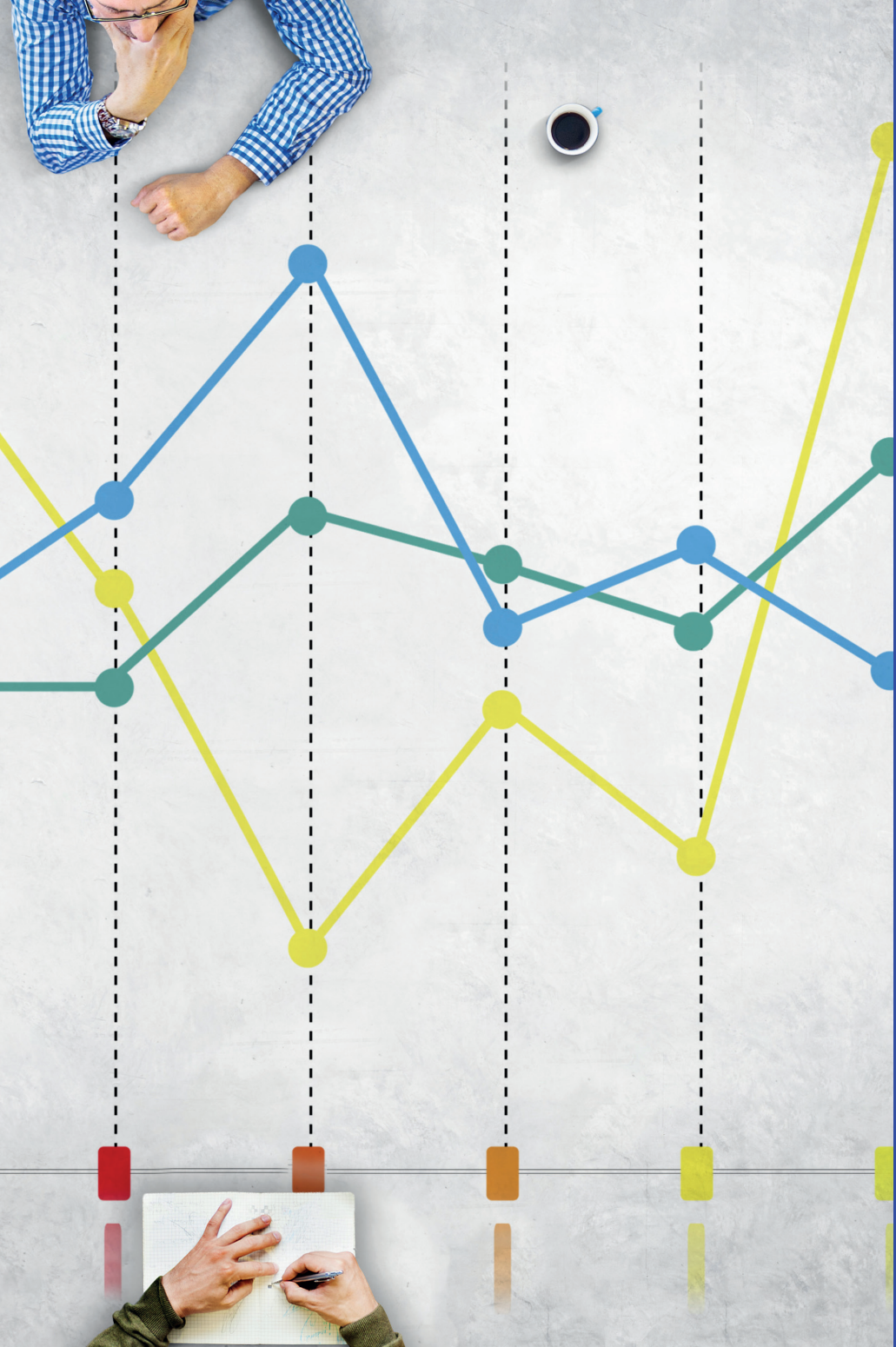
The European Union
for Georgia

Human Rights 4All

This publication has 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).

INTRODUCTION

2

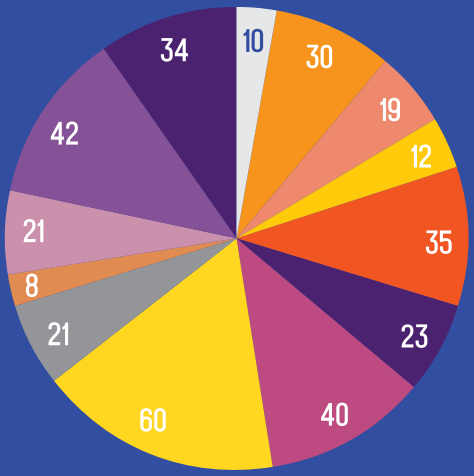


INTRODUCTION

The sixth annual report of the Personal Data Protection Inspector summarizes the state of personal data protection in the country and conducted activities in 2018. On the one hand, document contains the information about detected offences, problematic issues and existing challenges and on the other hand, it comprises information about the results of the Inspector's responses, improved processes and positive dynamics. The information about specific cases and statistics creates an opportunity to analyze the activities of the Inspector and general tendencies not only in 2018, but also over the last 6 years.

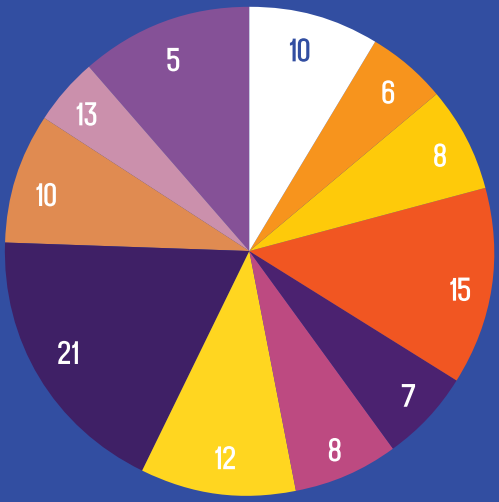
The tendency of increasing citizen's complaints and conducted inspections remains unchanged for the sixth year in a row. On the basis of 382 complaints lodged by citizens and 148 conducted inspections the Office studied 470 data processing operations by public and private organizations. As a result, 266 facts of administrative violations, were detected, 72 of these facts resulted in the imposition of a fine and 61 facts resulted in the issue of a warning. The Office was unable to impose a liability on 67 violations due to the expiration of the 2-months statute of limitations. Additionally, 316 recommendations and mandatory instructions were issued.

PRIVATE SECTOR



- Hotel
- Commercial Bank
- Microfinance Organization
- JSC Creditinfo Georgia
- Debt Collection Companies
- Gambling Games and Online Services
- Marketing Companies
- Trading and Service Providing Companies
- Communication Companies
- Private Universities and Educational Institutions
- Healthcare, Insurance, Pharmaceutical and Aesthetic Organizations
- Natural Person/ Individual Entrepreneur
- Other

PUBLIC SECTOR



- Election Subjects/Election Administration
- Ministry of Health and its Legal Entities of Public Law
- Public School
- Local Self-Governments
- Ministry of Finance and its Legal Entities of Public Law
- Prosecutor's Office of Georgia
- Ministry of Justice and its Legal Entities of Public Law
- Ministry of Internal Affairs and its Legal Entities of Public Law
- Ministry of Corrections and Probation/Special Penitentiary Service
- Security Service and Operative-Technical Agency
- Other

Importantly, against the increase in the number of citizens' complaints and conducted inspections, for the first time during the last 6 years a decrease in the number of violations and fines was observed. The level of awareness on data protection issues in the public sector, large and medium sized enterprises, as well as the interest in prior consultations with the Inspector's Office have significantly intensified. The increase in the citizens' active attitude is also important: an essential portion of more than 6100 consultations in 2018 was provided to the citizens.

Along with the progress, challenges remain in private, as well as in public sector, such as verification of information in databases in the absence of a legal basis, unlawful disclosure of data, the need to demonstrate a greater caution in relation to children's data, etc. Issues related to processing of voters' data were especially outstanding and are discussed in a separate chapter of the report.

The Inspector continued cooperation with the Parliament of Georgia, executive government, the National Bank and other regulatory bodies in order to raise data protection standards on legislative and practical levels. Within the reporting period the Office introduced opinions in relation to 40 legislative initiatives and studied over 100 draft normative acts regulating various legal areas.

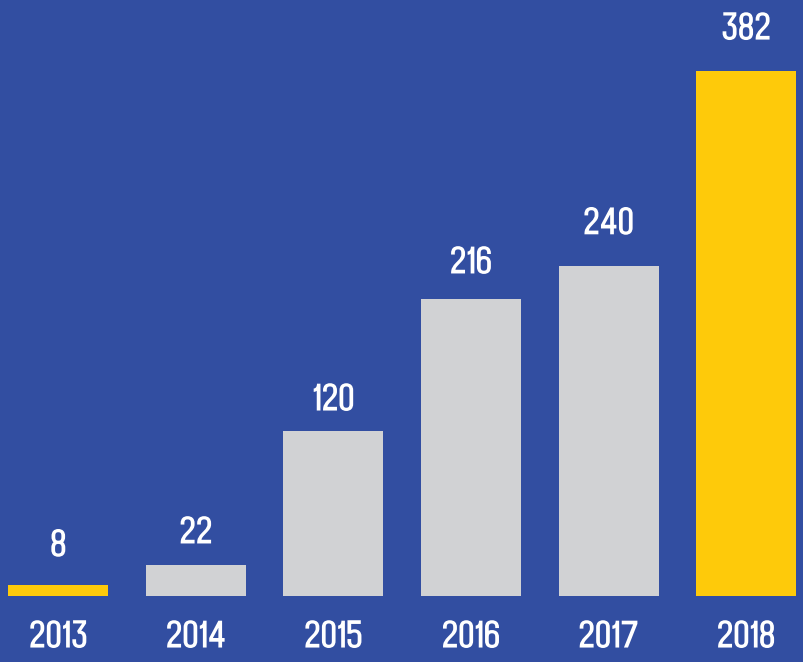
Throughout 2018 the Inspector's Office actively continued educational activities. As a result of trainings, 1200 private and public sector representatives were given an opportunity to gain and enhance knowledge on personal data protection issues. A series of trainings for self-governing bodies were conducted within the whole country.

Recommendations for healthcare and higher educational institutions were prepared and presented to the public. A guidebook on new EU regulation was drafted, translated and is available on the Inspector's web-page.

The Inspector's Office actively worked on raising awareness of citizens, as well. A number of meetings, events and campaigns were conducted. With the support of the EU and UNDP a new web-page was developed and adapted to the needs of disabled citizens. At the same time a new case management system was introduced that after the user's registration enables any type of communication with the Inspector's Office in a single online space.

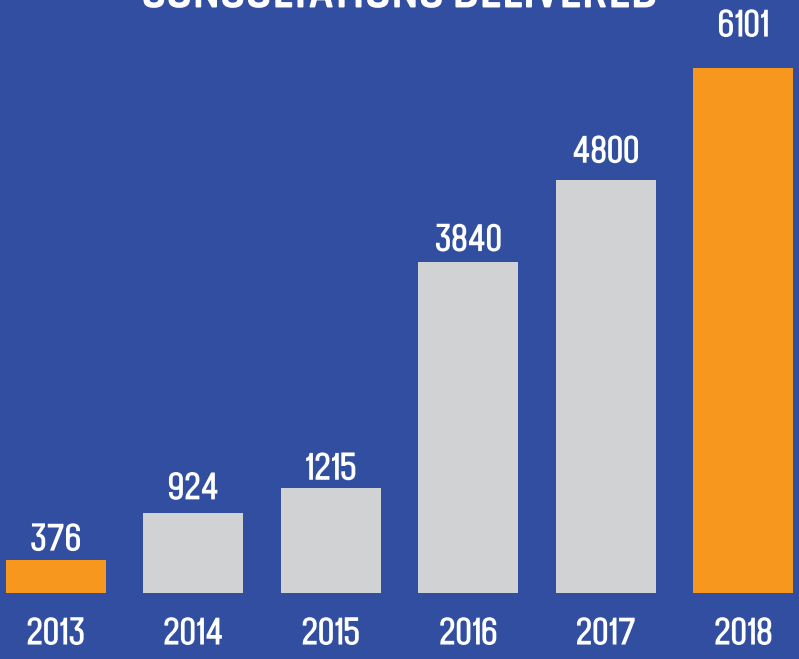
The Inspector's Office is still actively involved in the fulfillment of Georgia's international obligations, including the implementation of EU-Georgia Association Agenda. The Inspector was participating in international platforms and conferences, while in July 2018, at the plenary meeting of the Consultative Committee of the Convention 108 Tamar Kaldani was elected as a member of the Bureau and First Vice President. With participation of European experts, the Office prepared legislative proposals on the amendments to the Law of Georgia on „Personal Data Protection", that contribute to the harmonization of Georgian legislation with the European standards, fulfillment of the obligations laid down in the Association Agreement and improvement of the standards of personal data protection in the country.

CITIZENS' APPLICATION

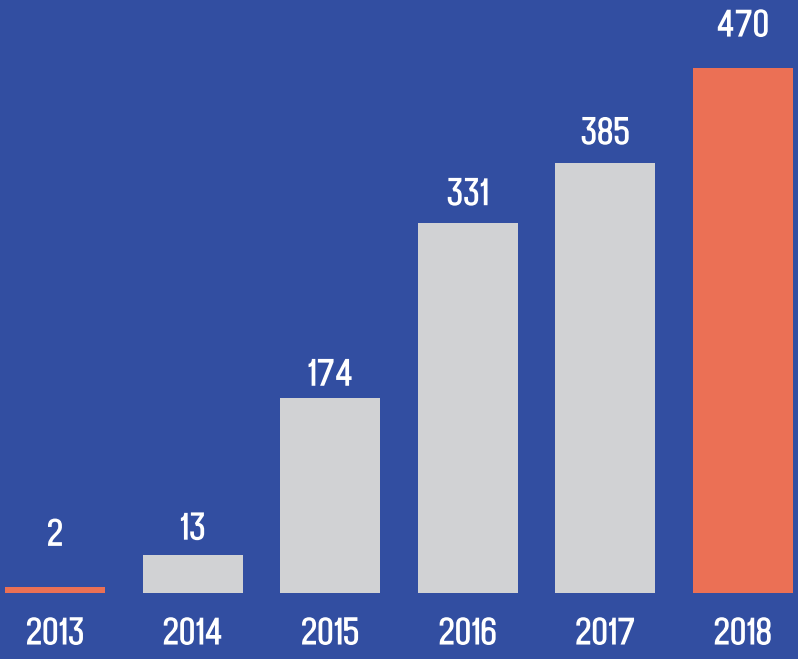


6 YEARS OF DATA PROTECTION

THE NUMBER OF THE CONSULTATIONS DELIVERED

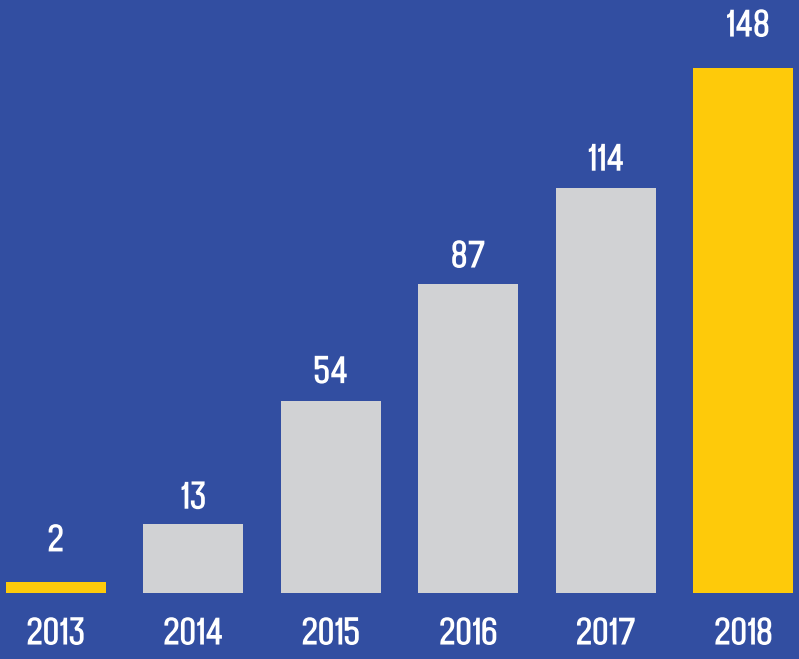


THE NUMBER OF STUDIED PROCESSES

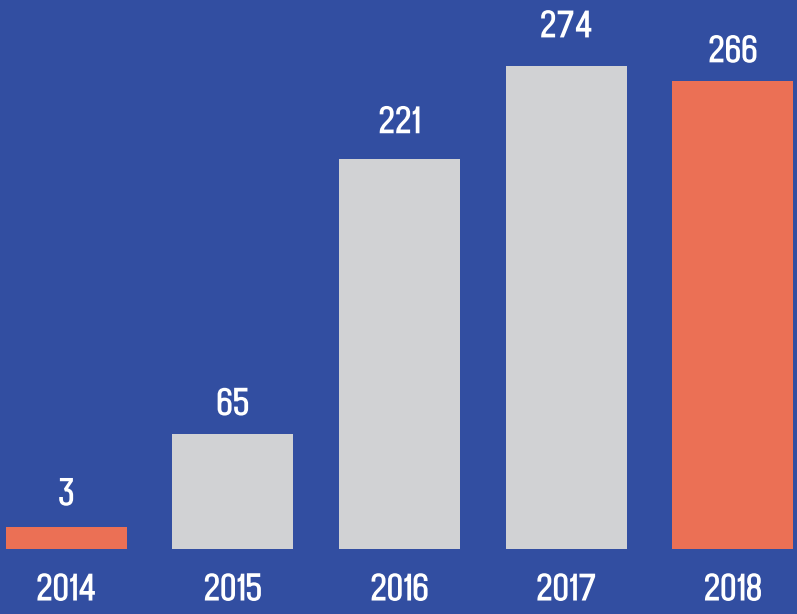


6 YEARS OF DATA PROTECTION

THE NUMBER OF INSPECTIONS

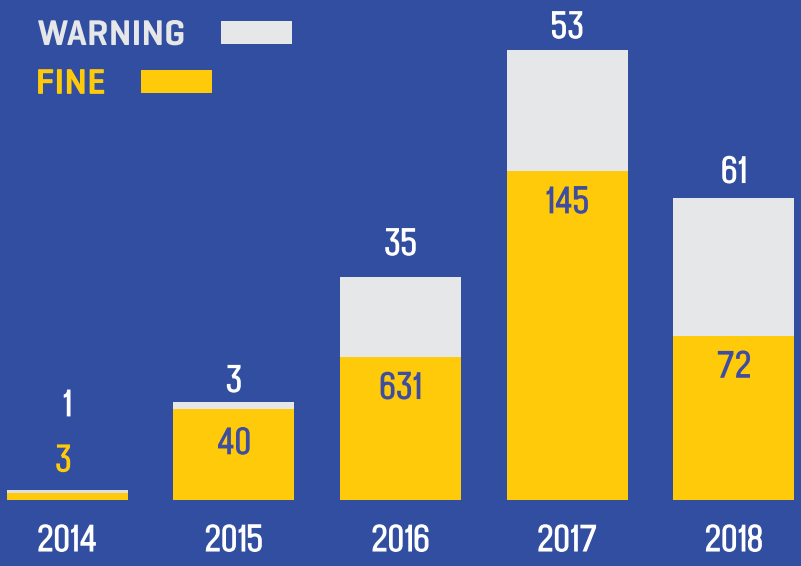


THE NUMBER OF REVEALED ADMINISTRATIVE OFFENCES

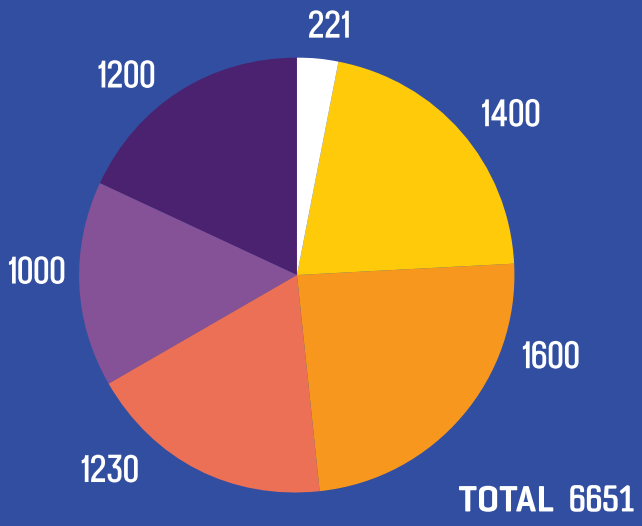


6 YEARS OF DATA PROTECTION

INTERRELATION OF IMPOSED ADMINISTRATIVE SANCTION – PENALTY/WARNING

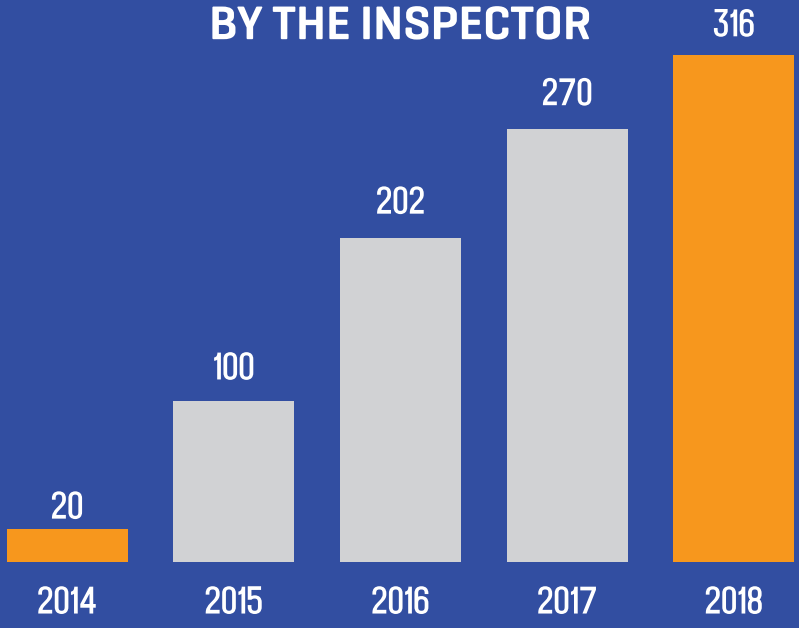


THE NUMBER OF TRAINING PARTICIPANTS



6 YEARS OF DATA PROTECTION

THE NUMBER OF INSTRUCTIONS/ RECOMMENDATIONS ISSUED BY THE INSPECTOR



DATA PROCESSING IN PUBLIC SECTOR

3

DATA PROCESSING IN PUBLIC SECTOR

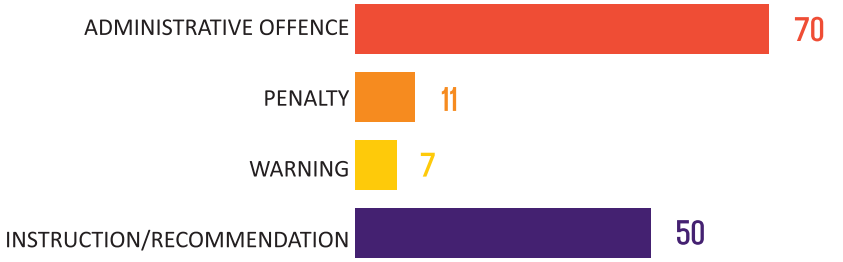
Ensuring protection of a person's right to privacy and personal data is an essential guarantee in the process of strengthening citizens' trust in public institutions. The activities of the public institutions and data processing rules they have to comply with are mostly directly regulated by legislation. However, several problematic issues were identified within the reporting period that point to the need of implementing effective legal as well as technical and organizational measures for the protection of personal data and the need to enhance the awareness of public servants.

In 2018 several facts were revealed where public servants accessed to personal data held in the databases of public institutions for unofficial purposes and breached data confidentiality. Remarkably, public bodies responded with disciplinary sanctions to the mis¬conducts by public servants that were revealed by the Inspector's Office. However, to prevent access to data for unofficial purposes it is essential to strengthen internal control mechanisms.

Within the reporting period the Inspector studied 115 data processing operations by ministries, election administration, courts, local self-governing bodies, legal entities of public law, including Civil Service Bureau, public schools and state universities. In response to 70 administrative offences, fine was imposed on 11 occasions and a warning was issued in 7 cases. Due to the statute of limitations the Office was unable to impose an administrative penalty in response to certain violations. However, 50 recommendations and mandatory instructions were issued.

2018 was marked with an increasing number of public institutions seeking consultation. Last year the Inspector's Office provided public institutions with 915 consultations. Tens of trainings and working meetings were conducted for 750

THE INSPECTOR STUDIED 115 DATA PROCESSING OPERATIONS IN 2018



representatives of 51 municipalities, National Archives of Georgia, Ministry of Defense of Georgia, the Parliament of Georgia, Ministry of Foreign Affairs of Georgia and various public organizations.

It should be highlighted that similar to the last year, a progress is notable in determining by public institutions the basis and volume of data processing and the period of data storage. However, certain shortcomings are in place (including the need to demonstrate a greater caution when dealing with minor's data), a part of which are presented in the report in the form of specific cases.

PUBLIC SECTOR, 2018

915 CONSULTATIONS WERE DELIVERED

750+ REPRESENTATIVES OF VARIOUS INSTITUTIONS ATTENDED THE TRAININGS

DATABASES MAINTAINED BY PUBLIC INSTITUTIONS AND DATA SECURITY

Public institutions develop databases with high volumes of personal data for the effectiveness of educational, employment, health and social care systems, accessibility of state services, ensuring citizen's security, protection of rights, administration of incomes and taxes, conducting democratic elections, fighting against corruption or for other legitimate purposes laid down by law.

Security of information contained in databases, protection of personal data against accidental or unlawful disclosure and use is an obligation of any data processing organizations, including public entities. Underestimation of the risks or implementation of insufficient organizational and technical measures may create a threat of unlawful processing of data and cause a reputational damage to public institutions as well as to the interests of citizens concerned.

Due to the volume of data contained in the databases and the ability to easily locate them, a regular monitoring of access to personal data in these databases is of key importance to ensure the security of data held by public institutions. At the same time, to prevent processing of data by the employees for personal purposes, it is significant to properly inform them of the data processing rules and consequences.

In the reporting period a citizen addressed the Inspector and claimed that an employee of one of the ministries, possibly with an abuse of official position, unlawfully obtained personal data concerning her. Within the framework of handling the complaint it was determined that a person employed at a ministry used the so-called Digipass under his responsibility for personal purposes and collected the complainant's data. In relation to the said fact the Ministry conducted an official inquiry and imposed a disciplinary liability on the public servant concerned.

One of the citizens claimed that the Ministry of Labor, Health and Social Care of Georgia made his written reference available to the persons named in the same reference. In demonstration of the mentioned fact

the citizen presented a photo material depicting a private communication between several persons in the social network – "Facebook". The participants of the communication discussed the issues raised by the complainant in the written reference addressed to the Ministry and named the author of the reference. In result of handling the complaint it was revealed that the written reference was related to the issues of possible HIV/AIDS infection risks. The Ministry sent the letter for further action to LEPL National Center of Decease Control and Public Health. To verify the facts indicated in the reference, LEPL in turn sent the reference to contractor organizations. According to the agreement concluded between the Center and contractor organizations, their obligation was to prevent HIV/AIDS, mobilization of the community members under the risk of the infection and providing them with accessibility of medical care. In the current case, seeking additional information from the contractors was possible without the identification of the author of the reference, especially considering that the content of the letter created the risk of a certain damage to the author. Notably, in response to the Inspector's instructions, the Ministry determined the need to implement certain organizational and technical measures to ensure the lawfulness of data processing.

A number of citizens addressed the Inspector and indicated that the former manager of one of the public institutions disclosed on "Facebook" page their personal data held by the same institution. The complainants claimed that by the time their data were disclosed the said person no longer served as the manager of the public institution. Therefore, it was unclear on what basis the said person had access to their personal data held by the institution. The disclosed information also contained a report on disciplinary proceedings conducted against one of the complainants. In result of the inquiry it was determined that the basis for dismissal of complainants from their positions at the public institution, including the report of disciplinary proceedings conducted against one of the complainants was known to the former manager by virtue of the official position. By the time the complainants' data were disclosed the person had already resigned from the official position and was no longer acting on behalf of the public institution. In the process

of the inquiry the former manager of the public institution insisted that by the time of publishing the so-called post, he was no longer bound by the obligation of tolerance and was acting as an individual. At the same time, the manager claimed that due to the information disclosed at the complainants' initiative in the media, he had a legitimate interest of providing the public with correct and true information.

It is notable that according to the Law of Georgia on „Public Service", while exercising official authority, as well as after dismissal, a public servant is obliged not to disclose the information that he/she became aware of in relation to exercising official duties. It should be highlighted that according to the regulations of the institution at issue, an employee had an obligation of passing the official documentation to the office after leaving the official position.

In the case at hand, the Inspector's decision ruled that the former manager of the institution had a legitimate interest of making clarifications in response to the information disseminated by the complainants in the media. However, the Inspector considered the disclosure of the report on disciplinary proceedings conducted against the other complainant unlawful and disproportionate. Therefore, the former manager of the institution was found to be responsible for administrative violation in relation to the disclosure of the report on the disciplinary proceedings. He was also ordered to delete the disclosed information. As for the public institution, it was recommended to determine the legal mechanisms of responding to violations of internal regulations.

In order to ensure security of data:

- It is desirable that organizations adopt internal policies, regulating the issues of data security and mechanisms for prevention of unauthorized access;
- Organizations should inform employees about data security rules and establish, as required, different levels of their access to data;

- Organizations should grant the employees an authorization to access databases only with an individual username/password and/or via a personalized Digipass;

- Organizations should record any activity in relation to the data in order to enable identification of a person responsible for specific action.

According to Georgian legislation, databases with a high public interest in the information held there, are considered public. Accordingly, public entities ensure their accessibility by publishing them on relevant web-pages (for example, www.napr.gov.ge; www.voters.cec.gov.ge; www.declaration.gov.ge; www.privatization.ge, etc.). Notably, legislation regulating these databases does not as a rule envisage restrictions on the use of data contained in the databases. Therefore, the technical features of the web-pages do not provide sufficient mechanisms to restrict collection of data.

Cases examined and circumstances revealed in the reporting period point to the fact that notwithstanding the existence of essential legitimate purposes of availability of personal data for the development of a democratic society, availability of personal data on the internet often causes certain awkwardness and in certain cases a damage to data subjects.

In the reporting period the Inspector's Office studied a number of databases that are publicly available on the statutory basis, including the following:

In the course of handling one of the complaints it was determined that it is possible to look up the names, surnames and personal identification numbers of the persons that won an auction related to management-disposal of state property at www.privatization.ge**. As the information availability period is not determined, the data of the winners of auctions are being published for uncertain period of time. At the same time, the web-page lacks a feature protecting from search engines and it is easily possible to obtain the personal identification number by indicating a data subject's full name in any search engine.**

This is the case where a legitimate basis for publishing personal data exists, however, determining the period for publishing the information

about auctions is part of competence of privatization authority. Accordingly, the Agency was instructed to determine the period of availability of data for publicity, transparency and other legitimate purposes and to implement such organizational and technical measures that restrict the easy availability of the concerned person's personal identification number in search engine.

A lot of citizens express their interest in the availability of data in the registry of entrepreneurial and non-entrepreneurial (non-commercial) legal entities and the database of real estate by LEPL National Agency of Public Registry. According to the applicable legislation, LEPL National Agency of Public Registry's web-page publishes the data of real estate owners, owners, managers and representatives of private organizations, also documents of an organization's registration documents, including a copy of the ID document of the petitioner. It was determined that a certain non-commercial organization collects the data available on the said web-page via a special algorithm and publishes them on its web-page in a form that is easier to access, in comparison to the Registry. By indicating a person's identification data in the search options it is possible to obtain a comprehensive information related to a person. Unlike www.napr.gov.ge, the web-page has no features restricting the access of search engines and the information becomes available by simply indicating just the full name of a person in any search engine. Due to the fact that the applicable legislation enables the use of public data and the web-page serves the purpose of transparency, no violation of data processing rules was found in publishing the Agency's data on a private organization's web-page. However, the organization was given a recommendation to generally asses the criteria of algorithmic availability of data published on the web-page and security issues.

The reporting period revealed a number of facts of using the data (photo, registration address and data of the persons registered with voters at the same address) from the voters' list published on the web-page of Central Election Commission of Georgia (CEC) for different purposes. The said database is actively used by the so–called debt collecting companies and private detectives. Although the page that is designed

for verifying the voters' list states that "the web-page is designated for voters only – to check their own and family members' data!", the legislation does not impose a restriction for further processing of the published data.

www.declaration.gov.ge – a web-page owned by LEPL Public Service Bureau publishes asset declarations of officials, that also include information about the identity, employment, incomes, place of residence and properties of the officials' family members. Bureau's web-page contains declarations submitted since 1998, including those of deceased and former officials (who have been resigned from office for tens of years). Provided that the purpose of publishing asset declarations of officials is to combat corruption, reveal the facts of illicit enrichment and conflict of interests, it would be advisable for the legislators to consider whether the accessibility of the data of deceased and former officials on the internet for an uncertain period of time is necessary for the legitimate purpose. Indeed, this should be without prejudice to the possibility of obtaining the declarations in the form of public information in case of relevant interest. Another issue revealed in the process of inspecting the Public Service Bureau is the possibility of the data subject to rectify inaccurate data. The Bureau was instructed in accordance with the applicable legislation to develop a mechanism for rectification of an inaccuracy/inaccurate data reflected in a declaration, to determine a rule of identification of an official and to ensure that data subjects are clearly informed about the possibility to update the declaration data and password.

It is important that the applicable legislation corresponds to the modern challenges related to the protection of personal data and privacy and maintains a fair balance between the public interest of the availability of information and the right of data subjects to the protection of privacy.

In case of publishing databases, it is advisable, that the legislation clearly establishes the volume of data published for legitimate purpose, criteria for their search (including through search engines), purposes of their further processing and terms of their publication.

PROCESSING OF MINORS' DATA

Information related to minors merits particular protection. Schools that store high volumes of personal data, including special category of data about pupils, have a particular responsibility in this regard, due to the fact that unlawful processing, in particular disclosure of those data might irreversibly affect the future life of a minor, restrict his/her right to privacy and right to free personal development.

Last year, on the basis of citizens' complaints and references from the Ministry of Education and Science the Inspector's Office inquired into the lawfulness of personal data processing by 8 public schools and established a number of facts of processing data in infringement of the law:

One of the cases examined by the Inspector concerned a victim of violence whose parent was forbidden to communicate with and approach the child on the basis of a restraining order. The child was living at a shelter and was in foster care by the state. In the best interests of the child it was considered advisable to relocate the child (to another city) and to change the school. However, the parent learned the address and made an appearance at the school. In the process of handling the case it was determined that the school failed to respect the confidentiality of information about relocation. In particular, the school handed over the student's documentation in an unsealed envelope to an unauthorized teacher to submit it to a postal service center. Disclosure of information about the child's location essentially damaged the child's interests, endangered the child's physical safety. The school was ruled to be responsible for administrative violation. On the basis of the Inspector's instructions, the school implemented various organizational and technical measures, namely: a meeting was held with the school's every staff member in relation to data protection issues; established the rule of data confidentiality in its internal regulations; purchased relevant envelopes and laid down a procedure of sending correspondence via a courier in a closed format.

One of the parents informed the Inspector, that a certain public school provided a journalist with a statement that contained the personal data of a child. The statement was regarding a conflict between the student and classmates. It was revealed that it was the headmaster who presented the statement to the journalist and gave permission to take a photo of the statement. The journalist in turn published the material in the form of an article. The school was found responsible for administrative violation, fined and was instructed with the view to prevent further violations.

Processing minor's personal data requires the following:

- Organizations should take into consideration a minor's best interests and his/her opinion, in accordance with one's age and maturity;
- Educational institutions should regularly provide for raising data protection awareness of the employees;
- To prevent violations during processing of minor's data and to ensure data security, it is necessary that organizations duly monitor data processing operations and provide an adequate response to revealed violations.

RIGHT TO ACCESS TO PERSONAL DATA HELD BY PUBLIC INSTITUTIONS

Article 18 of the Constitution of Georgia guarantees a person's right to get acquainted, in accordance with the statutory rules, to the information or official document related to him/her and held by public institutions, except when it contains a commercial or professional secret or when it is classified as a state secret to protect the necessary state or public interest or the interests of legal proceedings in a democratic society, in accordance with the law or a legal procedure. This right of a person, rules and conditions of its realization are strengthened by Article 21 of the "Law of Georgia on Personal Data Protection". Data controller has an obligation to provide a data subject with information about the processing of data concerning him/her in a chosen form and within the terms laid down by the law.

It should be noted that for the purpose of informing data subjects the legislator sets comparatively higher standards for public institutions. In particular, a public institution has on obligation to provide a data subject, on request, not only with information, but also to provide copies of data concerning him/her free of charge (except the data which is subject to a fee payment in accordance with Georgian legislation). Providing a data subject with proper information in a timely manner is directly linked to the realization of other rights laid down by the law, for example, to the right of erasure and rectification of inaccurate data and the right to appeal. Failure to be informed within reasonable terms might considerably damage the interests of a citizen.

Within the reporting period, certain shortcomings were identified in relation to informing data subjects:

A person that addressed the Inspector's Office with a complaint claimed that he had requested from the archive of LEPL Department of Common Courts the copies of files on a criminal case that resulted in his conviction. The letter of response explained that the requested case files were held at the Department in the form of 1 volume, a fee to copy the files constituted GEL 15.65 and the citizen would be provided with the copies only after the submission of a payment document. Within the framework of the inquiry it was established that the applicable legislation did not envisage a fee for the provision of the requested documentation. Furthermore, the Law of Georgia on "Fees for Copying Public Information" unambiguously states that no fee is envisaged for individuals for copying personal data concerning them held by public institutions. At the same time, in accordance with the Criminal Procedure Code of Georgia, a convicted person and/or his/her lawyer enjoy the right to receive certified copes of evidence and files in relation to a criminal case when a prosecutor has issued a decree on an essential violation of a convicted person's rights in the process of legal proceedings conducted against him/her. Notably, the public institution in question remedied the shortcoming in the process of handling the complaint and fully provided the complainant with the requested copies of case files free of charge.

Representative of a certain minor addressed the Inspector and indicated that with a view to protecting the interests of the child he repeatedly requested LEPL Social Service Agency for documents reflecting the measures taken in response to the possible violence against the child. However, the Agency was delaying the answer. Within the framework of examining the complaint it was revealed that together with other documents concerning the child in question, the Agency held a record of an emergency response filed in relation to the fact of possible violence against the child that reflected the circumstances related to the possible violence against the data subject and recommendations for improving the conditions of the child. In infringement of the terms of informing, the Agency provided the complainant with certain document, however, contrary the request, failed to provide him with the record of an emergency response. The Agency cited that the record of emergency response constituted the Agency's internal document and in accordance with the applicable legislation an internal document could not be submitted to a third party. It was determined that in consideration of the content of the record of emergency response, the child's representative had a direct interest in obtaining it since the document reflected the immediate actions taken by the Agency in relation to the alleged fact of violence against the child and recommendations. At the same time, the applicable legislation provides for the access of a child's parent and/or representative to the confidential information related to a possible violence. The institution was found to be responsible for administrative violation and was instructed to implement the relevant measures with the view to providing data subjects with comprehensive and timely information on request.

Apart from the mentioned cases, the Inspector handled complaints by a number of citizens concerning the infringement by public institutions of the statutory term for providing data subjects with information. On certain occasions public institutions provided data subjects with information concerning them long after the expiration of 10-day period laid down by the law. They explained the reasons of the delay with a heavy workload of the employees and the fact that a 10-day period might not be sufficient to provide comprehensive information. Upon the Inspector' s decision the relevant public authorities were instructed to imple-

ment the measures that will contribute to a timely and effective realization of data subjects' rights.

Each public institution, in consideration of its principles of operation, should adopt such mechanisms as to ensure that data subjects are provided with information/documents established by Article 21 of the Law of Georgia on "Personal Data Protection" in a comprehensive and timely manner. Such measure might be a designation of a person responsible for the implementation of the rules on requesting/providing information and/or for duly informing data subjects.

PARTICIPATION IN LAW-MAKING ACTIVITIES

Last year the Office was actively engaged in the law-making process and cooperated with legislative and executive government bodies. The employees of the Inspector's Office participated in working meetings, committee discussions and other formats. In order to ensure compliance with data protection legislation, the Office submitted opinions regarding 40 legislative initiatives and studied over 100 draft laws and bylaws regulating various legal areas. The mentioned draft documents were related to educational, financial, audit, archiving, electoral and other activities; healthcare, public security, electronic communications, minors, disabled persons and other issues.

The following draft documents should be highlighted:

Draft Order of the Minister of Internally Displaced Persons from the Occupied Territories, Labor, Health and Social Affairs on "Establishing the Rules of Functioning and Operation of Electronic Health Records (EHR)". The purpose of the EHR system is to collect from authorized persons, store and enable the sharing of the electronic records of a patient's health in accordance with the established rule and therefore contribute to the development of a continuous, effective, patient-oriented, quality and integrated healthcare system. The system contains a detailed information about a patient: medical history of life, information about the provision of healthcare services, diseases, hospitalization and information collected during an outpatient visit.

To ensure proportionate processing of data, security of data and prevention of unauthorized access to data, the Ministry was recommended to establish a clear distinction between the levels of access to the system, lay down the procedures for erasure/rectification of data, detailed organizational and technical security measures and persons responsible for monitoring these measures.

Regulation of minors and disabled persons' legal safeguards by various public institutions was an outstanding issue within the reporting period. Consideration of the best interests of a child in data processing is also indicated in EU Data Protection Regulation, that obligates data controllers to pay a considerable attention to the processing of a child's data and take consideration of a child's best interest in this process.

Within the reporting period the Office examined draft orders submitted by the Ministry of Education, Science and Culture and the Ministry of Internal Affairs on the "Adoption of the Rules and Conditions for Protecting Security and Public Order in Secondary Educational Institutions" and on the "Adoption of the Rules on Coordination and Exchange of Information between the Ministry of Internal Affairs, the Ministry of Education, Science and Culture and LEPL – Office of Resource Officers of Educational Institutions". On the one hand, the Inspector's Office shared the opinion of the ministries regarding the need to exchange information between the relevant agencies and planning various preventive measures with the view to improving the safety of educational institutions and protecting public order. On the other hand, in the best interests of the protection of children's data and to ensure the protection of their privacy, the Office provided the agencies with recommendations in relation to minimization of the volume of data intended to be processed and clarification of specific processing purposes.

PROCESSING OF VOTERS' PERSONAL DATA

4

PROCESSING OF VOTERS' PERSONAL DATA

For the last 2 years, protection of voters' personal data during election period is one of the outstanding issues. Voters' lists near the polling stations, processing of voters' personal information directly on the polling stations, sending text messages by candidates and disclosure of information about the donors of candidates – this is an incomplete list of the issues that the Inspector's Office handled during 2018.

VOTERS LIST AND DESK LISTS

Processing of voters' data on the election day became an outstanding issue since the local self-government elections in 2017. Media outlets and observer organizations spread information about the representatives of political parties or other observers on polling stations copying voters' registration numbers of the voters who came to the polling stations directly from the desk lists or taking photos of the voters' list. By checking this information in the lists outside the polling stations, they had an opportunity to determine the names, surnames and addresses of the voters who appeared at the polling stations. The Personal Data Protection Inspector addressed this issue in an announcement on the election day, two days after the elections started to examine the issue and completed the process in first half of 2018.

In accordance with legislation, representatives and observers involved in election process have an opportunity to fully observe the whole election process, including an opportunity to collect information in order to file a complaint in relation to the voting process and procedural issues. Conferring a vast authority to the election observers stems from the essential public interest and serves the purposes envisaged by the Constitution and the Election Code of Georgia. However, for ensuring a democratic process it is essential to provide for the protection of the voters' personal data.

During the October 2017 elections there was no legal act that established an opportunity, specific rules and conditions for election observers to record personal data. Upon the Inspector's decision the election administration was instructed to assess, what type of personal data an observer should be able to record and to establish such organizational and technical measures ensuring that the persons authorized to be present at the polling stations process the data to the extent that is adequate and proportionate to the purposes of processing and preventing the risks of monitoring voters' will.

It is notable that the Election Administration took the Inspector's instructions into account and within the reporting period relevant amendments were made to the organic Law of Georgia - "Election Code of Georgia". The amendments regulate the rules of photo/video recording at the polling stations and restrict further processing of data that are not public information in accordance with the law.

As a result, during 2018 presidential elections collection of voters' data by the observers directly at the polling stations was no longer and outstanding issue. However, different questions were raised in relation to the processing of voters' data.

In particular, on the election day of 2018 presidential elections media outlets spread information about coordinators of election candidates and political parties at the polling stations were holding voters' lists with voters' photos. It was alleged that it was the so-called desk lists that had been unlawfully obtained.

Based on the information received from Election Administration within the framework of the inquiry the Inspector's Office determined that in accordance with the rules established by the Election Code throughout 2018, the version of the voters' list with photos was submitted to 11 electoral subjects, including 6 political parties and 5 observer organizations.

The list of persons authorized to obtain the list with photos is determined by the applicable legislation. In particular, according to the organic Law of Georgia - "Election Code of Georgia", registered party, electoral alliance, initiative group of voters, an organization with observer status under the law and voters have a right to have access to the version of the voters' list that is considered public information and is held at Central Election Commission, district election commissions and the precinct election commissions and in case of revealing inaccuracies, request to rectify the data related to the voters and the voters list itself. At the same time, the named persons are provided with the public version of the voters list containing photos in electronic format only. To obtain the list, an authorized person must submit to the relevant election commission an electronic data carrier of a sufficient capacity. Further processing, e.g. alignment of the data transferred in electronic format in accordance with election districts or other criteria is easily possible.

In line with the existence of a legal basis for data processing, the Law of Georgia on "Personal Data Protection" requires observation of data processing principles and security rules too. However, "Election Code of Georgia", while granting the named persons an opportunity to obtain the unified list of voters, fails to establish the rules and restrictions for using it. It is essential that the mentioned issue is regulated on a legislative level, including, the determination of legitimate purposes for processing data prior to the elections and on the election day and obligation of the persons who receive the voters' list to implement organizational and technical measures to ensure the safety of personal data.

It should also be noted that according to the legislation, the unified list of voters is published on the web-page owned by the Central Election Commission - www.voters.cec.gov.ge, where after indication of a personal number and surname and after filling the "I am not a robot reCAPTCHA" security field, voters' personal data, including name, surname, photo, date of birth and address, become available to any interested person. It is indicated on the web-page that the list is only for the voters' purposes - to check themselves and their family members. However, considering the growth of technological opportunities the mentioned security mechanism might not be sufficient to ensure the adequate protection of voters' data from unlawful processing.

In light of the aforesaid, it is important to re-evaluate the applicable regulations and existing challenges, to implement legal and practical measures with participation of the parties concerned and with the view to establishing the standards and security measures for the protection of personal data in the election process to prevent the excessive processing of data by unauthorized persons.

PROCESSING OF DATA AT PRECINCT ELECTION COMMISSIONS

According to the Elections Code of Georgia, the precinct election commissions are provided with unified and special lists of voters, intended for the commission as well as a public version. On the basis of these lists the district election commissions must compose the list for mobile ballot boxes. Due to the fact that the voters list designated for public view does not contain personal identification number, the list of a mobile ballot box that is later published at the polling station in a public available format should also not contain the voters' personal identification numbers.

In the reporting period one of the journalists provided the Inspector's Office with a notification that a list of mobile ballot boxes at the polling stations of certain election districts in Ozurgeti and Chokhatauri municipalities besides names and surnames also displayed personal identification numbers. Within the framework of the inquiry the Office determined that the lists of mobile ballot boxes (that besides names and surnames, also contained personal identification numbers) were displayed on the inner walls of the polling stations in a form accessible to third parties. According to the clarifications received from the Election Administration, personal identification numbers in the list of voters signed up for mobile ballot boxes on the inner walls of the polling stations, were included by mistake. In light of the aforesaid, upon the Inspector's decision the disclosure of voters' personal identification numbers by Central Election Commission was ruled as a violation of the Law of Georgia on "Personal Data Protection".

DISCLOSURE OF INFORMATION ABOUT FINANCIAL INDEBTEDNESS WITHIN THE FRAMEWORK OF ELECTORAL DONATIONS

In October 2018 a media outlet spread information that the employees of a clinic had transferred certain funds to a presidential candidate as an electoral donation. Information about the donators' financial state, including credit history, amount of loans and other details were also disseminated through the TV channel. The media outlet did not disclose the source of information.

According to the applicable legislation, information related to a financial declaration (including source and amount of donation and the date of receiving) of a political party/electoral subject is open to any interested party. However, at the same

time it is established that public information on donation is limited to a person's name, surname, personal identification number and place of registration and does not include accessibility of data related to a person's financial state and indebtedness. It should hereby be taken into account that if lawfulness of a donation is under question, responding to the alleged violation falls under the competence of the State Audit Service.

Provided that JSC Creditinfo Georgia is a credit bureau holding a database of credit information, to verify the lawfulness of access to and disclosure of the information containing personal data of the individuals named in the story covered by the TV channel, at the Inspector's initiative an inspection was launched at JSC Creditinfo Georgia.

As a result of the inspection it was established that the donators' credit history held in the database of JSC Creditinfo Georgia had been at the material time checked by a microfinance organization. The donators were not the clients of the mentioned microfinance organization, they had never consented to processing of their personal data and they were not aware of the purposes and legal basis of checking their credit information by the microfinance organization in question.

Within the framework of the inspection, the microfinance organization at issue confirmed the fact of checking the personal data in the database of JSC Creditinfo Georgia. However, they explained that these actions were not in conformity with the purposes of the company's activities, they were not authorized by the management and were a personal initiative of a certain employee.

According to the company, due to acting without the authorization of the management and for violating the procedures laid down by the company, two employees were dismissed from their positions.

PHONE COMMUNICATION WITH VOTERS

Sending SMS by electoral subjects to voters during the presidential elections remained an outstanding issue. Notwithstanding that in cases at issue the electoral subjects had no direct access to the data when sending SMS and they were sent through intermediary companies (on the basis of a written agreement), and they contained a statutory opt-out mechanism, the said practice of communicating with the citizens often raised questions about the lawfulness of obtaining the data.

On the basis of the citizens' reports it was also established that they were contacted from various phone numbers and without introducing themselves/organization the callers would ask if they attended the elections. Within the framework of examining the case at issue it was determined that the members of a non-entrepreneurial (non-commercial) legal entity contacted selected citizens (generally, acquaintances and friends), to determine the voter turnout, however processing of personal data, including storing information about political opinions and phone numbers, did not take place.

Each electoral subject and observer organization that during elections collects data directly from voters is obliged under the law to explain to them the purpose of data processing in advance in order to enable the citizens to make an informed decision. During elections it is particularly important to protect voters' personal data since a person's political views fall into the special category of data and higher standards apply for their protection.

Accordingly, electoral subjects and observer organizations that process voters' personal data via telephone surveys, should provide them with detailed information, including on the identity of the person/organization that collects their data and how their data are planned to be used in the future.

At the same time, electoral subjects have to record the sources of data, determine the types of data needed to be collected to meet the legitimate purpose and implement relevant rules that will minimize the risk of processing the data on their behalf.

In similar cases it is equally important for the citizens to take into account that they are not obliged to provide the data. It is a person's choice whether or not to give out personal information and to what extent.

PROCESSING OF DATA BY LAW-ENFORCEMENT AUTHORITIES

5

Photo from the archive of the Ministry of Internal Affairs of Georgia


POLICE

PROCESSING OF DATA BY LAW-ENFORCEMENT AUTHORITIES

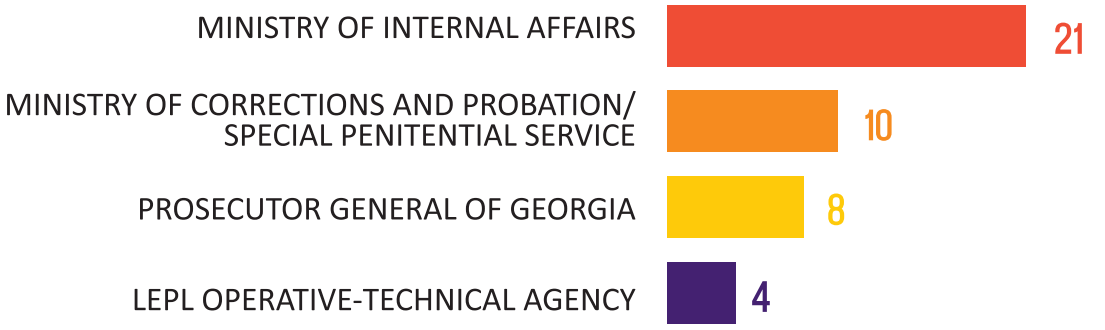
Processing of personal data by the law-enforcement authorities, that often represents an intrusion into the right to privacy guaranteed by Article 8 of the European Convention of Human Rights and Fundamental Freedoms and Article 15 of the Constitution of Georgia, should be based on a law, have a legitimate purpose and must represent a necessary measure in a democratic society. It is important that collection, storage and use of data by the law-enforcement, authorities was carried out in accordance with legitimate and clear purposes and in observance of the principles such as fairness and proportionality. At the same time, it is important to provide for the accuracy and authenticity of data and for the transparency of the general procedures related to data processing. Observance of the said rules by the law-enforcement authorities is of a particular importance since unlike other public bodies, within the framework of the authority vested upon them by the law, law-enforcement authorities have a possibility to collect and otherwise process the data obtained from open as well as covert sources, that in turn increases the risk of processing data without a legitimate purpose and beyond the necessary extent.

In the reporting period, within the process of handling 42 citizens' complaints and within the framework of 20 inspections the Inspector's Office examined up to 70 processing operations carried out by the law-enforcement authorities. Including the lawfulness of data processing by: Ministry of Internal Affairs in 21 cases, Ministry of Corrections and probation/Special Penitential Service, sub agency under the system of the Ministry of Justice of Georgia in 10 cases, Prosecutor General of Georgia in 8 cases and LEPL Operative-Technical Agency in 4 cases. Due to revealing components of a crime or for further response 7 cases were forwarded to the relevant law-enforcement bodies. Notably, in 2018 the Inspector's Office examined the lawfulness of data processing by all the investigative bodies envisaged by Article 34 of the Criminal Procedure Code of Georgia.

In order to respond to 39 violations revealed in the reporting period, a fine was imposed in 5 cases, a warning was issued in 2 cases and in 13 cases the liability could not be imposed due to the expiry of the statute of limitations.

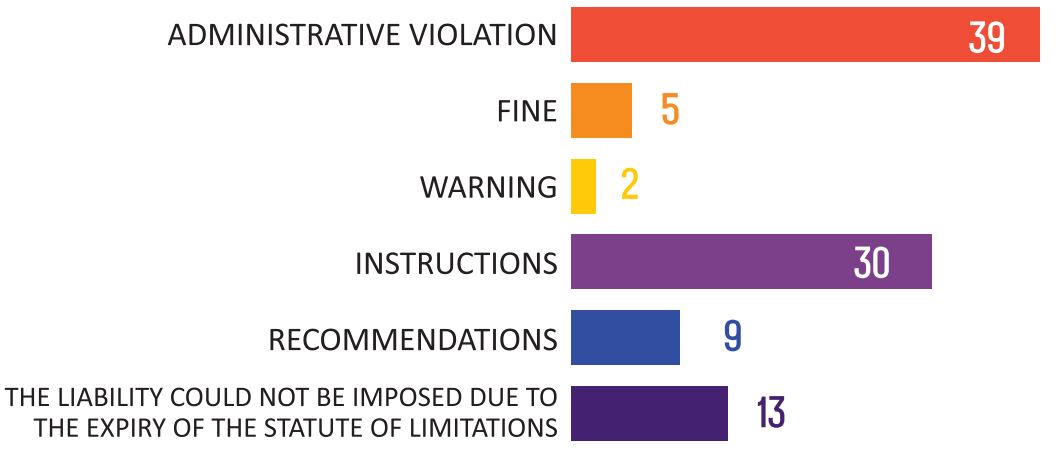
To improve data processing operations, the law-enforcement authorities were given 30 legally binding instructions and 9 recommendations. They were additionally provided with over 140 written and verbal consultations. A number of conclusions and recommendations were prepared on draft laws and normative acts related to the activities of the law-enforcement authorities.

IN 2018 THE INSPECTOR EXAMINED UP TO 70 DATA PROCESSING OPERATIONS CARRIED OUT BY THE LAW-ENFORCEMENT AUTHORITIES, INCLUDING:



In comparison to the previous years, the number of violations detected in the law-enforcement sector has significantly reduced, as well as the number of complaints submitted by defendants/convicts regarding the facts of processing data by penitentiary institutions through video surveillance or when exercising their right to a phone call. This in turn reflects the effectiveness of legislative amendments in this sector and the measures implemented by the authority. The interest of the law-enforcements in obtaining a written consultation of the Inspector's Office has also increased.

LAW-ENFORCEMENT SECTOR



However, simultaneously to the positive tendencies there are still certain issues that require additional efforts to improve the data protection standard in the law-enforcement sector. These issues are – checking, collecting, disclosure and storing contrary to the principles of the data held in the central databank without a legitimate purpose and legal basis, improper informing of data subjects, undue compliance with the obligation of informing the Inspector.

Observing data protection rules is particularly important against the increasing interest of the law-enforcement bodies to have access to various types and categories of data. For example, due to legislative amendments of 2018 the Ministry of Internal Affairs was granted an authority to access data held in the special electronic program of recording movable objects obtained by the creditors as a security for a monetary claim and to the data obtained by resource officers of educational institutions in the course of exercising their official duties. Against the challenges in the sphere of public security and order, access to data might be an important factor for effectively exercising the functions and duties vested upon these agencies by the law. However, it is necessary to observe a fair balance and the principle of proportionality at the same time.

COLLECTION OF COMPUTER DATA FOR INVESTIGATION PURPOSES

In comparison to the previous years, the cases of processing data without a legitimate basis within the framework of investigative activities related to computer data have significantly decreased. However, the fact of examining by the law-enforcements of a video recording held in the computer system of a private company, taking photos of specific segments and sending them over through communication channels in the absence of a court ruling and a prosecutor's resolution was revealed in 2018 too. In several cases private companies prevented violations by contacting the Inspector's Office and obtaining an immediate response from the Office. Provided that the Criminal Procedure Code clearly establishes that an investigative action related to computer data may be carried out only on the basis of a court ruling or in emergencies - on the basis of a prosecutor's decree, all the actions on the part of the law-enforcement bodies carried out in violation of the statutory regulations, was considered as data processing in the absence of a legal basis and sanctions envisaged by the law were used in response.

The positive tendency of decreasing violations related to obtaining computer data might be caused by the raised awareness on the part of the investigators and operative staff, as well as on the part of the private companies. The number of requests addressed to the Inspector's Office for consultations related to the collection of computer data has also increased. Aside from the Inspector's response, for a complete elimination of violations related to the collection of computer data, monitoring and undertaking preventive measures on the part of the law-enforcement authorities are also significant.

ACCESS TO DATA IN THE CENTRAL DATABANK AND SECURITY OF DATA

In order to effectively exercise the functions and duties vested upon the Ministry of Internal Affairs of Georgia, the ministry has created a central databank, that holds an extensive number of data, including special category of data.

In the reporting period on the basis of citizens' complaints the Inspector examined several cases of lawfulness of data access and consequently revealed certain occasions of accessing data for unofficial purposes and without a statutory basis.

In result of the internal inquiries carried out on the basis of the Inspector's reference, the Ministry's General Inspection established that one of the employees checked the data held in the central databank for unofficial purposes that was regarded as a flagrant violation of discipline which resulted in dismissing the employee from the office.

In the reporting period the Inspector's Office examined the measures implemented for the security of data held in the central databank. According to the legal acts and practical mechanisms, the Ministry has introduced the following organizational and technical measures: The Ministry's employees are admitted to the central databank on the basis of a substantiated written reference from the managers of the Ministry's structural units, territorial bodies, sub agencies and legal entities of public law via a device (DIGIPASS) for generating individual usernames, passwords and a one-time numeral password. Every action undertaken in relation to the data held in the central databank is subject to recording, which enables establishing the identity of the Ministry's employee who accessed the data and any action undertaken by him/her in relation to the data. The Ministry's employees are forbidden to collect, use or disclose the data held in the central databank for unofficial purposes. Obligation to monitor the said limitation is imposed on the managers of the Ministry's structural units, territorial bodies, sub agencies and legal entities of public law, as well as on the Informational-Analytical Department and the General Inspection (Department) of the Ministry. Processing of data held in the central databank for unofficial purposes creates the condition for imposing the statutory sanctions and/or severe disciplinary measures. As a result of the inspection, the organizational and technical measures implemented for the security of data held in the central databank were considered to be in conformity with the requirements of Article 17 of the Law of Georgia on „Personal Data Protection".

However, it should be noted that organizational and technical measures implemented for data security are a combination of complex measures and their adequacy and effectiveness is assessed on a case-by-case basis after a comprehensive, thorough and objective examination.

TIME-LIMITS FOR STORAGE OF DATA IN THE UNIFIED DATABASE FOR REGISTRATION OF ADMINISTRATIVE OFFENCES

According to the Code of Administrative Offences of Georgia, the Ministry of Internal Affairs of Georgia creates a unified database for registration of administrative offences which is composed of a detailed

information in electronic form submitted to the Ministry about the records and decrees of administrative offences drafted by the bodies that filed/examined the records of these offences. In accordance with the Georgian legislation the data held in the unified database were stored permanently, however by the decision №1/2/622 of February 9, 2017, the Constitutional Court of Georgia found the legal norm to be unconstitutional.

On the basis of a complaint of a certain citizen filed in the reporting period the Inspector examined the issue of permanent storage in the unified database (in an electronic form) of information about imposing on October 2007 on the said person of an administrative liability envisaged by Article 45 of the Code of Administrative Offences of Georgia. In order to comply with the decision of the Constitutional Court, the Ministry is working on determining the time-limits for the storage of data held in the unified database, however, the process of adopting the normative act or of making relevant amendments has not yet been finalized.

In result of the examination it was established that by the time of examining the case at issue, the purpose determined by the Code of Administrative Offences of Georgia for storing the data about imposing administrative liability on the said person in the unified database had been served. It should also be taken into account in this regard that in accordance with international standards and the decision of the Constitutional Court of Georgia, if relevant legal conditions exist, data subject has a right to request the erasure of data related to one's past actions in order to avoid a regular or recurring stigmatization by the society and to determine one's private life autonomously. Accordingly, in consideration of the mentioned circumstances, the Inspector found the storage of data about imposing on the complainant of an administrative liability from October 31, 2007 in the unified database of the Ministry past the moment of entry into force of the decision of the Constitutional Court (in particular, since February 9, 2017), as processing of data without the legal basis envisaged by the Law of Georgia on "Personal Data Protection" and contrary to the principles envisaged by the said Law. Therefore, the Ministry was instructed to erase the data about imposing administrative liability on the data subject from the unified database or to store it in a form that excludes the identification of the person.

DATA PROCESSING WITHIN THE FRAMEWORK OF PREVENTIVE MEASURES

In order to protect public security and order the Law of Georgia on Police envisages the possibility to use certain police measures, including preventive ones. According to the law, such measures are: interviewing a person; identification of a person; external checkup and examination; use of automated photo device (a radar) and video device, etc.

Within the reporting period, as well as the previous year, the Inspector's Office examined numerous cases of processing data subjects' personal data in various forms within the framework of police preventive measures, including the facts of video recording via a mobile phone, identification of persons by a photo and verification of their identities in databases. Provided that the absence of the rules and detailed instructions on carrying out the said measures raises the risk of processing the data of the

person subject to preventive measures without a legitimate purpose and contrary to the statutory requirements, the Ministry of Internal Affairs of Georgia was recommended to determine the rule of identifying a person via a photo/verification of identity in the database within the framework of preventive measures and to assess the feasibility of using for preventive measures of mobile phones and data transmission devices owned by the employees.

According to the information submitted by the Ministry, it is working on introducing an application, that will ensure provision of police or other emergency assistance as fast and effectively as possible, contribute to uncovering the fact of traffic rule violations, to establishment of an effective mechanism of submitting the evidence of misconduct to the law-enforcement units. One of the purposes of the application is to carry out the identification of persons via photograph in consideration of organizational and technical measures and in observation of data security rules.

The steps taken by the Ministry in order to comply with the Inspector's recommendations are undoubtedly positive. However, it is additionally important to lay down specific and detailed rules on identification of a person via a photo/verification of a person's identity in a database, that will contribute to establishing a unified standard in this regard and will minimize the risk of processing citizens' personal data within the framework of preventive measures contrary to the statutory requirements.

In the reporting period an outstanding issue was a proper informing of data subjects within the framework of preventive measures. In the scope of a preventive measure (personal interview) envisaged by Article 19 of the Law of Georgia on Police, a policeman is authorized to collect data directly from a data subject. At the same time, according to the Law, provision of data by a data subject is voluntary. To ensure the accomplishment of the purposes of the preventive measure and the lawfulness of data processing in this process it is important that the citizen be informed about the purpose of data collecting, whether it is mandatory to submit the data and the legal consequences of a refusal to submit data. Being informed enables the citizens to protect their rights and not develop a feeling that their data are processed unlawfully. In the framework of handling a certain citizen's complaint a problem of proof of properly informing a data subject was identified. The Ministry was provided with recommendations, on the one hand to ensure the existence of proof of properly informing an interviewee by a po¬liceperson and on the other hand, to exercise the citizens' rights enshrined in law.

MAKING DATA PUBLIC AND THEIR DISCLOSURE

According to the Law of Georgia on „Personal Data Protection", one of the types of data processing is disclosure of data/making data public. Since this type of processing carries a higher risk of causing an irreversible damage to a citizen's interest, it is essential that it takes place only on a statutory basis and in observation of data processing principles.

In the reporting period the Inspector's Office examined the facts of disclosure of data by the Ministry of Internal Affairs, Prosecutor's Office of Georgia, Investigation Service of the Ministry of Finance of Georgia and by Special Penitential Service, sub agency under the system of

the Ministry of Justice of Georgia. Among these were the facts of publishing video recordings and special categories of data on the web-pages of the law-enforcement authorities and disclosure to media outlets.

In one of the cases examined at the Inspector's initiative, the form of depersonalization used for the information related to a deceased person's health that was published on a web-page was found insufficient since the data published earlier by media outlets enabled indirect identification of the person without particular efforts. Upon the Inspector's decision, the information containing special category data was erased from the web-page.

One of the complaints examined in the reporting period concerned the disclosure of a son's physical address by means of serving the parents with a restraining order and providing them with a copy of the order. According to the Ministry, as the data subject repeatedly stated in numerous statements submitted to the Ministry that he did not want to disclose a factual resident address to his parents, an officer introduced him to possible measures to be taken and provided an oral explanation that if the restraining order was issued, the parents would become aware of his factual residence address. The complainant was also advised that as soon as the violators attempted to reach his house the patrol police would intrude and prevent the threat. The Ministry claimed that the data subject signed the restraining order only after receiving the aforesaid information.

The complainant on his part stated that the Ministry's employees failed to explain to him the contents of the restraining order and although he signed the order he did not notice that his physical address was reflected in the document. The complainant also claimed that because of the harassment on the part of his parents he was in a state of anxiety and was not able to fully process every procedural detail that was carried out by the police officers.

Provided that in similar situations a victim may be in a state of anxiety and may not be able to properly acknowledge the purposes and possible consequences of data processing, it is important to establish a mechanism that will ensure to the fullest extent the clarity of information submitted to a victim, free expression of a person's will and creation of proof on properly informing a data subject. In consideration of the aforesaid, the Ministry was provided with a number of recommendations. In compliance with these recommendations the Ministry instructed relevant structural units to ensure the assessment of the extent of data to be disclosed to violators and to provide for properly informing victims/data subjects about the purposes and possible consequences of data disclosure within the framework of the measures determined by the law undertaken for the purpose of security of the victims.

INFORMING DATA SUBJECTS

According to Article 18 of the Constitution of Georgia and Article 21 of the Law of Georgian on Personal Data Protection, data subject's right to request information implies an obligation of public authorities,

including law-enforcement bodies, to provide a data subject on request with information about the processing of data related to him/her. Data subject also enjoys the right to request the copies of documents containing his/her personal data. Effective fulfillment of an obligation to inform data subjects is essential since exercising this right enables a data subject to know, what types of data related to him/her are being processed and whether processing is lawful. Notably, due to a specific nature of the activities of the law-enforcements, there might be a precondition to restrict a data subject's right to information in accordance with Article 24 of the Law of Georgian on Personal Data Protection, which adds to significance of maintaining a fair balance between a data subject's right to receive information related to him/her and on the other hand – legitimate interests of law-enforcement agency to ensure confidentiality of information.

In the reporting period, on the basis of citizens' complaint the Inspector examined the lawfulness of informing data subjects by the Prosecutor General of Georgia, Ministry of Internal Affairs of Georgia, Ministry of Defense of Georgia and by the Special Penitential Service. It should be noted that a positive tendency is observed in the fulfillment by the law-enforcement agencies of their obligation to inform data subjects. In 2018 only a few cases of violation of the statutory time-limits and incomprehensive provision of requested information/documentation were revealed. It should also be highlighted that requests submitted by data subjects often did not objectively provide an opportunity to identify and search for the information/documents requested.

To facilitate to exercising the right to information enshrined in the Law, it is advisable for the agencies to provide the citizens in due time with the part of the information/documents that are easy to identify and simultaneously to inform them about the circumstances impeding provision of the rest of the documents. If an agency does not process the data related to a data subject or does not store a particular document, data subject should be clearly and unambiguously informed of it. As per the issue of requesting the copies of documents containing a data subject's personal data, notwithstanding that the legislation does not lay down a specific time-limit for the provision of such documents, it is important to provide them in reasonable time.

In the course of handling a complaint filed in the reporting period by a minor it was established that the minor and his representative requested the Prosecutor's Office of Georgia the report of the minor's psychological-psychiatric examination conducted within the framework of a criminal case. However, due to the fact the data subject in accordance with the Criminal Procedure Code of Georgia was not a party to the criminal proceedings and therefore had no right to access criminal case files, the Prosecutor's Office found the provision to the minor of the report on psychological-psychiatric examination containing his personal data unadvisable. Notwithstanding that in the case at issue there were preconditions to restrict the data subject's right to be informed, the Inspector found it necessary to assess the proportionality of the measure of restriction and the Prosecutor's Office of Georgia was recommended to assess the possibility of the partial provision of the report on psychological-psychiatric examination to the minor or other means of informing the complainant.

OVERSIGHT OF COVERT INVESTIGATIVE ACTIVITIES

Pursuant to the Georgian legislation, one of the key functions vested on the Inspector is oversight of covert investigative activities and control of the activities carried out in the central database of identification data of electronic communication.

Throughout 2018 the Inspector's Office continuously observed the process of covert investigative activities. Analysis of the process provides that within the reporting period the number of covert investigative activities in terms of statistics has significantly increased in comparison to the previous years. However, it should be noted that covert investigative activities are mostly carried out on the basis of a court ruling and the number of such covert investigative activities carried out in the absence of a court ruling or on the basis of a prosecutor's resolution has fairly decreased.

Similarly, to the previous years, within the reporting period the largest number of granted motions were related to requesting computer data envisaged under Article 136 of the Criminal Procedure Code of Georgia, while the least carried out investigative activity was real-time collection of internet traffic data. Investigative activity known as monitoring of a postal and telegraphic transfer was not carried out in the reporting period.

IN 2018 THE INSPECTOR'S OFFICE RECEIVED 1397 COURT RULINGS ON COMMENCEMENT, CONTINUATION, APPROVAL, PARTIAL GRANTING AND REJECTION OF INTERCEPTION OF TELEPHONE COMMUNICATIONS.

Suspension mechanism was used in case of 96 rulings/resolutions. After elimination of the grounds of suspension the covert investigative activities continued.

Competent authorities were informed through electronic control system about ambiguities/inaccuracies revealed in 9 court rulings, after which the shortcomings were eliminated.

One case related to an interception of telephone communication was transferred to the Prosecutor's Office of Georgia due to the components of a criminal conduct.

Within the reporting period the Inspector's Office received 1397 court rulings on commencement, continuation, approval, partial granting and rejection of interception of telephone communications. Along with the increase of authorizations on the interception of telephone communications, the number of court rulings rejecting authorization and rejecting motions on continuation of a covert investigative activity or delaying notification about the conduction of a covert investigative activity to a person concerned has also increased.

Following the legislative amendment of 2017 the Inspector was granted an authority to suspend the interception of a telephone communication if the Office was not provided with a court ruling or a prosecutor's resolution whether in an electronic or original form, or the data in a prosecutor's electronic and original resolutions are inconsistent, or they contain an ambiguity/inaccuracy. In 2018 the suspension mechanism was used in case of 96 rulings/resolutions. The covert investigative activities continued after elimination of the grounds of suspension. In addition to this, competent authorities were informed through electronic control system about ambiguities/inaccuracies revealed in 9 court rulings, after which the shortcomings were addressed and eliminated. One case related to an interception of telephone communication was transferred to the General Prosecutor's Office of Georgia due to the components of a criminal conduct.

In 2018 the Inspector's Office examined the issue of compliance with an obligation laid down in paragraph 14 of an Article 143[6] of the Criminal Procedure Code of Georgia – on the submission of a protocol of completion of a secret investigative activity to the Inspector's Office due to the fact that in certain cases the State Security service of Georgia, the Prosecutor's Office of Georgia and the Investigation Service of the Ministry of Finance of Georgia have failed to provide the relevant protocol to the Inspector's Office. On certain occasions the failure to provide a protocol was caused by the fact that the covert investigative activity had not been at all conducted. On other occasions the agencies provided for the submission of the protocol to the Inspector's Office.

As regards the inspections carried out pursuant to Article 35[1] of the Law of Georgia on „Personal Data Protection", it should be noted that in 2018 two inspections were conducted in LEPL Operative-Technical Agency and two inspections launched in 2017 have been completed.

The Office examined the lawfulness of a covert investigative activity – interception of telephone communications carried out by means of stationary technical capabilities of real-time collection of communication, as well as examined the lawfulness of data processing during recording the communication and the lawfulness of processing the data in result of the activities carried out in the central databank of identification data of electronic communications. In the reporting period the Ministry of Internal Affairs and State Security Service of Georgia were also inspected in relation to the covert investigative activities.

It should be noted that Article 143[9] of the Criminal Procedure Code of Georgia lays down an obligation of the prosecutor's office to inform the person subject to covert investigative activities about the conduction of these activities, the content of the materials obtained in this process and destruction of the materials. In 2018 at the Inspector's initiative the Prosecution's Office of Georgia was inspected in order to examine compliance with the mentioned obligation. On the basis of a random selection the Office examined covert investigative activities envisaged under Article 143[1] of the Criminal Procedure Code of Georgia in relation to which the data subjects should have been informed since January 1, 2018. In result of the inspection several facts of violation of the principles envisaged by the Law of Georgia on "Personal Data Protection" and breaching data security rules were identified. The Prosecutor's Office was served mandatory instructions to ensure properly informing data subjects pursuant to Article 143[9] of the Criminal Procedure Code of Georgia.

PROCESSING OF ELECTRONIC COMMUNICATIONS IDENTIFICATION DATA

In the reporting period the Inspector's Office examined 6 facts of unlawful transfer by electronic communication companies of identification data of electronic communication to law enforcement agencies and improper fulfillment of the obligation to notify the Personal Data Protection Inspector. On one occasion, notwithstanding that the law-enforcement authority did not provide a relevant court ruling on the authorization of requesting information from the electronic communication company, the company still transferred the requested information/documents. The Office identified one fact of providing a law-enforcement agency with identification data of electronic communications simply on the basis of a reference, in the absence of a court ruling and a prosecutor's resolution.

DATA PROCESSING IN PRIVATE SECTOR

6

DATA PROCESSING IN PRIVATE SECTOR

In the reporting period, within the framework of handling citizens' complaints and conducting inspections the Inspector's Office examined 355 data processing operations in private sector, including: 60 cases in trade and service provider companies, 40 – in marketing companies, 35 – in the so-called debt collecting companies, 21 – in electronic communication companies and 21 – in medical, insurance and pharmaceutical companies. 30 cases were related to the banks, 19 cases – to microfinance organizations, 15 cases – to internet service providers and 12 cases to – JSC Creditinfo Georgia. The Inspector's Office also examined the lawfulness of data processing by 10 hotels, 8 gambling businesses, 8 private universities and educational institutions.

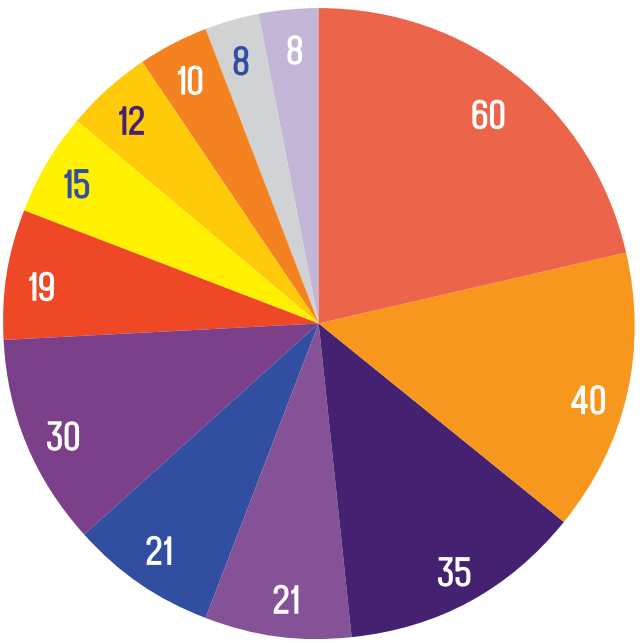
Throughout this year 196 administrative offences were revealed in private sector. A fine as a form of administrative sanction was imposed on 61 data controllers, while 54 data controllers were warned. Number of consultations provided to private organizations increased to 2135. Many organizations put an effort to acquire Inspector's consultation prior to planning the processing operations, which in turn contributes to risk minimization, prevention of violations and indicates to the increasing interest of private sector in the issue of protecting personal data. By the second half of the year an outstanding issue for large organizations was the new EU Data Protection Regulation, that was translated and became available through the Inspector's web-page.

In order to raise awareness on data protection issues tens of working meetings and trainings were organized with participation of over 500 representatives of private sector, including healthcare professionals and representatives of small and medium sized enterprises and educational institutions. Two sectoral recommendations were drafted on data protection issues in healthcare sector and on European Data Protection Regulation.

Lawfulness of accessibility of databases and time-limits for the storage of data remained outstanding issues in 2018. Notwithstanding that at the Inspector's instruction a few so-called debt collecting companies determined internal procedures of data processing, citizens kept reporting the facts of disclosure of their data to unauthorized persons. Within the reporting period, compared to the previous years, the number of complaints regarding video surveillance by individuals has increased.

The present chapter contains revealed violations in the form of examples, consequences of responding to these violations and recommendations which if complied with will significantly decrease the possibility of committing a violation in the future and will contribute to improving data protection standards in the private sector.

IN 2018 THE INSPECTOR EXAMINED 355 DATA PROCESSING OPERATIONS IN PRIVATE SECTOR



- Trading and Service Provider Companies
- Marketing Companies
- So called Debt collecting companies
- Electronic Communication Companies
- Healthcare, Insurance, Pharmaceutical companies
- Banks
- Microfinance Organisations
- Online Service Provider Companies
- JSC Creditinfo Georgia
- Hotels
- Gambling Companies
- Private Educational Institutions

DATABASES

Similar to the public institutions, processing high volume of data is a challenge for a private sector too. At the same time, doing contemporary business can hardly be imagined without using databases. This is especially true for the sector of banks and finances, that processes hundreds and thousands of data about a person's financial state and transactions. In 2018 the Inspector examined 96 data processing operations in the financial sector, including 30 cases in banks, 35 cases in the so-called debt collecting companies, 19 in microfinance companies and 12 in JSC Creditinfo Georgia.

One of the largest data controllers of the citizens' financial data is JSC Creditinfo Georgia, since it is the company's database that contains information about credit history. During previous years, as well as in the reporting period, activities of a credit bureau were not regulated by law and the data were processed on the basis of a contract concluded with private individuals (JSC Creditinfo Georgia and its customers).

It should be noted that as a result of the legislative amendments the National Bank of Georgia was granted an authority to oversee the activities of credit bureaus. Additionally, following the Inspector's recommendations, the rules of submitting information to credit bureaus in Georgia, recording information in their databases and accessibility to that information were laid down in a normative act - in the Order of the President of the National Bank of Georgia – which came into force on January 1, 2019.

The aforementioned Order established the rule of accessibility of organizations to the databases of credit bureaus and the latter's obligation to provide access to those employees only who are officially authorized to process credit information. The purpose of accessing the data was limited to assessing a person's creditworthiness. According to the adopted regulation, access to the credit information is admissible only on the basis of a data subject's consent. At the same time, the conditions and time-limits for checking information on the basis of a data subject's consent were established. Credit information bureaus, as well as the organizations using their databases were instructed to introduce the policies and procedures that ensure proper processing of an individual's credit information. It should be highlighted that the Order established an obligation of a credit information bureau to check by random selection and on a regular basis the legal grounds of processing a person's credit information, which is an important mechanism for preventing unlawful processing of data. Apart from this, the Order established an obligation of credit information bureaus and the organizations with access to their databases to process accurate and updated data, which was one of the outstanding issues revealed in the reporting period.

As a rule, databases of banks and financial institutions are accessed by thousands of employees on a daily basis, that increases the risk of unauthorized access to personal data.

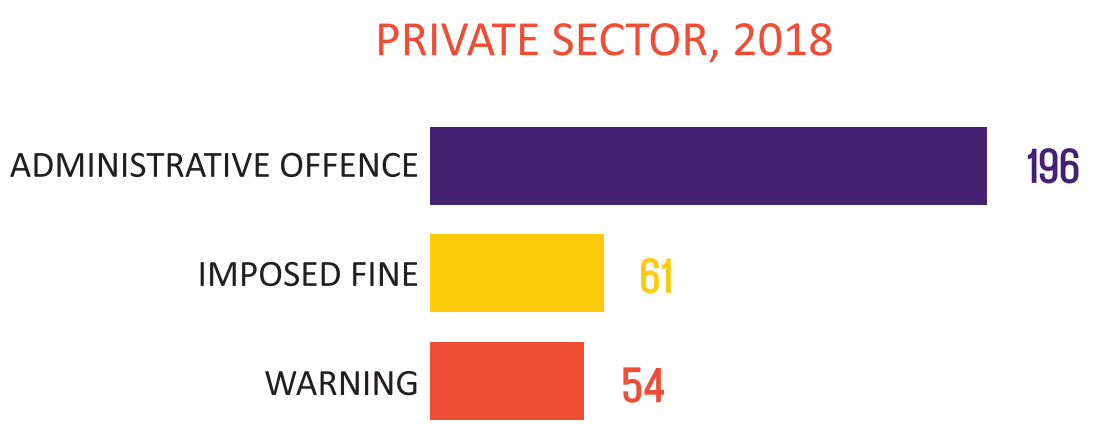
In the reporting period the Inspector's Office was approached by a person who indicated that within the framework of a legal dispute heard by Tbilisi City Court between him and a family member of person employed at one of the banks, the opponent disclosed a detailed information about the transactions carried out on the complainant's bank account and submitted a petition to request a bank statement from the bank. The complainant assumed that the opponent had become aware of the transactions through the person employed at the bank.

In result of the case examination it was revealed that the bank's employee checked the information about the complainant hold by the bank multiple times notwithstanding that by the time the information was accessed the complainant had closed all of the accounts at the bank. Notwithstanding the revealed circumstances, the bank did not confirm the fact of unauthorized access, failed to take additional measures

to reveal the possible violation and claimed that an agreement concluded with the complainant was still in force and it served as basis for access to the complainant's closed accounts. The bank also claimed that the purpose of access was to check the complainant's creditworthiness and offer him a credit product. The bank failed to provide any proof that would indicate to the necessity of accessing the closed account with the view to check creditworthiness and the fact of offering a credit product to the client. On the basis of the Inspector's decision it was established that the bank checked the complainant's closed accounts in violation of Articles 43-44 of the Law of Georgia on "Personal Data Protection". However, the sanction was not imposed due to the expiry of the statute of limitations. To ensure the lawfulness of data processing the bank was instructed to establish the procedure of processing personal data for the purpose of determining creditworthiness.

It is important for data controller organizations:

- to implement instructions/policy documents that establish the rule and conditions for processing personal data;
- to introduce their employees to the rules of accessing databases, consequences of unauthorized access and conduct a regular monitoring of data processing operations;
- In case of identifying a violation of data processing rules, to take relevant disciplinary measures with regards to the perpetrators.



TIME-LIMITS FOR THE STORAGE OF DATA

Simultaneously to collecting and using extensive data in databases data controllers pay less attention to the time-limits for the storage of data and continue to store them even after the purpose of data processing has been served or it does no longer exist.

In the reporting period the Inspector's Office conducted inspections of 10 hotels. In result of the inspections it was revealed that at the customers' request and/or for statutory purposes hotels collect and store quite extensive numbers of data about their customers. However, they have no time-limits for their storage. Aside from this, data security issues were revealed in the part of the inspected hotels. Some of the hotels had no established rules of access to customer data and the software was not recording the identity of a person who accessed the data and the date of access. In light of this, the hotels were instructed to take organizational and technical measures to protect the security of data held in their databases and to establish reasonable time-limits for the storage of data.

DATA PROCESSING IN THE EMPLOYMENT RELATIONSHIPS

A person's privacy is protected from unlawful intrusion, including from an employer. As interpreted by a European Court of Human Rights in one of the cases, an employer can not diminish a private social life at a workplace. A right to privacy continues to exist, whether an employer has prohibited a certain action or not.

As a rule, employers use various organizational and technical mechanisms to control the behavior of employees. Indeed, to achieve an effective performance, to prevent or detect disciplinary misconducts, employers have a legitimate interest of monitoring their employees. However, this opportunity is restricted by law and is admissible only for a specific purpose and to an adequate extent. Accordingly, a fair balance should be struck between the right to inviolability of an employee's privacy and the legitimate interests of an employer. It is important that employers take into account that employees maintain their right to privacy during business hours and it requires a prior notification of employees about the forms and extent of the possible monitoring.

In the reporting period the Inspector detected several facts of violation of an employee's right to personal data protection on the part of employers.

The Inspector's office examined the fact of monitoring by a bank of its employee's bank transactions. It was established that the bank had been using an automated data processing software that detected the transactions carried out by the bank's employees on the accounts of gambling institutions (casinos, bookmakers, etc.) during business as well as non-business hours. After a detailed analysis of data, the bank decided on the issue to dismiss employees from their positions. The bank explained the necessity of monitoring with the fact that gambling causes addiction.

By means of the employment contract and internal regulations of the bank, the employee was provided with a general information about the monitoring. However, he was not aware of the specific forms (through an automated software) and extent (period of data processing and volume of data) of monitoring. Herewith, the bank checked the information related to the transactions carried out during non-business hours when the person, as a bank's client enjoyed the bank's services for unofficial purposes and through unofficial means and just like other clients had a legitimate expectation of confidentiality of personal data. The bank failed to take into account that the person in question might have been somehow related to the person in a gambling business and not have been addicted to the gambling itself or that the transaction might have served the purpose of covering not the employee's but another person's financial obligations.

In the case described processing of personal data in such a form to serve the purposes indicated by the bank was found unreasonable and inadequate means of data processing. The bank was found to be re-

sponsible for administrative offence in accordance with Article 43 of the Law of Georgia on „Personal Data Protection".

The Inspector's Office was addressed by a citizen who claimed that the employer had placed an order about the imposition of disciplinary sanction on him in the administrative building, on a publicly accessible stand. In result of handling the complaint it was revealed that the organization systematically placed on the stand its decisions on the imposition of disciplinary sanctions, incentives (including bonuses), appointments/dismissals without a specific requirement to do so.

The employer was found to be responsible for the administrative offence in accordance with Article 43 of the Law of Georgia in Personal Data Protection and was instructed to take into account the requirements of the law in order to change the wrongful practices.

When processing employees' data within the framework of employment relationship, an employer should:

- In the existence of a legitimate interest of monitoring the behavior of an employee to consider and observe employee's privacy and notify him/her in advance of the form and extent of monitoring;
- Restrict the accessibility of any concerned parties to the information about employees' official activities, including their career promotions and misconducts without a specific requirement.

PROTECTION OF PERSONAL DATA IN HEALTHCARE SECTOR

According to applicable legislation, information about a person's health is a special category data that contains sensitive details about one's privacy, psychological and physical health. Therefore, unlawful or accidental disclosure of a special category data might cause a person's humiliation, stigmatization or discrimination. It is important that when a person applies to a medical institution, he/she has a feeling and legitimate expectation that confidentiality of his/her data will be protected, because in the absence of trust, a person might abstain from providing important information or receiving necessary medical care.

The Inspector's Office actively cooperates with clinics, as well as with Ministry of Internally Displaced Persons from the Occupied Territories, Labor, Health and Social Affairs of Georgia. Simultaneously to consultations provided individually, specific recommendations tailored for this sector have been prepared. Nonetheless, the violations and shortcomings identified in the reporting period reflect the challenges in processing the data related to health. For instance, the facts of disclosure of health data to third parties without a patient's written consent and in the absence of statutory derogations were revealed.

The Personal Data Protection Inspector was addressed by a citizen who became aware that her daughter obtained a document about her health (so called form #100) and used it as evidence against her in a court dispute. In the course of examination, it was revealed that the medical institution had provided the complainant's daughter with the document without the patient's consent, only on the basis of a verbal reference and had not asked for a document certifying representative powers.

In the course of handling the complaint it was also revealed that the medical institution did not record activities related to disclosure of patients' personal data.

Following the identified violations, in order to safeguard the lawfulness and security of data processing, the medcial institution in accordance with the Inspector's instructions implemented the rules of managing medical documentation in the institution that solved the issues of disclosure of patients' documents and recording related activities.

Within the framework of handling a certain citizen's complaint it was revealed that information published on social media by one of the medical institutions contained data about the specific medical procedures applied to the complainant and health status of the complainant, also the person's name and surname indicated in the documents and used by the said person in everyday life, which in turn revealed the complainant's gender identity. The medical institution insisted that the information was disclosed to protect the organization's business reputation, in response to the information published by the complainant in a media outlet, where the complainant asserted that the institution had failed to provide him with relevant medical help.

The Inspector did not share the position of the medical institution and pointed out that the indicated purpose could have been met by the institution without making the special category data available to third parties. Accordingly, the medical establishment was found to be responsible for disclosure of special category data in absence of legal grounds envisaged by Article 6 of the Law of Georgia on „Personal Data Protection". The medical establishment was instructed to erase the information containing the complainant's special category data.

To avoid unlawful or accidental disclosure of patients' information, organizations should fully acknowledge and asses the risk related to the processing of special category data and implement adequate and effective measures. Consideration should also be given to arrangement of waiting and examination spaces for patients. Although a large number of medical institutions use technological means, such as queue number system for signing patients up for a doctor's visit and medical services, citizens still report instances of publishing the names and surnames of patients signed up for a doctor's visit. It is equally important that institutions solve the issues of storage and accessibility of documents on an internal basis so that the document containing patients' data is not easily available to unauthorized persons.

The Inspector was addressed by a citizen who claimed to have visited a medical institution to receive the so-called drug test certificate. In the process of providing the medical service other patients were also present in the room and were simultaneously answering the questions of practitioner of narcology. According to the complainant, other patient's answers to a doctor's questions were audible and his answers could have been easily audible to the other patient as well. In result of examining the circumstances of the case it was confirmed that a drug examination was being conducted in the same room on several patients simultaneously.

Although patients physically meet one another at medical institutions and they might guess that a certain person is undergoing a drug examination, by attending the drug examination itself they receive accurate and official information about the identity of a patient, his/her medications, illnesses and other medical details. The Inspector found that a simultaneous examination of several patients in the same room is contrary to the standard of security of data processing and constantly creates a risk of accidental disclosure of data. At the Inspector's instructions the institution implemented procedures safeguarding patients' personal data from unlawful/accidental disclosure in the course of drug examination.

In one of the cases it was determined that a certain citizen got access to a prescription issued to an unknown person. In particular, the citizen in question bought a bread at a bakery and the loaf was handed over to him wrapped in a prescription issued by a medical institution. In result of the examination of the case it was revealed that the mentioned prescription had been presented to a pharmacy, that sent the documentation, including prescriptions to the warehouse of the pharmaceutical network. From the warehouse the documents were later sent to a partner organization for utilization. The wastepaper had been transferred by weight and the organization had failed to record the requisites of the documentation and the date of transfer. In the course of the inspection it was additionally established that the agreement concluded between the owner of the pharmaceutical network and the partner organization managing utilization process did not contain clear instruction as to the specific rules of data processing and restrictions.

Based on the circumstances and shortcomings identified in the course of the inspection the organization was instructed to record with relevant requisites the facts of transferring waste paper containing personal data for utilization. It was also instructed to reflect in the agreement concluded with the partner organization the obligations related to data processing and monitoring mechanisms.

To provide for the lawfulness of processing of the data related to citizens' health in medical institutions and to ensure security of data it is important that these institutions:

- Implement standard rules and take effective measures to ensure recording of any activity related to storage, transfer to third parties and disclosure (to whom, what data, when and on what legal basis) of the patients' health data;
- Introduce mechanisms of control that ensure compliance by the institution's employees to the stablished rules of data processing;
- Take necessary organizational and technical measures to protect the patients' data from accidental or unlawful disclosure.

MAKING DATA PUBLIC

When data are made public, they become available for an indefinite time to large number of persons and further control on their dissemination is practically impossible. In some cases, making data public might be a necessary and legitimate mean, however considering the accompanying risk it is important that data controller assessed on a case-by case basis whether there is a legal ground to make data public and whether accessibility of data is necessary for legitimate purposes.

In the reporting period the Inspector's Office examined a number of cases when data were made public. On certain occasions administrative offences were identified.

In the course of inspecting two universities it was revealed that the universities had published information about students' financial indebtedness and suspension of their status on an information board (the list contained students' names, surnames, personal identification numbers, group numbers) without legal grounds established by the Law of Georgia on „Personal Data Protection"

The universities claimed that the purpose of making data public was to inform the students. Within the framework of the inspection it was determined that the students could have been provided with information through alternative means – individually, via electronic database and e-mail. However, the universities made the students' data publicly available.

The Inspector found both universities to be liable for an administrative offence envisaged by Article 43 of the Law of Georgia on „Personal Data Protection". They were instructed to implement standard procedures of informing the students about their financial indebtedness and change of status. To comply with the said instruction, the universities actively cooperated with the Inspector's Office in the form of consultations.

Making data public on a disproportionately large scale became the subject of another citizen's complaint. The complainant had a court dispute with a certain organization. The organization made the complainant's surname, sums transferred to his account and information about his family relations public through a television. The financial organization claimed that the information was made public to defend its own interests and in a form that excluded the person's identification.

In order to consider information to be personal data it is not necessary for it to enable a person's direct and full identification. In certain cases, combining various circumstances makes it possible to identify the subject of the information without a person's identity (name and surname). At the same time the data controller failed to demonstrate the necessity of making the information about the complainant public in such a form and to such extent.

Another case is also noteworthy in this regard. A microfinance organization published notifications for the complainant and his guarantor in a newspaper. The notifications contained a detailed information about the complainant's indebtedness, sum of the realization of the subject of mortgage and the name of the buyer. According to the company, complainant's prior consent expressed in the contract concluded between the parties served as a legal basis for publishing the notifications in the newspaper.

According to the contract, if the creditor failed to otherwise serve a notification on the debtor, the organization was authorized to publicly disseminate the notification. The company stated that the purpose of making the notifications public was to submit a legal suit to the court and establish a legal claim through a court.

The Inspector did not share these reasoning as prior to publishing the information the company had failed to use all available means of informing the complainant and his guarantor. The necessity of publishing the information in a newspaper was also unsubstantiated.

When data are made public it is important to establish the time-limits of their accessibility.

In the course of inspecting a court of arbitration it was revealed that the court published announcements containing information about the parties to arbitration (names, personal numbers, information about the subject of dispute, etc.) on its web-page in a publicly available form. Resolutions were published on the web-page only with regards to the cases where correspondence could not be delivered on the addressees. Although arbitration parties personally consented to making the information public, the legitimate purpose of the processing did not require accessibility of information for an indefinite time. According to the Statute of the court of arbitration, if summons/lawsuit could not be delivered to a party otherwise,

the court is authorized to render a resolution about publicly disseminating the notification. In such cases the notification is considered to be delivered to the party on the 7th day of its publication on the web-page.

As already stated above, making data public in certain cases might be a necessary and a legitimate mean to accomplish the purpose. Public interest of receiving information may differ in accordance with the public status of the data subject.

In one of the cases the complainant claimed that the Charter of Journalistic Ethics published a decision containing complainant's personal data (name, surname, place of employment) and deliberation on the issue whether the complainant breached the principles of the Charter.

In the course of handling the complaint it was also revealed that the personal data indicated by the Charter in its decision had been made available by the complainant himself, which became the legal basis for processing his data. As for publishing the information about the hearing by the Charter's Council of the complainant's case and the decision of the Charter, the Inspector found that the Charter's decision reflected an opinion of the Charter's Council in the capacity of an authority established for the purpose of journalists' ethical self-regulation, regarding the issue of violating by a journalist of the Charter's principles. Journalistic activities are public and they have a great influence on public opinion. Journalists are public persons and due to their social status they have a higher obligation of tolerance. Therefore, within the framework of handling the complaint in question, the Inspector found no violation on the part of the Charter.

Prior to making data public data, controllers should ensure that:

- There is a statutory legal ground for data processing;
- Making data public is necessary to achieve a legitimate purpose;
- The volume of data is adequate to the purpose;
- The data will be available for the time-limit that is adequate to the purpose.

DATA PROCESSING IN THE CONTEXT OF LOAN MANAGEMENT

The Inspector's reports from the previous years reflected numerous issues related to data processing in the context of loan management. In 2018 the Inspector's Office examined 35 cases of data processing by debt collecting organizations. In the course of examining the cases the Office yet again identified the facts of unlawful processing of data.

Most of the complaints filed by the citizens were against the organizations contacting third parties (debtor's family members, neighbors, friends in social networks, co-workers) in order to ensure the payment of loans. In the course of this communication the organizations disclosed information about the existence of the debt and in some cases detailed information about the debt (amount of debt, payment and interest).

During handling the complaints, the data controllers and data processors state that communication with a debtor though third parties is a necessary measure in debt collecting process since a direct communication with a debtor is complicated in such cases. It should be noted that negotiating with a debtor in order to ensure payment and communicating with third parties to this end might on certain occasions actually be a legitimate interest of a creditor. However, it is necessary to observe in this process the data processing principles laid down in the law. Organizations should resort to all possible measures to the widest extent to prevent in the process of defending their interests the abuse of a citizen's dignity and the right to personal data protection.

In the cases examined in the reporting period the Office revealed several instances where creditors contacted third parties even when direct communication with a debtor was not problematic. Moreover, organizations contacted with a debtor and third party simultaneously, with a several-minutes interval. In some cases, it was revealed that the organizations failed to use all contact details at their disposal (e-mail, residence address, etc.) and communicated with third parties after a few failed phone calls, without using other means of communicating with the debtor. On several occasions the information about the debt has been disclosed to third parties.

The issue of lawfulness of the means used to collect the contact details of third parties is also questionable. The creditors claim that the sources of information are open databases, social networks and debtor's neighbors –when the creditor visits their places of residence. However, they fail to record specific sources of collecting information. In 2018 numerous creditors and loan management companies were instructed to implement the standard written rules/procedures on recording the information obtained for the purpose of locating debtors and ensuring the payment of the loan, including the information about the third parties allegedly related to debtors.

Within the framework of handling a complaint its was established that a certain organization had been processing customers' IP addresses to locate the "problematic" debtors. Particularly, the organization stored the IP addresses by which the users registered on the web-site and filled out a loan application. The organization's software system established that the complainant and the debtor had used the same IP address at different times to fill out the loan application. On the basis of this information the organization linked the complainant to the debtor and contacted the former. According to the complainant, the debtor was not his family member and/or a relative. In the course of handling the complaint it was established that the organization was not providing data subjects with proper information: it had obtained from the complainant a consent to processing certain categories of data for a specific purpose, but it had not obtained a consent to processing IP addresses for the said purpose; additionally, the organization had not otherwise informed the complainant of processing the IP address for the said purpose. In the absence of a customer's consent and awareness, the organization failed to demonstrate the necessity of processing the complainant's IP address for the purpose of protecting the company's legitimate interests.

In the process of loan management certain shortcomings were identified in the context of data security. In particular, several facts were identified where correspondence addressed to debtors were delivered to the third parties. In one of the cases a creditor delivered a letter to the complainant's neighbor, in an open form, without an envelope. This neighbor in turn, with the help of another neighbor delivered the latter to the complainant's mother. In this manner information about the complainant's financial debts became available to the complainants' neighbors as well as to his mother.

In the process of managing the loans, data controllers and data processors should:

- Ensure that there is a relevant necessity to contact third parties in order to communicate with debtors, including that all other means of communication are exhausted and a reasonable time has elapsed after attempted communication;
- Provide that during communication with third parties information is disclosed to the extent which is strictly necessary to achieve the legitimate purpose;
- Record the sources of collecting information about debtors and third parties;
- Implement organizational and technical measures that ensure security of data related to debtor, including information about the debt, from accidental or unlawful disclosure.

DATA SUBJECT'S RIGHTS

For the purpose of protecting a person's privacy when processing data, Council Of Europe's Convention №108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as the Law of Georgia on „Personal Data Protection" envisages certain rights for a data subject, the exercising of which enables the citizens to make sure that data are processed lawfully and to take the relevant measures for the protection of their rights.

In the context of maintaining control over personal data one of the most important rights is the right to request rectification, update, completion, restriction of processing, erasure and destruction of data. Organizations have an obligation to take the relevant measures within the statutory time-limits in order to ensure compliance with the request or inform the data subject about the grounds for refusal.

In 2018 the Inspector's Office revealed a number of facts where organizations failed to comply with the citizens' legitimate requests.

A citizen claimed that he was regularly receiving e-mails about a financial indebtedness from a loan company that were addressed to another person. The complainant addressed the organization with a request to remove the e-mail address from the relevant database, to no avail.

Although the organization became aware that the e-mail address that was recorded in its database as the address of the debtor belonged to another person, the company failed to take the necessary measures to prevent the disclosure of the debtor's personal data and to protect the complainant's rights. The organization continued to use the complainant's e-mail address and it was consequently found to be liable for an administrative offence, fined and instructed to stop using the complainant's e-mail address.

The Inspector was addressed by a citizen who claimed that after purchasing a mobile phone he was constantly contacted by a debt collecting company regarding an unknown person's overdue loan. According to the citizen, he requested the organization to erase his phone number on multiple occasions. As an evidence the complainant submitted a contract on the purchase of the phone number concluded with a mobile network operator that proved his ownership of the number. In the course of examining the case it was revealed that the organization had failed to duly review the complaint and continued to use the number owned by the complainant in the absence of a legal ground. The organization was fined for the administrative offence and was instructed to stop the processing of the phone number and to inform the organizations at whose instructions the data were processed about the erasure/update of the information.

Among data subject's other rights, no less significant is a citizen's right to withdraw a consent at any time and without explanations and to request the restriction of processing and/or erasure/destruction of data. Organizations should take the relevant measures to comply with such request, unless there is another legal ground to continue processing of the data.

The Inspector was addressed by a citizen who claimed that during a visit at a beauty parlor prior to a procedure she was offered to record the provision of the service in real time and publication on the social media (the so-called Facebook live). She consented to the offer. The video recording was published on the social media page of the beauty parlor. After a certain period of time the citizen requested the administration to erase the video recording, however the beauty parlor failed to comply with the request within the statutory time-limits. After the imposition of an administrative penalty in the form of a fine the beauty parlor erased the video recording.

Data subject's rights are not absolute and the applicable legislation establishes occasions when the restriction of a data subject's rights is permitted. For instance, data subject enjoys the right to receive easily, in a reasonable time and free of charge information on the processing by a certain organization of his/her personal data (which data are processed, for what purpose, on what legal basis, by which means were the data collected, who were they disclosed to and for what purpose). However, in certain cases when exercising data subject's right might cause a risk to the rights and freedoms of other persons, restriction of this right might be considered permissible.

The Inspector was addressed by a citizen who claimed that he had requested information about processing of his personal data from his former employers in a written form. The citizen was requesting the identity of the persons who reported his undue behavior to the employer that resulted in the commencement of internal inquiry against the employee. The complainant was not informed about the identity of specific persons but was provided with a general information about the source. Protection of the legitimate interests of the sources was indicated as the reason for withholding the information as the employees should have had an expectation of anonymity when reporting such cases to the employer. The preliminary inquiry against the complainant did not result in disciplinary proceedings and therefore the issue of imposing a disciplinary sanction on the complainant was not raised.

The Inspector found that in the case in question the complainant's interests were not overriding and the organization had not consequently violated the law.

In order to properly exercise the rights of a data subject organizations should:

- Thoroughly examine citizens' requests on rectification/update/erasure of data and respond in a timely manner within the statutory time-limits;
- As soon as inaccurate data are identified, take appropriate measures to prevent the accidental or unlawful disclosure of a confidential information to a person not authorize to consult the data;

TRANS BORDER FLOW OF DATA

Authorizations issued by the Inspector and the consultations provided by the Office in the reporting period indicate that transferring data to foreign countries is still an outstanding issue. Georgia-based companies often use the services offered by overseas enterprises and this process requires the transfer of certain types of data to compa-

nies operating in the foreign states. In 2018 the Inspector's Office received 8 applications on the authorization of data transfer to another country. In one case the Inspector issued a partial authorization, in two cases the companies were denied an authorization to transfer the data. In all remaining cases the companies were authorized to transfer the data.

REGISTRY OF THE CATALOGUE OF FILING SYSTEMS

For the purpose of overseeing data processing operations and ensuring the accountability of data controllers, the Personal Data Protection Inspector maintains an electronic registry of the catalogue of filing systems that is publicly available and interested persons enjoy the possibility to consult the information about the data processed by public and private organizations, legal grounds, purposes and volume of processing, measures implemented for data security.

In 2018 the Inspector's Office provided over 400 written and verbal consultations regarding the catalogues of the filing systems.

In the reporting period a total of 1282 catalogues of filing systems were submitted to the Inspector's Office. 1156 catalogues were submitted by data controllers in private sector, out of which 350 catalogues were submitted by financial service providers, 320 – by trade centers, 32 – by organization in the field of information technology, 29 – by medical service providers, etc.

VIDEO SURVEILLANCE

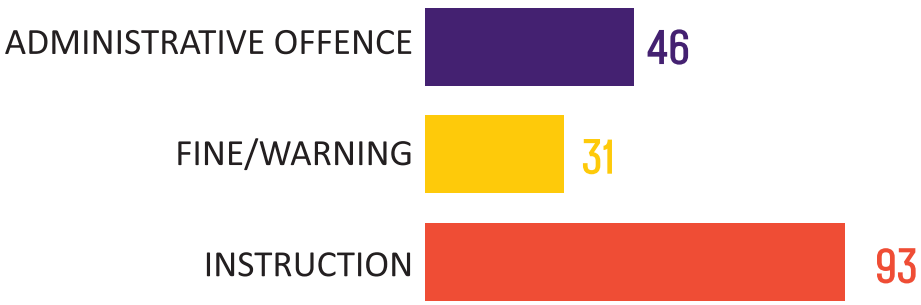
Technological development is followed by a yearly increase in the rate of using video surveillance systems not only by public institutions and private organizations but also by private individuals. Accessibility of technical means, including video surveillance devices for the purpose protecting security and property, made video surveillance integral part of day-to-day life. In light of the aforesaid, thorough compliance with the requirements set forth by the law gains a particular importance.

In 2018 the Inspector's Office examined 60 cases of lawfulness of data processing by means of video surveillance systems installed in trading centers, medical institutions, sports complexes, hotels, public organizations and residential buildings. 46 facts of violating the rules on video surveillance and data security were identified in result. Relevant sanctions in the form of fines and warnings were imposed on 31 data controllers for administrative offences. Additionally, 93 instructions were issued on the installation of warning signs, informing employees, time-limits for the storage of video recordings, organizational and technical means for data security and disclosure of recordings to third parties.

In result of the inspections carried out in the reporting period it was revealed that as a rule, data controllers used video surveillance in accordance with the statutory purposes. However, there were cases when organizations used audio surveillance to monitor persons' behavior and communication. A tendency of failure to properly inform the citizens about the ongoing video surveillance was also revealed. Namely, there were issues regarding the installation of a relevant warning sign in a visible place and informing employees in a written manner.

When data are processed by means of video surveillance systems, data security issues are of importance too. As a result of the inspections it was determined that organizations had failed to take appropriate organizational and technical means to protect the security of video recordings. Video monitoring in a changing room did also take place.

VIDEO SURVEILLANCE, 2018



VIDEO SURVEILLANCE IN CHANGING ROOMS

In accordance with the applicable legislation, video surveillance is inadmissible in changing rooms and places of hygiene, which on the one hand serves as a protection of inviolability of a person's privacy and on the other hand, citizens give a legitimate expectation that video monitoring will not be carried out in such places.

Last year the Inspector's Office was addressed by a citizen who claimed that a video surveillance system was installed in the men's' changing room on the territory of a sports complex. The Inspector's Office launched an inquiry immediately after receiving the report. In result of the inspection it was determined that the video surveillance cameras were actually installed in the changing room and their field of view covered an area for men, where lockers and closed changing cabins were situated at the territory through which the visitors entered showers, toilets and swimming pool. Although the inner space of changing cabins did not fell into the field of the cameras' vision, the onsite inspection revealed that in certain cases the visitors were unable to use the changing cabins due to lack of capacity and changed clothes directly near the cabins and benches, which made them fall into the field of view of the video surveillance cameras. The company claimed that the mentioned area was not a changing room, however in the company's internal documents and in the director's orders this area was referred to as "changing room".

As the Law of Georgia on „Personal Data Protection" imperatively bans video surveillance in changing rooms and places of hygiene, at the Inspector's decision the company was found to be liable for administrative offence, it was fined and instructed to change the field of view of the video surveillance cameras.

VIDEO SURVEILLANCE IN RESIDENTIAL BUILDINGS

The reporting period was marked with an increased number of citizens' complaints regarding video surveillance systems installed in residential buildings. In result of the inspections it was determined that in certain cases together with video surveillance, audio monitoring was carried out in residential buildings. Often the field of view of video surveillance cameras covered neighboring yards or houses, while people leaving in the neighborhood were not informed in advance about the video surveillance of their property and had not expressed their consent.

10 individuals were found liable for administrative offence. However, due to the fact that they had not been previously found liable for a violation and they took measures to eliminate the shortcomings in the process of the inspection, the Inspector's Office issued a warning as an administrative penalty.

Increasing number of family hotels and the so-called hostels in the recent years was followed by the practice of using video surveillance systems in multi-residential buildings. According to the Law of Georgia on „Personal Data Protection", more than half of the residents have to agree in writing to allow installation of a video surveillance system in the entrance and common area of the residential building. Video surveillance of the entrance of an apartment unambiguously requires a written consent of an owner.

In result of examining a case in 2018 it was determined that the field of view of video surveillance cameras installed outside of a family hotel covered the door of a neighboring apartment, common entrance hall and shared balcony. In addition to this, the cameras were carrying out audio monitoring contrary to the will of the residents and in the absence of a warning sign which constituted a disproportional intrusion into the residents' privacy.

It should be noted that audio-video surveillance system installed in residential buildings for property protection and security purposes might breach the inviolability of neighbors' or co-owners' right to privacy. Accordingly, it is necessary that citizens carry out audio-video monitoring in accordance with the law and to the extent that is adequate in relation to the specific purpose, in order to avoid violating the right to others' privacy when exercising their property rights.

STORAGE OF VIDEO RECORDINGS

In practice there are cases when organizations still don't appropriately asses the necessity and save the data, including video recordings for an indefinite time. Herewith, they fail to take into account, that big data processing/storage requires acquisition of various technical means and software, which in turn is related to certain costs. In addition, if no appropriate organization and technical means are in place, the risk of unlawful disclosure of personal data increases.

Inspection of a medical institution in the reporting period revealed that the documents limited the period for the storage of video recordings in the mentioned institution to 30 (thirty) calendar days. However, the software stored the data for over a year, without any necessity to do so.

ACCESS TO VIDEO SURVEILLANCE SYSTEM AND DATA SECURITY

According to the applicable legislation, installation of video surveillance system is mandatory for pharmacies, currency exchange objects, gas stations, gambling and organizers of other prize games. For the listed organizations the legislation lays down the settings and technical features of video surveillance system, as well as the rules for its installation and application and the persons authorized to access video recordings, which is a significant measure for data security.

Within the framework of inspecting numerous organizations, in 2018, it was determined that it was possible to directly access video recordings through the video surveillance system, as well as to consult and extract video recording obtained through video surveillance (the so-called export). However, the systems lacked an electronic journal for recording the actions performed on the data (the so-called logs) and subsequently the companies failed to make a record of the actions performed on electronic data. Also, the persons authorized to access the system did not have a personified username and used a common name ("admin") and password. Accordingly, even if the system recorded the actions performed by a specific username, it was impossible to identify a particular person who processed the data.

To ensure the safety of electronic data, taking into account easy accessibility, it is important that organizations record every action performed on the data, including the data that was disclosed, when and on what basis. Herewith it is important that every person authorized to access personal data have an individual username and password in order to identify a person liable for unlawful use of data.

In light of the foregoing when data are processed by means of video surveillance the following should be taken into account:

- Video surveillance must be carried out only for the purpose laid down by the law and to the extent that is necessary to achieve the statutory purpose;
- In the process of video surveillance, it is essential to inform the persons within the field of view in accordance with the law. Particularly, it is necessary to place a warning sign in a visible area, informing organization's employees in written about the video surveillance and their rights, also, informing the owners of neighboring apartments in residential buildings and obtaining their consent on the installation of the system;
- To ensure data security organizations should implement appropriate rules and organizational and technical measures that enable recording every action performed on electronic data, and to determine personified and differentiated levels of access to video surveillance systems, per requirement and in accordance with their authority.

DIRECT MARKETING

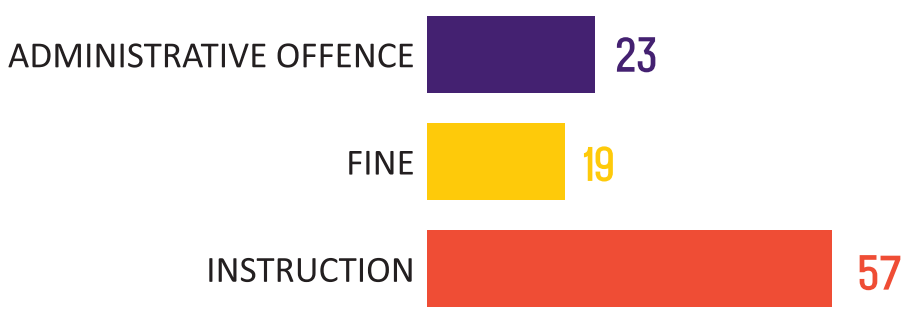
In 2018 direct marketing remained an outstanding issue. On the basis of 59 citizens' complaints the Inspector examined tens of direct marketing cases. In 23 cases the Inspector found the violation of statutory rules, fined 19 organizations and issued 57 mandatory instructions.

Notwithstanding numerous activities of the Inspector's Office in the context of awareness raisings, inspections and handling citizens' complaints, absence or malfunctioning of an opt-out mechanism remains problematic issue. On certain occasions the text of an opt-out mechanism does not clearly reflect the procedure of its use.

This year one more tendency came into light – several organizations maintained that the messages sent by them were not of an advertising nature but constituted an informational notification. The Law of Georgia on „Personal Data Protection" defines direct marketing as an offer of goods, services, employment or temporary job through mail, phone call, e-mail or another telecommunication means. Accordingly, any direct or indirect offer to an addressee of goods, services and/or employment suffices to consider that the offer is direct marketing. The aforesaid assessment made by the Inspector has been upheld by court decisions.

To prevent the violation of the law it is advisable that companies draft the texts of sent messages attentively and place an opt-out mechanism, so that the consumer will be able to opt out of unsolicited information.

DIRECT MARKETING, 2018



VAGUENESS OF OPT-OUT MECHANISMS

In the reporting period the Inspector's Office examined the cases when the advertising messages sent through a data processor (the so-called intermediary company) had an opt-out mechanism, but the indicated combination of digits and words could have been interpreted in a different way.

It is noteworthy that the major purpose of the regulations on direct marketing laid down in the law is to prevent the processing of a person's data contrary to his/her will. Therefore, the opt-out mechanism must ensure the achievement of this purpose and the citizens should be properly informed about their right to object to receiving messages.

SENDING MESSAGES VIA INTERMEDIARY COMPANIES

The cases examined in the reporting period indicate that in the majority of these cases advertising messages are sent via intermediary companies (including mobile service providers).

Within the framework of handling a complaint it was determined that a company used to send advertising texts via two different channels –through a mobile service provider and via web application of an intermediary company. Therefore, it used two different opt-out mechanisms and even if a citizen opted out via one mechanism, he/she was still receiving texts on behalf of the company via the second channel.

It is important that when data are processed through data processors, the companies create an effective mechanism that will enable them to stop processing the data completely for direct marketing purposes if data subject requests so.

In the reporting period it was also revealed that oftentimes the contract concluded between data controllers and processors did not cover significant issues such as: a person in charge of determining an opt-out mechanism for data subjects and of response; what happens if a data subject requests to stop processing his/her data without using the opt-out mechanism, by directly addressing the company; after the termination of contractual relations whether the data processor should transfer to the controller the database of telephone numbers that opted out of processing, etc.

Therefore, when direct marketing is carried out by an intermediary company the organization should lay down in the contracts the statutory requirements and the issue of forming and transferring the so-called black list, and introduce effective and adequate opt-out mechanisms.

COLLECTION OF DATA

In 2018 citizens often questioned the lawfulness of collecting their telephone numbers and requested to determine the source of data collection since they were not aware how the companies obtained these telephone numbers.

As a rule, the companies reference open sources for the collection of data for direct marketing purposes and the information obtained directly from customers within the framework of various services. However, oftentimes organizations fail to indicate specific sources of data collection and to record relevant information, which in turn increases the risk of unlawful data processing.

It should be noted that according to the applicable legislation a person is authorized to request information about the means of collecting his/her data. Therefore, it is important that an organization record the information about the sources of data.

Accordingly, when data are processed for direct marketing purposes organizations should:

- Together with an opt-out mechanism provide data subjects in a clear and understandable form with detailed information about the procedure of using the mechanism;
- Record the information about the sources of obtaining data for direct marketing purposes;

- Conclude a written agreement with an intermediary company and ensure that the statutory rules and limitations related to the processing of data for direct marketing purposes are reflected in the agreement.

Notwithstanding that the opt-out mechanism was introduced in practice, in certain cases it is not sufficient and effective to protect the citizens from the so-called spam messages. The applicable legislation enables the collection of data from open sources without citizens' consent and their subsequent use for direct marketing purposes. At the same time, considering the multitude of organizations carrying out direct marketing it is often difficult to identify a particular data controller. In order to protect the interests of the citizens, to take into account the European experience and to develop the legislation, it is advisable to review the applicable regulations, restrict the possibility of using open source data and to consider a citizen's informed consent as the only legal basis for conducting direct marketing. The Inspector has prepared a legislative initiative in this regard that will be submitted to the Parliament of Georgia at the beginning of 2019.