STATE INSPECTOR'S SERVICE

REPORT ON THE ACTIVITIES OF THE STATE INSPECTOR'S SERVICE

2019

STATE
INSPECTOR'S
SERVICE

REPORT ON THE ACTIVITIES OF THE STATE INSPECTOR'S SERVICE

2019

Norwegian Ministry
of Foreign Affairs

Empowered lives.
Resilient nations.

This publication has been created with the assistance of the Norwegian Government, the United Nations Development Program (UNDP) and the Office of the High Commissioner for Human Rights (OHCHR). Its contents are the sole responsibility of the State Inspector's Service and do not necessarily reflect the views of the Norwegian Government, UNDP and the OHCHR.

CONTENTS

STATE INSPECTOR'S FOREWORD

It is a great honor for me to serve as a State Inspector at the most important stage of the Service's development and transformation.

2019 stood out as a year of challenges and the new beginning for the State Inspector's Service. The vitally important function of investigating crimes committed by the officials was added to the functions of the Service. This has further increased our role and responsibilities in the sphere of human rights protection.

It was not easy to deal with novelties. The entire team has been working practically 24 hours, in order to respond well to the existing challenges. Despite short deadlines and scarce human

resources, we managed to start implementation of our new investigative powers without any hindrance to monitoring personal data protection and supervision over lawfulness of covert investigative actions.

This report will provide you with detailed information on the work carried out by the Service, on existing challenges, trends and achievements. However, this is only the start of the reforms. Due to a very short time since the introduction of our new mandate, some may still not fully appreciate the importance of establishing an independent investigative mechanism in Georgia, as well as of having its functions entrusted to the Service that enjoys only positive public attitude. I think, the 2020 Annual Report will even better reflect the results of the work of this institution and its importance.

The Office is determined to work hard in 2020, in order to respond well to high public expectations, to protect rights of each and every citizen and to provide timely and effective response to each violation.

The State Inspector's Service will actively cooperate with public and private sectors, with each target group for strengthening prevention-oriented policies. We will plan public awareness activities; ensure effective and impartial investigation and review of cases of human rights violations. International cooperation will be strengthened; public accountability will be our priority; at the same time, this year will be important in terms of organizational developments. We will work hard, to make our activities even more result-oriented and to make every employee of the State Inspector's Service proud of the work they do.

I would like to thank all representatives of government institutions, international organizations, the Public Defender's Office, non-governmental organizations and the private sector, as well as each and every citizen, who actively cooperated with the Service and made a valuable contribution to the development of the State Inspector's Service. I would also like to thank my predecessor, former

State Inspector – Ms. Tamar Kaldani, who gracefully handed over the mandate of the successful institution.

I would like to extend my special gratitude to every employee of the State Inspector's Service who carried out their work professionally and made tireless efforts for overcoming challenges that we faced and for constantly caring for protecting human rights. It is our goal to establish a high professional standard through our qualified conduct.

State Inspector,

Londa Toloraia

MISSION STATEMENT AND VALUES OF THE STATE INSPECTOR'S SERVICE

I. MISSION STATEMENT AND VALUES OF THE STATE INSPECTOR'S SERVICE

The State recognizes and respects human rights and freedoms. In case of human rights violation, a person shall have access to an effective legal remedy.

The State Inspector's Service is a mechanism for preventing and reacting to violations of human rights.

The mission of the State Inspector's Service is to encourage the establishment of a culture of respect for privacy, to carry out an effective supervision over personal data protection, to ensure comprehensive, impartial and effective investigation of specific crimes committed by a representative of law enforcement authorities, by an official, or a person equal to an official.

While carrying out its duties, the Service shall be guided by the following values and principles:

- **Independence and Political Neutrality –** the State Inspector's Service is independent and it is not subordinated to any institution, official and/or political force;
- **Lawfulness –** the activities of the State Inspector's Service are guided by the Constitution and the legislation of Georgia;
- **Protection and Respect for Human Rights and Freedoms –** the State Inspector's Service strives to ensure protection and respect for human rights and freedoms. Its work is guided by the principles of equality and non-discrimination. It also respects and appreciates needs and specificities of vulnerable groups;
- **Impartiality, Objectivity and fairness** – the activities of the State Inspector's Service are guided by the principles of impartiality, objectivity and fairness;
- **Engagement of an applicant and a victim** – the State Inspector's Service ensures engagement of an applicant and the victim/his or her representative in the case handling process and protection of their interests;

- **Timely and comprehensive response** – the State Inspector's Service fully understands the importance of its work and performs all required actions in order to proceed with each and every case in a timely manner and within reasonable deadlines;
- **Transparency and Openness** – the State Inspector's Service is accountable to the public. It is open to cooperation and proactively disseminates information about its activities;
- **Professionalism** – the State Inspector's Service constantly strives to recruit professional employees, and to raise qualification of its staff in order to ensure high quality of its work and to overcome contemporary challenges;
- **Development-Orientation** – the State Inspector's Service regularly assesses its performance and challenges and is concerned about development;
- **Innovation** – the State Inspector's Service applies modern technologies, approaches, and methodologies in its work;
- **Teamwork** – the structural units/employees of the Service have integrated vision, aspirations and goals. They work all together to overcome existing challenges the Service faces.

MANDATE OF THE STATE INSPECTOR'S SERVICE

II. MANDATE OF THE STATE INSPECTOR'S SERVICE

The State Inspector's Service is an independent state authority accountable solely to the Parliament of Georgia. The Service was established on 10 May 2019 as a successor of the Office of the Personal Data Protection Inspector (operating since 2013).

According to the law of Georgia on "The State Inspector's Service", the Service performs its functions in three directions:

- Monitoring lawfulness of personal data processing;
- Monitoring covert investigative actions and activities performed within the central databank of electronic communications identification data;
- Ensuring impartial and effective investigation of specific crimes committed by a representative of law enforcement authorities, by an official or a person equal to an official.

The State Inspector's Service is equipped with various powers for discarging its functions.

The State Inspector's Service carries out preventive actions and responds to violations in order to control lawfulness of personal data processing: the Service delivers consultations on personal data protection to the interested persons, contributes to public awareness-raising, reviews citizens' complaints and monitors lawfulness of personal data processing by conducting inspections.

In order to monitor covert investigative actions as well as the activities performed in the central databank of electronic communications identification data, the State Inspector's Service receives documents from various state agencies throughout 24 hours (from courts – decisions on carrying out covert investigative actions; from the Prosecutor's Office of Georgia - the rulings by prosecutors on conducting covert investigative actions due to urgent necessity; from law-enforcement bodies – written records of covert investigative actions; from electronic communications companies – about transferring identification data of electronic communication to a law-enforcement authorities), verifies submitted documents with the information reflected in the electronic systems and through the electronic system controls the central databank; It also conducts inspections of data controller/data processor;

The State Inspector's Service Investigates following crimes committed after 1 November 2019:

- Torture (Article 144[1] of the Criminal Code of Georgia);
- Threat of Torture (Article 144[2] of the Criminal Code of Georgia);
- Degrading or Inhuman Treatment (Article 144[3] of the Criminal Code of Georgia);
- Abuse of official powers, committed using violence or a weapon, or the same act resulting in offending personal dignity of the victim (Article 332, sub-sections 'b' and 'c' of the Criminal Code of Georgia);
- Exceeding official powers committed using violence or a weapon or by offending personal dignity of the victim (Article 333 sub-sections 'b' and 'c' of the Criminal Code of Georgia);
- Coercion to providing explanation, evidence or opinion (Article 335 of the Criminal Code of Georgia);
- Coercion of a person placed in a penitentiary institution or liberty rest into changing evidence or refusing to give evidence, as well as coercion of a convicted person in order to interfere with the fulfillment of his/her civil duties (Article 378.2 of the Criminal Code of Georgia);
- Other crime resulting in the death of a person, who at the time of death was placed in the temporary detention temporary detention isolator, at the penitentiary establishment or in any other detention facility where he/she had been confined by a representative of a law-enforcement body, an official or a person equal to an official against his/her will and where the detained person had no right to leave the place of detention or was otherwise placed under effective control of the state.

The State Inspector's Service is authorized to carry our full-scale investigation and apply operative and investigative actions in the cases of abovementioned crimes.

STRUCTURE AND HUMAN RESOURCES OF THE STATE INSPECTOR'S SERVICE

III. STRUCTURE AND HUMAN RESOURCES OF THE STATE INSPECTOR'S SERVICE

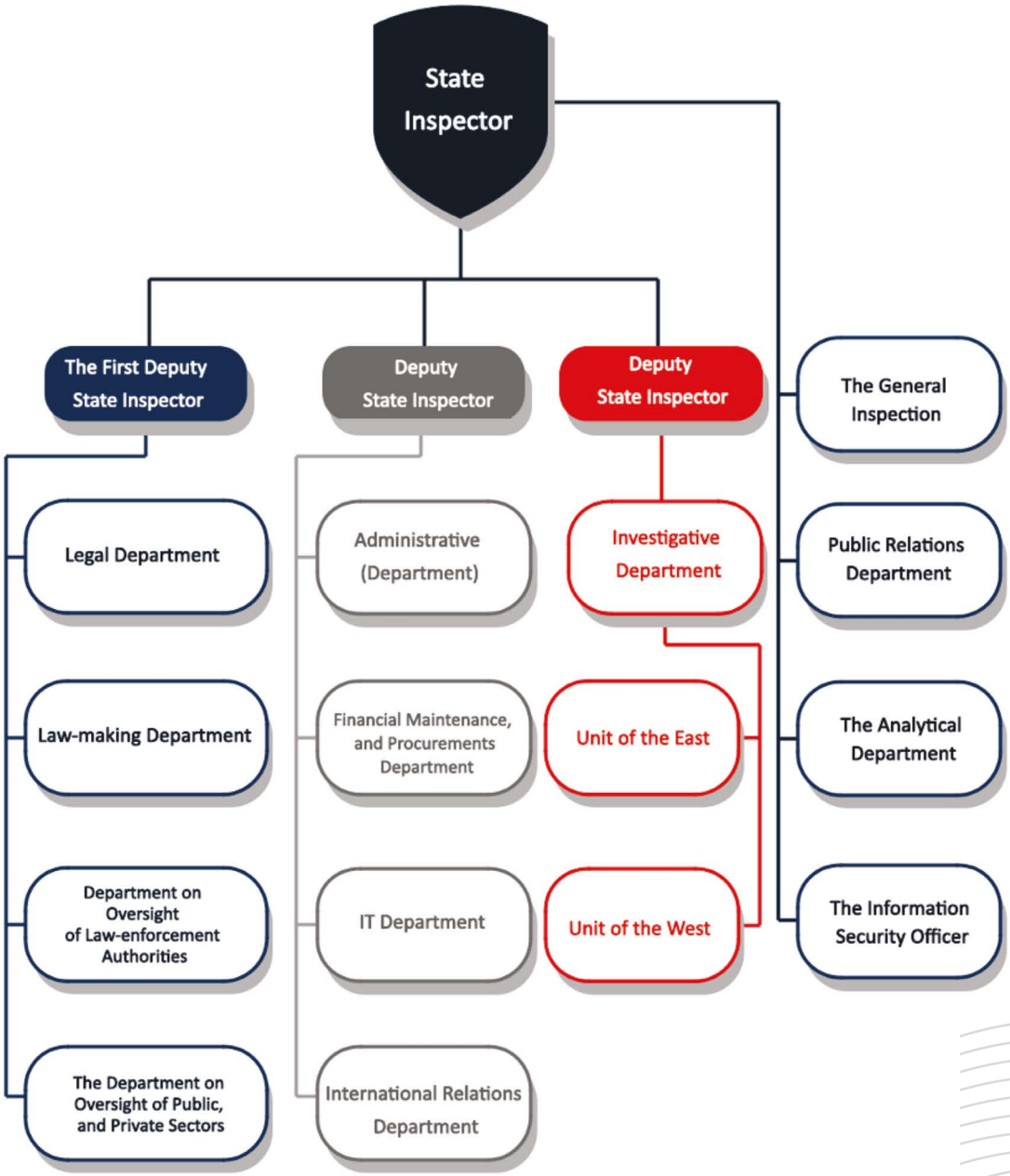
The State Inspector's Service is managed by the State Inspector, who is elected by the Parliament of Georgia for a 6-year term. The inspector has 3 deputies, whose functions are clearly delineated.

This year was important in terms of structural renewal. In parallel to expanding functions of the Service (the new function of investigation was added) the total number of employees of the Service went up from 53 to 116. Three new structural entities were created: Investigative Department, Analytical Department and General Inspectorate.

The function of the Investigative Department is to impartially and effectively investigate certain crimes committed by a representative of a law-enforcement authority, by an official, or a person equal to an official.

The General Inspectorate monitors the observance of Georgian legislation and fulfillment of the State Inspector's individual administrative-legal acts by the employees of the State Inspector's Service; reveals instances of conflict of interest, violation of ethics and internal regulations; reacts to possible violations against other persons' rights, to administrative offenses and other violations committed by the employees of the State Inspectors Service,.

As for the Analytical Department, it is responsible for collecting and processing statistical data; it also drafts analytical documents on trends and challenges in the areas of investigation and personal data protection and elaborates recommendations for improving quality of work.


State Inspector
The First Deputy State Inspector
Deputy State Inspector
Deputy State Inspector
The General Inspection
Legal Department
Administrative (Department)
Investigative Department
Public Relations Department
Law-making Department
Financial Maintenance, and Procurements Department
Unit of the East
The Analytical Department
Department on Oversight of Law-enforcement Authorities
IT Department
Unit of the West
The Information Security Officer
The Department on Oversight of Public, and Private Sectors
International Relations Department

Professional development of the staff is a constant process at the State Inspector's Service and great attention is dedicated to raising their qualification. Working procedures and information technologies are constantly upgraded. The Service, therefore, invests in deepening knowledge, upgrading competencies as well as professional and social skills of its employees in order to properly respond to new challenges.

Throughout 2019 14 educational activities were carried out for the professional development of the staff of the State Inspector's Service and total of 122 participants were retrained.

Considering the specificities of the work of the State Inspector's Service following training activities were held: Risk Assessment, Mastering Communication Skills, General Overview of the EU Law, Administrative Offences, Occupational Safety, Personal Data Protection in the Course of Investigation, New Electronic Criminal Case Management System, Prohibition of Torture, Inhuman or Degrading Treatment; Positive Obligations of a State and Effective Investigations; Effective Investigation of Hate Crimes; Gender Equality and Violence against Women.

In addition, 23 employees of the Service are currently enrolled in the Course on Personal Data Protection and Privacy Rights through the Council of Europe distance learning platform (HELP).

The aim of all previous and planned educational activities is to promote introduction of European human rights protection standards in the work of the State Inspector's Service and to contribute to upgrading and developing professional qualifications of staff.

INTERNATIONAL AND STRATEGIC PARTNERS ABOUT THE STATE INSPECTOR'S SERVICE

INTERNATIONAL AND STRATEGIC PARTNERS ABOUT THE STATE INSPECTOR'S SERVICE

Let me again congratulate Georgia on the establishment of its new independent institution, the State Inspector's Service, with the important task to carry out key oversight functions of state institutions and private companies. Merging the two pillars of personal data protection and investigations into crimes committed by law enforcement officers under one authority was a challenging task, but a task taken on with commitment and dedication. I commend the data protection staff who have taken an active role in modifying their home institution and new staff taking on pioneer roles in defining and shaping the new functions.

The State Inspector is mandated to oversee state institutions where their actions infringe upon the rights and freedoms of citizens, to ensure that they adhere to applicable legislation. The ability to register and follow up on citizen's complaints is necessary to effectively protect these rights and hence a necessity for any well-functioning democracy. It was, therefore, with great anticipation that we welcomed the new State Inspector's Service last year as the competent body to fill this gap in the overall oversight architecture.

The first Annual Report of the State Inspector's Service gives testimony to the activities carried out and the impact the institution has already had on peoples' lives, in particular in defending their privacy. The European Union remains an avid supporter of both pillars of the new institution. New EU assistance is being prepared with the aim to further strengthening all core functions of the institution in the interest of Georgian citizens. Congratulations on a good start. Keep up the good work!

Carl Hartzell

Ambassador of the European Union to Georgia

We have a very good cooperation with the State Inspector's Service, in view of supporting this institution to fulfill its mandate in the areas of data protection and investigation respectively. The motivation of the Service's leadership and staff to strive for high standards of their work is outstanding, and very much appreciated. This has certainly contributed to the achievement of very good results, bringing this work closer to European standards.

In the field of data protection, the Council of Europe and the State Inspector›s Service have developed important e-learning and awareness raising tools for Georgian legal practitioners, as well as media representatives. I hope that these and future efforts will facilitate Georgia›s accession to the Council of Europe Modernized Convention for the Protection of Individuals with regard to the Processing of Personal Data, which will help aligning Georgia›s law and practice with European standards in this field.

Meanwhile, development of a truly independent investigating mechanism of possible abuses by law enforcement agencies is an important expectation of the Georgian civil society and public at large. The Council of Europe will support work aimed at institutional capacity building and policy development, as well as awareness raising, in order to ensure that this function is carried out efficiently.

I wish the State Inspector and the entire staff of the Service success in their work, to the benefit of the people of Georgia.

Cristian Urse
Head of Council of Europe Office in Georgia

UNDP has been a proud supporter of the State Inspector's Service from the very beginning and offers congratulations on the achievements of 2019, including the adoption of new investigative functions.

In a shared mission to protect personal information and data from the multiplying threats posed by new technologies, UNDP Georgia began supporting the Personal Data Protection Inspector's Office immediately upon its establishment. This support has included advising on legislative changes, building institutional capacity and broadening public awareness. The Office has become an institutionally strong and professional body with high public trust, as is clear in the steady increase in applications from citizens and six consecutive years of growth in the number of inspections conducted. This shows that more and more people are grasping the importance of personal data protection.

In 2019, the Office took on new functions to investigate crimes committed by law enforcement personnel. This was a transformation advocated by UNDP as a timely and necessary contribution to the protection of human rights in the country. UNDP is now working with our international partners to support the State Inspector's Service in undertaking its new investigatory functions while maintaining high professional standards in protecting personal data. The State Inspector's Service has a crucial role to play in Georgia's democratic development and UNDP is proud to continue to stand by its side.

Louisa Vinton
UNDP Resident Representative in Georgia

The adoption of the Law on State Inspector's Service was an important step forward in combating torture and other forms of cruel, inhuman or degrading treatment in Georgia. State Inspector's Service is seen as a ray of hope in the struggle to tackling a long standing of impunity by conducting investigations of allegations of human rights abuses committed by representatives of law enforcement agencies.

The adoption was preceded by considerable number of recommendations and suggestions by universal and regional human rights supervisory bodies, high level experts, Public Defender, international and national NGOs[1]. OHCHR Field Presence in South Caucasus[2], was privileged and pleased to assist the authorities in developing the law and its basic principles and on the other hand advocate its adoption as well as provide substantial first hand assistance to the newly created service.

The Law foresees strong guarantees of independence and impartiality of the State Inspector who is independent from executive and accountable only to the Parliament of Georgia. We are convinced that these guarantees will bring long awaited results and increase the credibility among of Georgia's efforts to increase respect for human rights in the Georgian society. The statistics -- 68 cases being addressed only in 2 months (from 1st November 2019 to 31 December 2019) and additional 59 cases pending before the State Inspector's Service as of 23rd of March 2020 -- demonstrate the volume of the work the service has before it, and also serves as a clear proof that alleged victims of ill treatment trust the newly created Service and hope that it will bring justice. Along with State Inspector, we all bear responsibility to ensure that these hopes of victims are fulfilled.

Vladimir Shkolnikov

Senior Human Rights Adviser,
Office of the UN High Commissioner for Human Rights for South Caucasus

1 The EU Special Adviser on Constitutional and Legal Reform and Human Rights in Georgia Mr. Thomas Hammarberg in 2013, the former UN High Commissioner for Human Rights Ms. Navi Pillay in 2014, the UN Human Rights Committee in 2014, the Council of Europe's Committee on Prevention of Torture in 2014 and 2018, Georgia's Public Defender in his/her reports 2014-2018 all called on the authorities to create an independent mechanism for investigation of allegations of human rights abuses committed by law enforcement representatives.

2 In the framework of EU funded project 'Human Rights for All'

Good governance is a key pillar of the U.S.-Georgia strategic partnership. USAID supports the Government of Georgia to ensure that public services are provided in an effective, efficient, and transparent manner. Stronger personal data protection standards are crucial to good governance and a precondition for Georgia's capability to plan, finance, and implement its own solutions to development challenges.

Georgia formally recognized this in 2013 when it established the body we now know as the State Inspector's Service, which is tasked with ensuring personal data protection in the country. Here are a few reasons why USAID considers the work of the State Inspector's Service to be so important.

First, establishing and enforcing strong standards for personal data protection is necessary for the Government of Georgia to protect human rights and fundamental freedoms in this country.

Second, the Government of Georgia has committed to improving personal data privacy under the EU-Georgia Association Agreement. Progress in this area means progress toward Europe.

Third, data protection is growing in importance in an era when governments and businesses increasingly rely on information technologies to function.

We're encouraged by the progress that has been made even as we see room for further improvement. USAID is proud to partner with the State Inspector's Service and will continue to strengthen its capacity to better serve the Georgian people.

Peter A. Wiebler
Mission Director, USAID/Georgia

Successful bilateral cooperation between the Georgian and the Polish data protection authorities has always been of importance to us and one of the priorities of our international activities. From the beginning of the functioning of the Georgian authority, the Polish DPA offered its support to it. We welcomed the Georgian authority's declaration upon its establishment in 2013 to aim at achieving the highest standards of personal data protection. Therefore, we offered our support in terms of giving advice and information on the aspects of the functioning of a data protection authority, as well as exchanging experience in the field of personal data protection and in general developing cooperation between our DPAs. Those objectives were achieved among others during the visit paid by the Polish delegation at the Georgian authority's office in Tbilisi 2014, as well as subsequent visits of the Georgian delegation at the Polish DPA's seat in Warsaw in 2015 and 2017, and the visit of the Polish delegates in Tbilisi in 2018. It is worth stressing that the latter two visits were organised within the framework of the EU and UNDP project "Human Rights for All".

In 2014 the Georgian DPA was accepted as member of the Central and Eastern Europe Data Protection Authorities (CEEDPA), a group established at the initiative of the Polish DPA for the purpose of international cooperation between Central and Eastern Europe DPAs, with the fundamental objective of supporting newly established DPAs. The Georgian DPA became an active member of the Group and in 2017 hosted the 19th CEEDPA annual meeting in Tbilisi.

During the meeting on 18 August 2015 in Warsaw, the Memorandum of Cooperation was concluded between the Polish and the Georgian DPAs, providing for developing the relationship between the Parties in all areas of common interest, in particular the promotion of personal data protection of both countries. Bilateral cooperation has been conducted in the areas such as legislative, institutional and technological developments, programs aimed at promoting personal data protection and organisation of conferences, study visits and other meetings. The delegates of both authorities actively participate in the data protection events organised by the Polish and the Georgian DPA.

The international activities of the Georgian DPA on various fora need to be highlighted. An important forum of cooperation between the European DPAs is the annual Conference of European Data Protection Authorities. The Georgian DPA was the host of the 29th edition of the Conference in

2019 in Tbilisi, which focused on such important topics as the implementation and application of GDPR, the modernised Convention 108+ and the impact of international organisations on raising data protection and privacy standards.

To sum up, the President of the Personal Data Protection Office would like to stress the importance of the variety of activities of the State Inspector of Georgia in the field of personal data protection. It also needs emphasising that the President of the Office much appreciates friendly and successful cooperation with the State Inspector of Georgia and looks forward to its further development.

Jan Nowak
President of the Personal Data Protection Office of Poland

MONITORING THE LAWFULNESS OF PERSONAL DATA PROCESSING

IV. MONITORING THE LAWFULNESS OF PERSONAL DATA PROCESSING

MAJOR INNOVATIONS WITH REGARDS TO PERSONAL DATA PROTECTION IN 2019

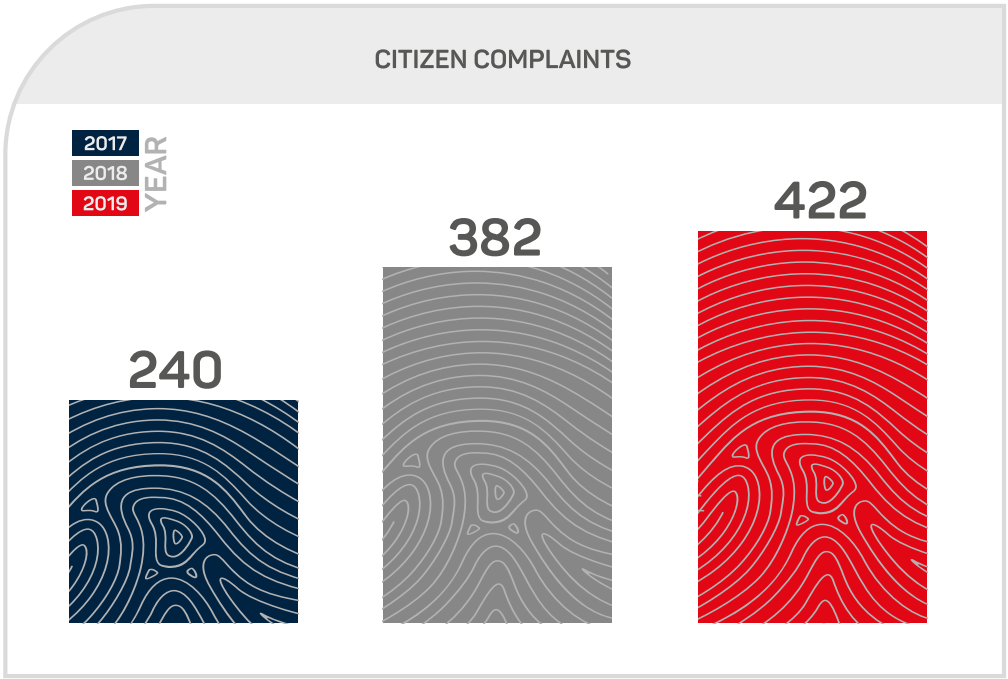
- SERVICE PRESENTED THE LEGISLATIVE PROPOSAL ON "PERSONAL DATA PROTECTION" TO THE PARLIAMENT OF GEORGIA
- GEORGIA HOSTED THE SPRING CONFERENCE OF EUROPEAN DATA PROTECTION AUTHORITIES FOR THE FIRST TIME
- RECOMMENDATIONS ON PERSONAL DATA PROCESSING BY COMMERCIAL BANKS WERE DEVELOPED
- A MANUAL OF EUROPEAN LAW ON PERSONAL DATA PROTECTION AND GUIDELINES FOR THE PROTECTION OF PRIVACY IN THE MEDIA SPACE WERE TRANSLATED INTO GEORGIA AND PUBLISHED
- WITHIN THE SCOPE OF THE COUNCIL OF EUROPE DISTANCE LEARNING PLATFORM (HELP) A TRAINING COURSE ON PERSONAL DATA PROTECTION AND THE RIGHT TO PRIVACY WAS IMPLEMENTED FOR THE FIRST TIME IN GEORGIA
- NEW WEB-PAGE WAS LAUNCHED FOR THE PROPOSE OF IMPROVING PUBLIC COMMUNICATION AND INFORMATION
- THE ELECTRONIC MANAGEMENT SYSTEM FOR CONSULTATION, APPLICATIONS/COMPLAINTS, NOTIFICATIONS, AS WELL AS INSPECTIONS WAS INTRODUCED
- COMMUNICATION STRATEGY OF THE SERVICE WAS DEVELOPED IN ORDER TO RISE PUBLIC AWARENESS, IMPROVE CREDIBILITY OF THE SERVICE AND ENGAGE IT IN EFFECTIVE PUBLIC COMMUNICATION

1. GENERAL OVERVIEW

This chapter provides information on following topics: general state of personal data protection in 2019, main trends, open problematic issues, challenges, general statistical data and the activities of the State Inspector's Service in Georgia.

In parallel to outlining the main statistical information, the report provides more detailed account of those cases of personal data processing that are subject to a high number of applications, are connected with people's everyday lives and/or are sensitive, or that enjoy high public interest.

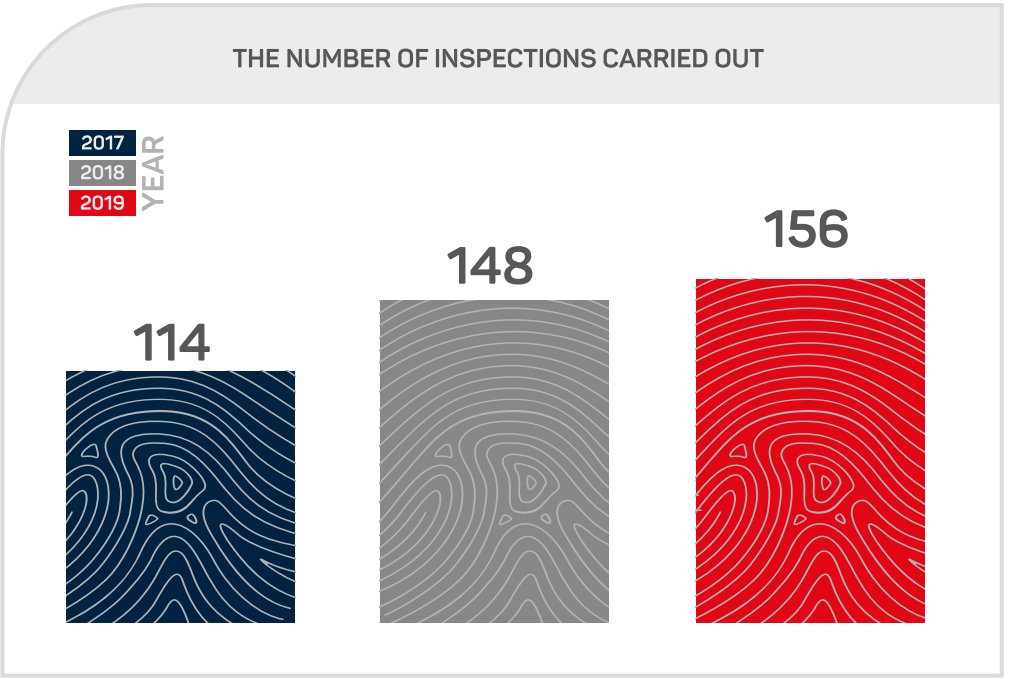
The rate of filing complaints maintained its upward trend throughout 2019. 422 persons filed a complaint with the Service.



242 applications were made by data subjects, 175 – by other interested persons and 5 applications were anonymous.

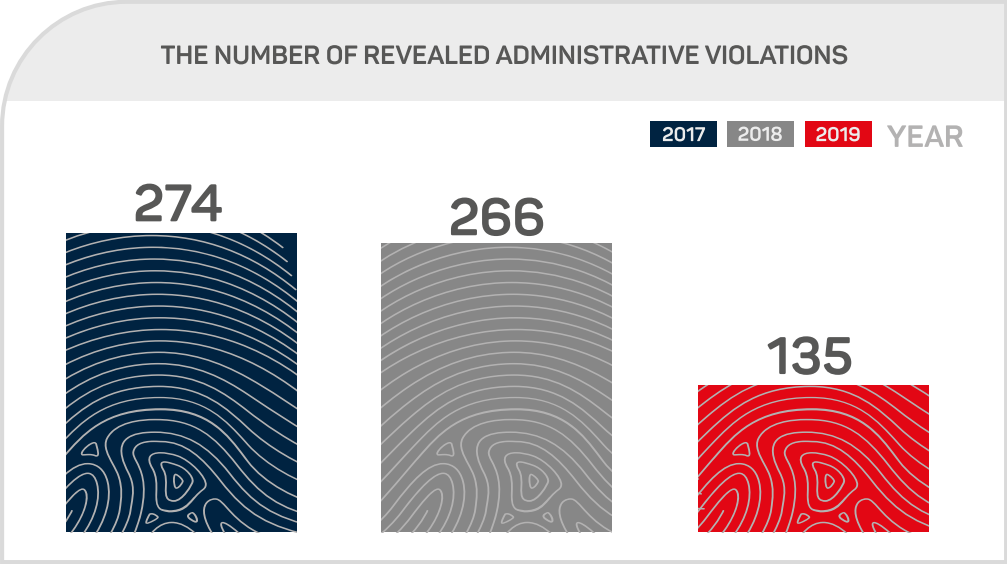
81% of submitted complaints concerned data processing in private sector; 11% - concerned processing of personal data in law enforcement authorities and 8% - in other public bodies.

The number of inspections also increased in 2019 same as in previous years. The State Inspector's Service conducted 156 inspections; 29% of total inspections were carried out on the initiative of the State Inspector's Service, while 71% were carried out as a response to complaints and notifications.



The inspections carried out on the initiative of the State Inspector's Service aimed at monitoring lawfulness of personal data processing by public institutions (41%), private entities (35%) and by law enforcement authorities (24%).

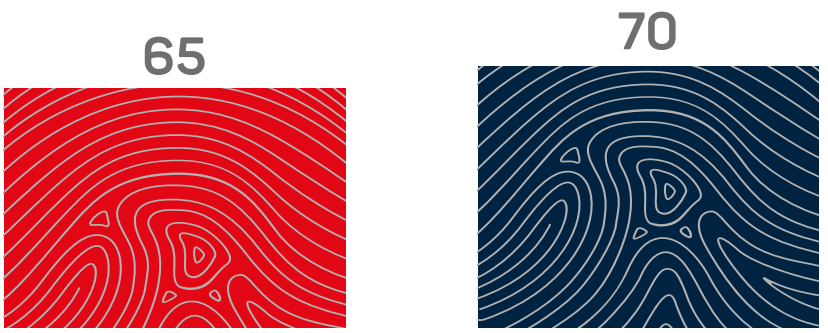
In 2019 the State Inspector's Service has identified 135 cases of unlawful processing of personal data.



As for the types of violations, the most frequently committed offence in 27 cases (20%) was the failure to comply with data security requirements (the offence stipulated in Article 46 of the Law of Georgia on Personal Data Protection); 25 offences (18%) involved data processing without legal grounds (Article 43), 24 cases (18%) dealt with offences of principles of data processing (Article 44); 17 cases (12%) – were related to offences of video surveillance rules (Article 48); 12 cases (9%) involved the violation of the rules for notification of a data subject by a data controller (Article 50); 12 cases (9%) – dealt with misusing of personal data for direct marketing purposes (Article 47); 9 cases (7%) concerned the data processing without observance of data processing rules by a data processor (Article 52); in 4 cases (3%) special category data were processed without legal grounds (Article 45); 3 cases (2%) – concerned the non-fulfilment of the requirements of the State Inspector's Service (Article 53); 1 case (1%) – concerned violation of rules of processing data for registration of entry into and exit from buildings of public and private institutions (Article 49); 1 case (1%) – concerned violation by a data controller of established rules of assigning data processing tasks to a data processor (Article 51).

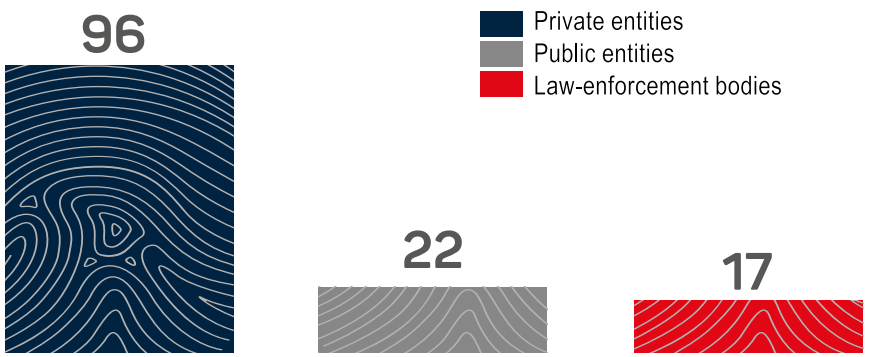
In 52 % of administrative offences, fine was applied as an administrative penalty, while in 48% of cases warning was issued.

ADMINISTRATIVE SANCTIONS IMPOSED



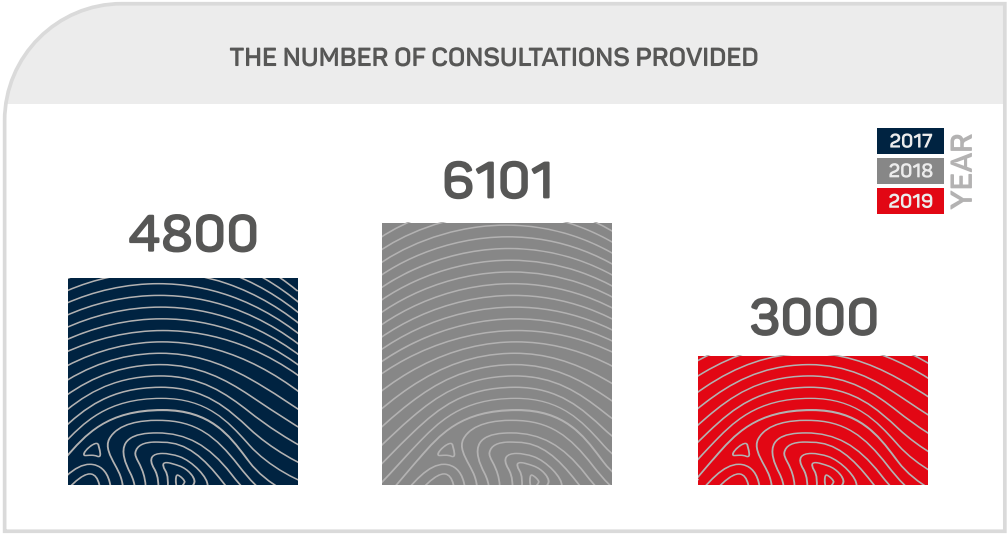
In 96 cases administrative liability was imposed upon a private entity, in 22 cases – on public bodies and in 17 cases – on law enforcement authorities.

PERSONAL SUBJECT TO ADMINISTRATIVE LIABILITY



In parallel with the application of administrative sanctions, the State Inspector's Service issued 195 recommendations and mandatory instructions to data controllers in order to eradicate shortcomings. Vast majority of them have been fulfilled, while some are in the process of implementation.

In 2019 the State Inspector's Service continued to provide consultations, however, the number of requests for consultations decreased. This might be a result of ongoing structural reforms at the Service (adding a new function, changing a name).

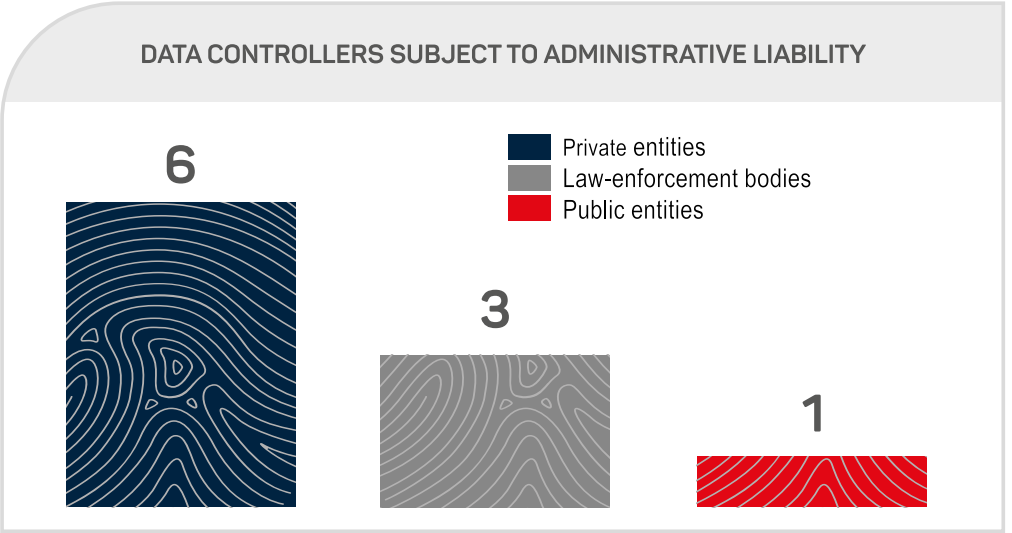


2. PROTECTION OF DATA SUBJECT'S RIGHTS

The law of Georgia on Personal Data Protection grants certain rights to a data subject (to request information about processing of his/her personal data, to request to have his/her personal data corrected, renewed, supplemented, blocked, deleted and destroyed; to withdraw at any point his/her consent on processing his/her personal data; to address the State Inspector's Service or the court concerning any violation of his/her rights), and a data controller shall ensure practical application of these rights.

The State Inspector's Service reviewed 21 cases throughout 2019 concerning the rights of data subjects: 10 cases against public institutions (including 9 – against law enforcement bodies) and 11 cases against private entities.

As a result, 12 administrative offences have been revealed. Administrative liability was imposed upon 6 private institutions, 3 cases resulted in a liability of law enforcement bodies and 1 case concerned other public entity (several data controllers were imposed administrative sanctions for more than one offence).



2.1. PROVIDING INFORMATION TO A DATA SUBJECT

According to the Law of Georgia on Personal Data Protection, when collecting data directly from a data subject, data controller or a data processor shall provide data subject with the following information: the identity and the registered address of the data controller and the data processor (when applicable); purpose of data processing; whether provision of data is mandatory or voluntary; if it is mandatory to provide information on legal consequences of refusal to submit them; the right of a data subject to obtain information on his/her personal data processed, request their correction, updating, addition, blocking, deletion and destruction.

The analysis of cases reviewed by the State Inspector's Service demonstrates that in the course of administrative proceedings conducted by public bodies, they fail to provide comprehensive information to data subjects, including about the fact that their interviews are being audio-video recorded.

2.2. REQUESTING INFORMATION BY A DATA SUBJECT

The State Inspector's Service examined the cases of informing data subjects by private and public entities based on the applications of data subjects. As a result, violation of established rules was revealed in number of cases. Following types of violations have been identified: the data subject

was not provided information within 10- days term established by the law; the information provided was not complete and didn't comply with the request; the data subject's right to receive information was unlawfully restricted.

Reorganization, application of new case management systems, systematization of archives and other similar reasons were cited as cause for not providing information within established deadlines. These reasons have been considered non-compliant with the law, as the law provides for no possibilities of extending established deadline for informing the data subject.

In contrast with the requesting information on data processing, the law establishes no deadlines for handing over copies of documents containing personal data to a data subject. However, it is important to satisfy the request of a data subject in a reasonable time in order to ensure efficient implementation of data subject's rights. Reasonability of this term should be assessed considering the volume of work that needs to be carried out, the form in which the requested document is being kept, need for requesting information / document from other structural entities or subdivisions and other factors characteristic to each individual case. In some cases, that were reviewed by the Service, unreasonable delays have been established. The State Inspector's Service considered that failing to submit information in a reasonable time constituted the violation of the rule of informing data subject and issued relevant recommendations.

The cases reviewed during the reporting period also indicate that data controllers do not always substantially review individual circumstances of data subjects' requests; the data subjects often receive incomplete information issued based on certain templates that do not correspond to data subjects' requests.

According to the law of Georgia on Personal Data Protection, it is possible to restrict data subject's right to receive information only in cases when exercise of these rights endangers: the interests of national security and defence, the interests of public security, crime detection, investigation and prevention, significant financial and economic interests of the country. In some cases, the State Inspector's Service found the restriction of data subject's right unlawful.

Following trend was observed in 2019 in relation to restricting data subject's right to information: persons having status of a victim in criminal proceedings requested criminal case files, referring to the provisions of the Law of Georgia on Personal Data Protection. The Criminal Procedure Code of Georgia does not entitle a victim in a criminal procedure to receive copies of criminal case file, which may be assessed as a rule limiting data subject's right to information. However, the State Inspector's Service issued a recommendation to respective entities (Ministry of Internal Affairs of Georgia and Prosecution Service of Georgia), requiring that they assess balance between the

interests of a data subject and other lawful interests and issue information to a data subject if no legal grounds for restricting their right to information are present. It is noteworthy to mention that in the majority of cases that were reviewed, relevant competent bodies provided copies of respective documents to data subjects.

2.3. RECOMMENDATIONS

The cases reviewed in relation to data subject's rights during the reporting period attest that timely and complete submission of information related to data processing, as well as maintaining fair balance between the interests of a data subject and other legitimate interests – remain a challenge.

In order to effectively apply data subjects' rights, data controller shall:

- Inform a data subject of his/her rights stipulated by the law, including in the cases, when data is collected online;
- To inform / warn a data subject of audio/video recording (it is recommended to record fulfillment of this requirement for the purposes of future verification);
- In case of request, provide a data subject with relevant, complete and accurate information in a plain and understandable language;
- To provide information to a data subject within the term stipulated by law or within reasonable time, where such deadlines are not established;
- In case of restricting data subject's right, to apply restrictions that are strictly necessary for the purposes of respective restriction.

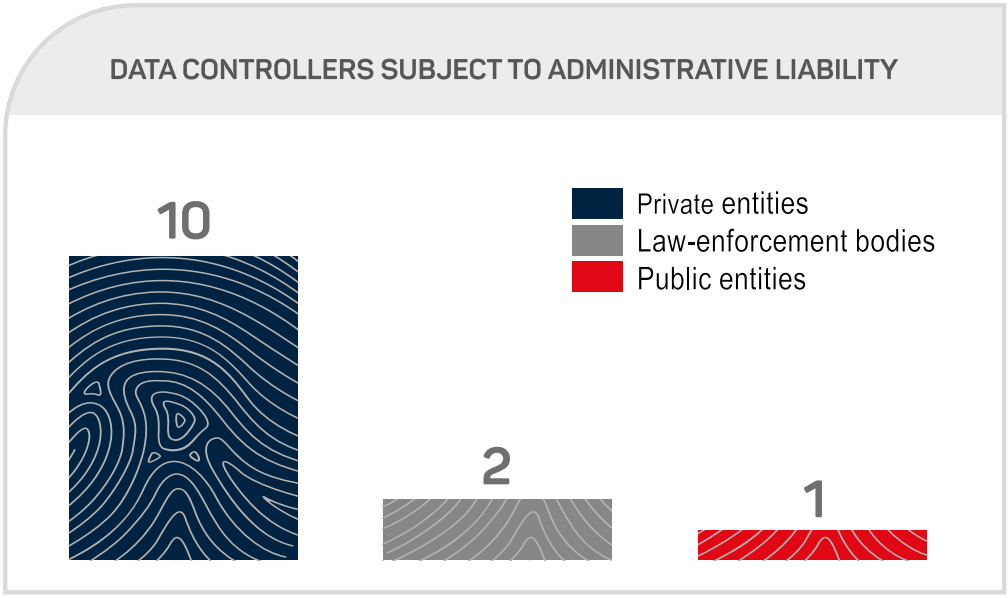
3. DATA PROCESSING IN ELECTRONIC SYSTEMS

As modern technologies develop, more public and private entities process personal data in electronic systems. Therefore, ensuring lawfulness of personal data processing in electronic systems and databases constitutes one of the most important challenges of data protection.

The Law of Georgia on Personal Data Protection specifies the measures data controller shall take. Namely, according to the Law, data controller shall take appropriate organizational and technical measures to ensure protection of data against accidental or unlawful destruction, alteration, disclosure, collection, or any other form of unlawful use, and accidental or unlawful loss. Measures applied for data security shall be appropriate to the risks associated with data processing. At the same time, a data controller shall register all operations performed in relation to electronic data. Any employee of a data controller and of a data processor, who is involved in processing of data shall remain within the scope of powers granted to him/her.

In 2019 the State Inspector's Service has reviewed total of 24 cases of personal data processing in various databases on its own initiative, as well as based on applications by interested parties: 12 of them in public entities (including 8 – by the law enforcement bodies) and 12 – in private sector.

As a result of inspections, 18 cases of administrative offences were revealed. Private entities were subject to administrative liability in 10 cases, law enforcement bodies – in 2 cases and a public institution other than a law enforcement body – in 1 case (several data controllers were imposed administrative liability for more than one offence).



3.1. PRIVATE SECTOR

When reviewing lawfulness of personal data processing by private entities throughout 2019, the following were found:

- Through their webpages, they collect and store more data than they need for providing services to their consumers (this mainly concerns requesting unnecessary data for registration on websites);
- They do not register all operations performed in relation to electronic data in the databases that contain consumers' personal data, therefore it is impossible to establish who and when had access to consumers' personal data;
- Majority of them have not established for how long data can be stored and they keep personal data of consumers even after the purpose of data processing has already been achieved or is no longer relevant, and/or when the consumer no longer wants to have his/her personal data processed by the company.

The companies were found administratively liable in order to prevent similar violations in the future. In addition, they were given mandatory instructions to apply necessary organizational and technical measures for ensuring security of electronic data.

3.2. PUBLIC SECTOR

The State Inspector's Service examined data processing in electronic programs implemented by public entities. As a result, it was found that relevant organizational and technical measures for ensuring data security had not been applied. Namely: the programs did not register facts of accessing and viewing of data; there was no record of information searched by a consumer in the system.

✓ *After inspecting the electronic case management system of the Tbilisi City Court (which has a record of ongoing cases and parties to those cases) it was found that any authorized user of the system had access to case files registered in the system, however the facts of accessing and viewing those files were not registered. Considering the number of persons employed at the court, as well as the number of the access and volume of data contained within the electronic system, there is a risk that processing of data contained in the system might go beyond legal purposes of administering justice and a user could view and/or use information concerning an ongoing court case for*

personal purposes. In order to ensure data security, Tbilisi City Court was instructed to apply necessary organisational-technical measures and to implement mechanisms that would ensure registering of all operations in relation to electronic data, including viewing data (According to the statement of the High Council of Justice, it is planned to launch a new case management system in the common courts, which will have a function of registering all operations).

✓ *As a result of inspecting Treasury Service of the Ministry of Finance of Georgia it was revealed that the electronic system of the Service (through which state funds are transferred and electronic circulation of documents between the State Treasury and the budgetary organisations is ensured) has a function of registering all operations in relation to data, however it doesn't record information with respect to which natural person's data was processed by a person authorized to access the system. (The Treasury service of the Ministry of Finance of Georgia was instructed to apply organizational–technical measures that would allow registration of all operations in relation to electronic data. Ministry has made necessary adjustments.*

3.3. LAW ENFORCEMENT BODIES

For crime prevention, investigation, carrying out operative-investigative activities and for protecting rule of law, law enforcement bodies possess databases containing large volumes and sensitive categories of personal data.

The analysis of data processing in those databases demonstrates that organizational-technical measures applied by those agencies for ensuring data security are not sufficient. Namely: they do not register all operations performed in relation to data; term for the storage of data is not specified; the mechanisms of automatically deleting or depersonalizing data after certain period of time are not applied; the need for granting access to databases to certain persons or institutions is not sufficiently justified.

✓ *As a result of inspecting the Ministry of Internal Affairs of Georgia it was established that representatives of other state entities also have access to data contained in the unified information databank (on administrative offences). Written applications by state entities to the Ministry of Internal Affairs requesting access to the data in the unified information databank are not sufficiently justified. In addition, the documents do not clearly indicate the purpose and grounds for data processing. The Ministry was in-*

structed to apply appropriate organizational-technical measures through which the legal ground for granting access to other state institutions to the data of the unified information databank would become clear.

- ✓ *The State Inspector's Service reviewed access to data and registration of operations in relation to data contained in the electronic criminal case management system (so-called Crime Case) of the General Prosecutor's Office of Georgia. As a result of inspection, it has been found that the system registers every operation in relation to data contained in the system; however, the system does not clearly establish the duration of storing the data, that are also available in other databases and are used for the purposes of juvenile diversion. The General Prosecutor's Office was instructed to set specific term for which it would be necessary to store data for legitimate purposes identified by the Office (application of measures for juvenile diversion); it was also required to apply organizational–technical measures that would ensure that data is automatically deleted, destroyed and/or stored in a way that makes identification of a person impossible, after certain time passes.*

- ✓ *The State Inspector's Service reviewed lawfulness of processing personal data on cases of administrative offences in the unified information databank of the Ministry of Internal Affairs. As a result of inspection it was established that information on administrative offences is stored within the Ministry's database for unlimited term without a legal ground. It shall be noted that on 9 February 2017 the Constitutional Court of Georgia in its Judgment N1/2/622 declared the norm on permanent storage of information on administrative offences in the unified information databank in the electronic form unconstitutional (The Ministry was found administratively liable and was ordered to establish timelines for storing information on administrative violations in its unified information databank; it was also instructed to immediately delete, destroy or store in a way that makes identification of a person impossible, upon attaining respective goals).*

During the reporting period, several cases of usage of data registered in the databases of the Ministry of Internal Affairs without respective legal grounds, as well as cases of violation of rules set by law for data security were found. In one case an employee handed over his login and password for accessing the database to his coworker, who didn't have an access to Ministry's database; in another case, the Ministry passed on to the Service Agency of the Ministry of Internal Affairs information from its database about a criminal record of a person, when the Service Agency was deciding to issue him/her a driver's license however there was no need for disclosing/passing such information. In the abovementioned case, the State Inspector's Service found a violation of data

security requirements and imposed administrative sanction upon the Ministry. The State Inspector's Service also identified cases, where it was found that Ministry of Internal Affairs applied data security measures corresponding to legal requirements. For example, data processing through automatic audio and video recording equipment attached to a special uniform of the Ministry of Internal Affairs was found compliant with the requirements of the Law of Georgia on Personal Data protection.

3.4. RECOMMENDATIONS

The cases reviewed during the reporting period indicate that organisations processing personal data contained in electronic systems/databases continue to face following challenges: ensuring data security, controlling access to information, establishing clear timelines for data storage, deleting data or storing data in a way that makes identification of a person impossible after the expiration of term established by law; as well as awareness raising of employees.

Considering technological progress, it is indeed difficult to apply measures that would ensure absolute protection of personal data contained in an electronic system. However, data controllers shall reduce the risks of unlawful data processing to minimum. For this purpose, respective organisations shall:

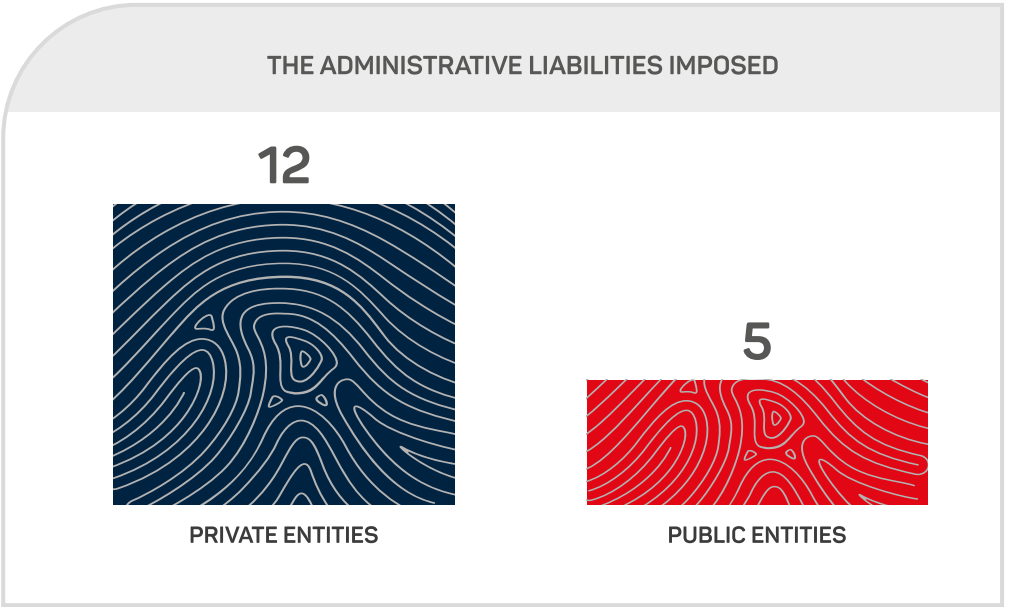
- Elaborate internal guidelines and policy documents with detailed regulations on data processing and security requirements;
- Grant access to databases solely to those individuals having need to access data for official purposes and having relevant authorization;
- Consider security measures (including measures for registering all operations in relation to data), including measures against unauthorized access to databases when forming databases;
- Proactively and regularly reveal instances of unauthorized access to databases;
- Establish clear and adequate measures of responsibility for their employees in cases of unauthorized access to data;
- Establish terms for storing data in databases and apply mechanisms for automatic deletion or depersonalization of data after the storage term elapses;
- Retrain their staff on processing and securing data contained in electronic systems.

4. DATA PROCESSING THROUGH VIDEO SURVEILLANCE SYSTEM

Organisations and citizens often resort to video surveillance systems in their daily lives. The usage of such systems serves different purposes.

Throughout 2019 based on citizen's applications, as well as on its own initiative, the State Inspector's Service reviewed 48 cases of data processing through video surveillance systems installed at the state entities, universities, shopping centers and stores, medical facilities, gyms and rehabilitation centers, restaurants, hotels and residential buildings. 9 cases dealt with data processing in public sector (including 4 by law enforcement authorities) and 39 cases – in a private sector.

17 facts of administrative violations have been established through inspections. 12 private entities and 5 public institutions were held administratively liable.



4.1. PRIVATE SECTOR

The use of any type of monitoring at a workplace is strictly limited both by Georgian legislation as well as by international practice.

Despite clearly established purposes set forth by the Law of Georgia on Video Surveillance, a practice of audio and video monitoring by private entities at the workplaces remains a challenge. The inspections of private companies revealed that use of video surveillance systems at the places of employment didn't serve purposes of ensuring personal security and protection of property, protection of secret information or testing/examining employees, as identified in the law.

As a result of inspections following violations were found:

- One of the companies used audio-video surveillance system to monitor employees' behavior at the workplace and the quality of services they rendered to their clients;
- One of the companies carried out audio-video monitoring of the workplace, as well as other spaces of common use (including kitchen and other rooms of common use). The company could not justify the use of monitoring systems at the offices, meeting rooms, training areas, in the rooms of the administration or the kitchen.
- Video surveillance cameras installed by one of the companies on its outer perimeter for purposes of security and protection of property recorded voices of by-passers.

Private companies note that the purpose of audio-video surveillance is to monitor quality of services and therefore, to improve the work of the company. This argument is unacceptable, as audio-video monitoring at a workplace automatically translates into direct control of all activities, including work-related or non-work-related talks (e.g. among co-workers). Companies can improve quality of their services through processing much less information (e.g. recording telephone calls directly with customers, use of the so-called "mystery-shoppers", etc.). Implementation of effective quality assurance mechanisms does not always require 24-hour audio-video surveillance of the workplace. Thus, processing much larger volumes of data on the employees than necessary by the companies, interferes with personal lives of employees and does not meet the requirements of the Law of Georgia on Personal Data Protection.

As the companies were not able to justify the use of audio-video surveillance, they carried administrative penalties and were required to stop audio-video monitoring.

During the reporting period, there were also few cases, when employers provided employees with written information about the video surveillance at a workplace, however, they didn't provide them with information on their rights enshrined in law (e.g. right to request rectification, renewal, addition, blocking, destroying of data).

4.2. NATURAL PERSONS

Natural persons install video surveillance systems at the residential buildings to ensure personal safety and protection of their property. This type of monitoring is allowed under the Law of Georgia on Personal Data Protection, however, it is important that a data controller (owner of a property) serves these purpose (ensuring personal safety and protection of property) in such a way, that co-owners of the property/or persons leaving in the same yard or the same building are able to use their property without being monitored and ensure the realization of their right to privacy without hindrance.

Throughout 2019 the State Inspector Service reviewed number of cases of use of video monitoring in residential buildings. The number of respective applications was especially high.

The inspections revealed, that natural persons fall short of complying with the requirements of the Law of Georgia on Personal Data Protection: they install video-surveillance systems without collecting written consents of more than half of the co-owners of the property; residents of the building are often unaware of video-monitoring; the monitoring encompasses not only one's own entrance and a common space, but also the entrances of apartments of other owners (without their written consent).

✓ *The State Inspector's Service looked into the lawfulness of data processing through a video surveillance system installed in one of the residential buildings. Through inspection it was identified that a person implementing video monitoring had installed 6 cameras in a residential building for the purposes of personal security and protection of property. In the absence of written consents of more than half of the neighbors, video cameras captured the public entrance of the building, the elevator, staircase of common use and the entrance to his/her private apartment.*

4.3. LAW ENFORCEMENT BODIES

In 2019 the State Inspector's Service reviewed legality of data processing through video-surveillance implemented by law enforcement bodies in cases, where violating the legislation on data processing ran into high risk of causing harm to a data subject. The State Inspector's Service reviewed lawfulness of processing data through video surveillance carried out at the temporary

detention isolators of the State Security Service of Georgia. In addition, 3 inspections were carried out to review the legality of data processing in the framework of policing and preventive measures as identified in the Law of Georgia on Police by the Ministry of Internal Affairs. The Service has studied the practice of the Ministry of Internal Affairs processing data in relation to administrative violations through automatic photo (radars) and video cameras ("smart" cameras) installed at the outer perimeter of the Ministry; as well as processing personal data through automatic photo/video equipment and portable/mobile speed cameras mounted on non-identifiable police vehicles (contactless patrolling system). As a result, it was found that:

- ✓ *At the stages of identification of an administrative violation and while imposing administrative sanctions, the Ministry processes large volumes of data in various forms (collecting, recording, printing photos, video-recording, storing and using) through automatic photo (radar) and video equipment ("smart camera") installed/mounted on the roads and on outer perimeters of buildings. When processing data, Ministry fell short of complying with data security requirements established by law. Namely, not all operations carried out in relation to electronic data were registered; at different stages of data processing no specific timelines for storing data were set and data was not automatically deleted after certain time had passed; in several cases it was identified that data obtained through various technical means had been double-stored. The Ministry was tasked to set specific timelines for storing information and to implement relevant organizational-technical measures to ensure automatic deleting or de-personalizing of data after established time passed and prevention of double storing of data.*

- ✓ *Identification of administrative violation and imposing an administrative penalty by contactless patrolling system is carried out through the use of various technical means and passing through several procedural steps. The latter inter alia includes: recording the fact, copying, processing, sending, uploading it in relevant software, etc. It was established that means used for data processing could not ensure protection of personal data from illegal processing (for example, in several cases there was no need to enter a username and password on specific technical equipment; the measures applying for data processing had not integrated the electronic registry for tracing all operations performed in relation to data; the deleting of data depended on the user of the technical equipment. The Ministry was tasked to implement data security requirements in practice).*

The State Inspector's Service has no revealed facts of illegal processing of personal data through automatic audio and video recording equipment (shoulder cameras) attached to the special uniform of the Ministry of Internal Affairs and through video surveillance carried out at the temporary detention isolators of the State Security Service of Georgia.

4.4. RECOMMENDATIONS

Cases examined during the reporting period indicate that the following challenges still persist: observing provisions of the law by natural persons when placing CCTV cameras in buildings; video surveillance of employees at private entities; taking relevant organizational-technical measures by law enforcement agencies in the course of video surveillance.

Given that video surveillance is a very intensive form of interference within the right to respect for private life, it is important that private/public entities as well as natural persons abide by the requirements of the law, in particular:

- In each case analyze purposes of audio-video surveillance and not use this form of data processing in cases when the purpose can be achieved through less intrusive means;
- Accurately assess existing needs and conduct video surveillance proportionate to the specific purpose and to a relevant extent;
- Pay special attention to video surveillance at workplace and use this means in cases of absolute necessity, for the specific purpose and on condition that the obligation foreseen by the law to inform employees in writing is properly implemented;
- Take all relevant organizational-technical measures, that, on the one hand will protect data from accidental or unlawful processing in any form and on the other hand, will assist in studying the circumstances of the incident in case of violation of the law.

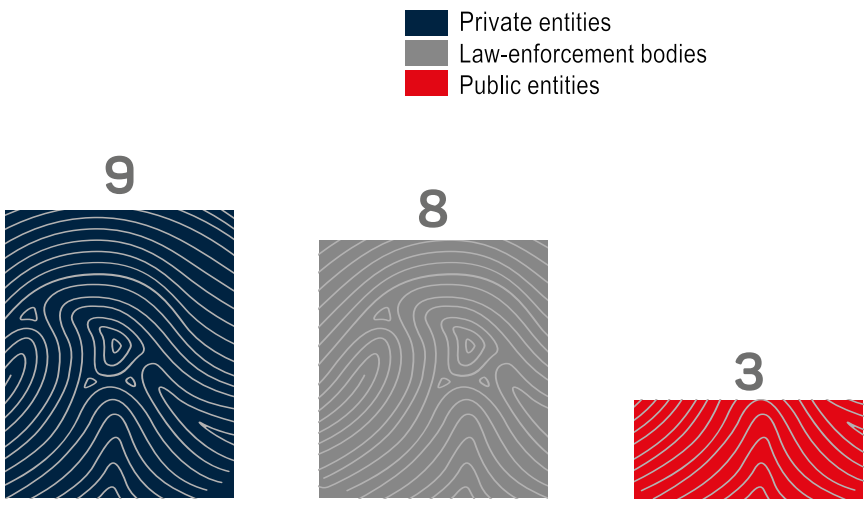
5. DISCLOSURE AND PUBLICATION OF INFORMATION

During the reporting period several facts of disclosing data or making it public by public and private organizations have become known. Making data publicly accessible significantly increases the intensity of infringement of privacy.

During the reporting period the State Inspector's Service looked into 46 cases of disclosure of personal data: 18 cases in the public sector (including 8 – by law enforcement bodies) and 28 cases in the private sector.

As a result of inquiry, 23 facts of administrative violations were established. In 9 cases administrative liability was imposed upon public entities, in 8 cases – upon private institutions and in 3 cases upon law enforcement bodies (several data controllers were imposed administrative liabilities for more than one violation).

DATA CONTROLLERS SUBJECT TO ADMINISTRATIVE LIABILITY



5.1. PRIVATE SECTOR

The instances of unlawfully disclosing personal data were identified in the private sector as well. Data controllers were found processing personal data they had collected during provision of services or other activities often without any legal grounds and needs.

- ✓ *One company published the personal identification document, bank account number and the information on bank transaction of one of its clients on social network – Facebook for informing other companies of his/her lack of good faith. The company was subject to administrative liability.*

- ✓ *One of the companies uploaded a record of its own video surveillance into the social network Facebook, which depicted illegal trespassing of an applicant from the gate through the yard. The video also indicated the full name of the person. The company indicated that the disclosure of applicant's personal data served its legitimate interest of protecting its property and security, revealing the possible fact of illegal trespassing on its property, and informing law enforcement bodies of the fact. The company was found administratively liable and was tasked to depersonalize the information published on the Facebook (including the video recording).*

One case concerned disclosure of a personal data of another person by a lawyer in the scope of his/her professional activity. Namely, it was identified that a defense attorney shared information on the victim of the same case on television; specifically, attorney revealed personal information of special category (the fact of being a victim in another criminal case). When reviewing the application, data controller could not provide relevant evidence to the fact that at the time of revealing personal data there were grounds for processing personal data of a victim (in accordance with Article 6 of the Law of Georgia on Personal Data Protection). Therefore, the lawyer was found responsible for unlawful disclosure of personal data and was subject to administrative punishment.

5.2. PUBLIC SECTOR

During the reporting period there were cases, when public entities sometimes intentionally, and other times through negligence (due to technical or human mistake) disclosed personal data in their possession.

We pay special attention to cases of publishing information on internet, which differs from other forms (e.g. print) of dissemination of information, as via internet the information becomes accessible to much wider population without any restriction.

Based on citizens' applications, two universities were inspected:

- *Ilia State University had made excel sheets with information on 190 MA students, including their results of exams, personal numbers, full names, mobile telephone numbers, year of study, scores, sex, legal address, etc., available through Google search engine. After applying "unhide" function the same excel file made information on additional 243 persons available. The publication of results of exams on the web-page of the University served the purpose of ensuring transparency of examination process and of meeting the legal requirement of publication of examination results. However, when implementing this obligation and processing data, the university failed to observe the requirements of data security. As a result, the university published more information and for longer period of time than it was necessary for reaching its legitimate purposes. The university carried administrative liability.*
- *Apolon Kutateladze Tbilisi State Academy of Arts published the list of 73 students with delayed payments to the University on its own Facebook page, in order to inform them of their due payment. As the Academy could not justify why it was necessary to publish information intended only for 73 students through means that made this information available to any person, the publication of data was considered unlawful and administrative liability was imposed upon the Academy.*

Based on citizens' applications and an information published on Facebook, the State Inspector's Service inspected one of the self-governance bodies. As a result, it was established that:

- *Mayor's office of Tianeti Municipality published on its Facebook page audio-video recording of the meeting of the conscription commission for the compulsory military service, which related to the issue of one conscript. The video reflected conscript's face, full name, content of his application to the Mayor's office requesting postponement of his military conscription and the fact that he had joined clergy. The State Inspector's service didn't share the position of the Mayor's Office, according to which the purpose of publication was to draw attention to the problematic issues related to military conscription process. The Mayor's Office could inform public and other entities of the deficiencies of relevant legislation and the ways of fixing loopholes without identification of the conscript. Respectively, the Mayor's Office was found administratively liable and was ordered to remove audio-video recording from its Facebook page.*

In addition to above-mentioned fact there have also been instances where the organisations had not intended to disclose data, however the documents containing personal data had become accessible to unauthorized third parties due to lack of observance of some technical and organizational measures. In one such case, "Agency for Public Communication Development" by mistake sent the press release of Tbilisi Mayor's Office together with identification documents of a citizen to the e-mail addresses of 71 media organizations. In a different case, in response to a request for public information, LEPL "Animal Monitoring Agency" submitted to one of the NGOs electronic case management materials in PDF format; Personal data contained in the documents were covered with the so-called black "blocks", however editing of the document was not restricted. Therefore, it was possible without any extra effort to remove the "blocks" and to uncover the personal data. In both cases data controllers were held administratively liable.

5.3. LAW ENFORCEMENT BODIES

It is of utmost importance to avoid any illegal disclosure/publication of data by law enforcement authorities, considering sensitivity of information available to them.

Law Enforcement bodies and their employees intentionally, or in some instances unintentionally (due to technical or human mistake) disclosed personal data available to them. The main problem in this respect has been the use of personal data contained in databases for non-official purposes (disclosure of information to third parties).

- ✓ *On the request of a third party and based on the license plate number of a vehicle, an employee of the Ministry of Internal Affairs searched for the full name and the registration number of the owner of the car in the dashboard computer installed in the patrol police vehicle and disclosed the information to third party (it shall be noted that prior to finalizing the State Inspector's Service's inquiry into the case, the General Inspection Service of the Ministry applied disciplinary measures against the employee of the Ministry).*

The State Inspection Service also reviewed a case of publishing personal data (including data of special category) of certain individuals on the internet.

- ✓ *The State Inspection Service on its own initiative inspected the Special Penitentiary Service, which had published personal data (including data of special category) of convicted persons in the social network. As a result, it was established that the Special*

Penitentiary Service had no legal grounds for processing personal data. Consequently, the data controller was found guilty of administrative offense and was ordered to de-personalize or remove respective personal information.

It shall be noted that in cases of disclosure of personal information law enforcement bodies often refer to the disclosure of personal information by a data subject and/or to the existence of important public interest.

According to the Law of Georgia on Personal Data Protection, both reasons are identified as lawful grounds for processing data. However, in each and every individual case law enforcement bodies shall be sure that the data subject has made data accessible. As for citing important public interest as a legitimate ground for disclosing data, the data controller shall accurately and closely assess whether publication of precisely the personal data in question serves the above interest, and whether making it accessible to public (based on its content) could be assessed as proportional to the legitimate interest of disclosure.

5.4. RECOMMENDATIONS

The reviewed cases demonstrate that data controllers most often cite the following reasons for disclosing data: high public interest, the need of informing public and the need to ensure quick and easy communication with them.

In order to prevent illegal disclosure/publication of personal data:

- In each and every case it shall be individually assessed whether disclosing data is necessary (not just easy) way and means of attaining the purpose;
- It shall be analyzed whether there is a proper balance between data subject's private life and the legitimate interest of disclosing data; sensitivity of respective information and sufficiency of public interest for disclosing it to any person shall be considered;
- The public and private entities shall raise awareness of their employees;
- Data controllers shall enhance organizational-technical measures for ensuring data security.

6. DATA PROCESSING IN THE HEALTHCARE SECTOR

According to the Law of Georgia on Personal Data Protection, information related to a person's health condition is considered a data of special category due to its high sensitivity. It is allowed to process this data only in exceptional cases and under strict observance of security measures.

Several public and private institutions obtain, store and use information on person's health. State institutions collect and use medical data for purposes of monitoring diseases and quality of medical services and for public health management purposes. In cases prescribed by law, law enforcement bodies also process health data. Private entities collect and use data while providing medical and insurance services to the citizens.

Throughout 2019 the State Inspector's Service examined 9 cases of processing health related data by private entities (5), public institutions (1) and law enforcement bodies (3).

According to Georgian legislation, data on patients together with material documents, are electronically registered and compiled in the "Electronic Health Registry (EHR)" of the Ministry of Internally Displaced Persons, Labor, Health and Social Affairs.

✓ *During the reporting period EHR was examined. Personal data of special category of patients are processed (collected and stored) in EHR. This data includes: personal number, date of birth, blood group and blood rhesus, information on previous illnesses and surgical interventions, pregnancy, patient's account of his/her medical history, chronic diseases, lab tests and vaccination. At the time of monitoring EHR contained data on 310 761 patients, to which 5 768 doctors had access with patient's consent. Despite certain technical measures that had been applied for ensuring data security in EHR system (including registering all operations in relation to the data; also, patient can see his/her personal data in the system and log data of processing; authorized users can access the system with their personalized username and password), The Ministry of IDPs, Labor, Health and Social Affairs was tasked to apply additional measures for ensuring data security, namely, to strengthen authentication mechanisms (measures applied for verifying users).*

As a rule, hospitals, clinics, labs, specialized centers, independent practitioners provide medical services to the citizens. When dealing with personal data of special category organizational and technical measures for data security are of utmost importance. The cases examined during the

reporting period indicate that in certain cases, organizational and technical measures applied by these institutions, fail to ensure effective data security and to trace an offender.

- *In one case citizens indicated that an employee of a medical facility had used and disclosed their and their minor child's personal data for non-work-related purposes. As a result of inspection, it was established that certain operations carried out in relation to electronic copies of medical files were not registered. This created the risk of illegal disclosure of information and made it impossible to identify the offender.*

The Law of Georgia on Personal Data Protection and legislation regulating health care system (The Law of Georgia "On Patient Rights" and the Law of Georgia "On Health Care") provide an exhaustive list of cases, when patient data can be shared with a third party. The same legislation also strictly obliges a person providing medical service to ensure confidentiality of patient information. All medical staff and every employee of a medical facility is obliged to protect medical privacy.

Despite abovementioned regulations, protection of patients' personal data by medical staff and preventing its third-party disclosure (including to the members of patient's family) is challenging in practice. The State Inspector's Service reviewed cases that concerned disclosure of HIV/AIDS status of a patient or his/her treatment by a psychiatrist to members of family. Disclosing such information on health condition can be very harmful to a data subject and may result in his/her stigmatization.

Data controller shall observe principle of confidentiality in relation to health data even in cases when such data is of high public interest.

- *In one of the cases examined by the State Inspector's Service, a complaint of several inmates from a penitentiary establishment, which among other issues concerned problems related to accessibility to healthcare services, was published by several media sources. The Special Penitentiary Service, structural unit of the Ministry of Justice of Georgia reacted to the complaint. The Penitentiary Service published a statement on social media. Among other issues, the statement publicly disclosed information on the health condition of respective inmates. The State Inspector's Service considered it to be a violation, as personal data of special category had been disclosed. The Special Penitentiary Service was asked to delete or depersonalize the statement.*

6.1. RECOMMENDATIONS

The cases examined during the reporting period demonstrate that despite strict legislative regulations on privacy of medical data, medical facilities and healthcare employees have limited understanding of its importance and of consequences that unlawful disclosure of medical data to unauthorized persons may have. Ensuring security of health-related data by data processing organizations is also problematic.

For ensuring security of health-related data, data controller shall:

- Set out regulations on disclosure of patient information to a third party which shall specify in detail the conditions of disclosing information, the circle of recipients, rules ensuring security and mechanisms for monitoring implementation of the regulation;
- Apply strict security measures in case of processing data in electronic systems;
- Keep complete and accurate registry of all operations in relation to electronic data;
- Only grant access to patent's medical files to those employees, who need to have it for performing their professional duties;
- Implement an effective system of monitoring over personal data processing.

7. PROCESSING PERSONAL DATA OF MINORS

Protecting best interest of a child is of particular importance for European Personal Data Protection legislation and practice. Some data protection regulations (GDPR) stress that children require special protection, as they may not have sufficient information on their rights, as well as risks and consequences that relate to processing of their personal data.

In order to ensure compliance of Georgian practice with international approaches and for better protection of children's rights, the State Inspector's Service monitored processing of children's personal data in various spheres. The cases that were examined were chosen on State Inspector's initiative or based on applications of interested parties. During the reporting period 13 cases of processing children's personal data were examined (12 – on data processing in public entities (including 3 - by law enforcement bodies) and1 in the private sector).

As a result, 9 cases of administrative violations have been revealed. 1 private and 6 public schools were imposed an administrative liability (some data controllers were imposed administrative liability for more than one offense). As for the law enforcement bodies, the facts of administrative violations have not been established in the examined cases, however in order to address some of the shortcomings, they were given certain tasks and recommendations.

In parallel with inspections and examination of applications, the State Inspector's Service also considered special regulations concerning minors in the draft law on personal data protection which has been initiated at the Parliament of Georgia.

7.1. PRIVATE AND PUBLIC SECTORS

Special responsibility for the protection of personal data of minors lays with those institutions and organizations which compile large volumes and especially sensitive data on children, such as schools (public and private).

The following violations have been revealed as a result of inspecting schools:

- In addition to the officially requested documents for enrollment in the school, one of the public schools additionally processed documents that contained personal data of children, but were not required by law;
- In one of the public schools, personal file containing special categories of personal data of hundreds of pupils was stored as an open document, at the workplace of a school administrator (to which other persons also had access). This created a risk of unlawful/accidental processing of data;
- The facts of unlawful video-monitoring were revealed in several schools (both public and private); namely this concerns monitoring of WCs. Video cameras didn't capture inside part of the cabins and monitored only the wash basin area and the corridors. The schools didn't consider those territories part of "hygiene facilities" and therefore didn't believe their actions constituted a violation of video monitoring rules. As the law declares it inadmissible to monitor hygiene facilities without any exceptions, the State Inspector's Service didn't share their justification, according to which the use of video cameras in the WCs served the purposes of children's safety and control of use of tobacco. A hygiene facility is a special private space. This space cannot be limited to only the inner parts of cabins. The entire WC facilities, including wash basin areas, corridors and the inner parts of cabins are used for hygiene purposes.

Therefore, right of person to use these facilities freely, without any monitoring, represents an important guarantee of inviolability of his/her privacy. Thus, monitoring a data subject in those facilities was considered inadmissible no matter what the justification would be;

- The administration of one of the private schools handed over their video surveillance records containing personal data of children to the police, without the latter having presented any legal basis for their request (court order, prosecutor's ruling);
- In one of the private schools the students were unaware of video monitoring; there were no warning signs displayed contrary to the requirements of law.

7.2. LAW ENFORCEMENT BODIES

The State Inspector's Service examined the processing of personal data of minors by law enforcement authorities.

The legality of processing children's personal data for the purposes of juvenile diversion by the General Prosecutor's Office was assessed because data used in the process of juvenile diversion represent a data of special category and its unlawful processing may pose danger.

✓ *As a result of inspection of the General prosecutor's Office it was established that the timeframe during which the personal data used for juvenile diversion can be stored is not specifically defined. The Prosecutors Office was tasked to define clear timelines.*

The State Inspector's Service also examined the legality of processing personal data of children under 3 years of age, who are placed at the penitentiary establishments with their mothers by the penitentiary service.

✓ *As a result of inspection, it was established that when a convicted mother of a child under 3 years requests that the child is placed with her in the penitentiary establishment, relevant procedures require processing of a child's personal data, including special categories of data. In most cases, mother's written consent serves as a ground for data processing, however this consent is not always comprehensive. It was also established, that there were no specific timelines identified during which it would be allowed to keep/store health data of a child staying with his/her mother. In order to protect best interest of a child and to prevent unlawful processing of child's personal data, the Penitentiary Service was recommended to design various forms of consent that would be signed by convicted mothers as their agreement to have personal data of their children processed.*

Disclosing personal data of children by the law enforcement authorities (in their press releases and briefings) remains a challenge. The majority of cases didn't concern disclosure of a juvenile's first and last names, but rather providing to wider public the data, that in its entirety, made identification of a child possible (child's age and exact location (village, region) where crime had been committed; displaying juvenile's clothes, etc.). The disclosure of personal data of a juvenile offender or a child victim can cause serious harm to him/her. Therefore, it is necessary that law enforcement authorities deal with the disclosure of children's personal data with utmost care.

7.3. RECOMMENDATIONS

The analysis of cases reviewed indicates that the children's personal data of different category is not always processed in line with legal requirements. The cases of data processing without legal grounds and/or in breach of data processing principles have been revealed.

In order to protect children's interests, it is necessary that public and private institutions:

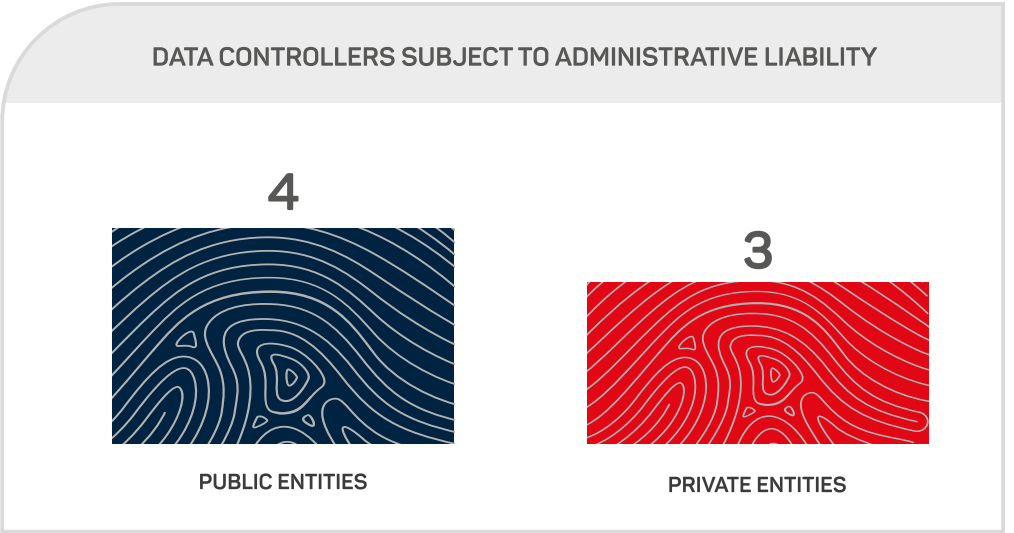
- Define rules that would regulate processing (including disclosure) of personal data of children;
- Process personal data of children only in the presence of clear and legitimate purpose and only in the volumes and during minimum time, required for attaining legitimate purpose;
- Apply all necessary organizational and technical measures to protect children's personal data from accidental or unlawful destroyed, alteration, disclosure, obtaining or any other unlawful use and from accidental or unlawful loss;
- Apply all necessary measures to ensure that a consent issued by a legal representative of a child to process child's personal data meets all relevant legal requirements.

8. DATA PROCESSING IN LABOR RELATIONS

Any public and private entity processes personal data of its employees. Before entering into labor relations, employer is entitled to obtain information that is necessary for assessing candidate's skills and his/her capability to handle the job. Considering specificity of work, the law allows to process candidate's personal data of even special category, such as his/her prior criminal record or health condition.

During the reporting period, the State Inspector's Service reviewed 10 cases of processing personal data in labor relations (5 cases concerned data processing in public sector and 5 cases – in private sector).

As a result of inspections 11 facts of administrative violation have been established. In 4 cases administrative liability was imposed upon public entities and in 3 cases – upon private institutions (Some data controllers were imposed administrative liability for committing more than one offense).



From cases reviewed in 2019, the case of processing personal data of candidates for the Supreme Court Judges submitted to the Parliament of Georgia is to be noted. Any information on candidates proposed for life-time appointment at the Supreme Court became a subject of high public interest.

✓ *As a result of inspection, it was established that the High Council of Justice reviews large volumes of information on the candidates and his/her family members (including professional reputation and activities of a candidate, information on any criminal/administrative or disciplinary charges against him/her in the past, verifies accuracy of information provided by a candidate). The High Council is entitled to contact candidate's references, his/her former employers and colleagues, administration and academic staff of the relevant education institution, as well as institutions, which might possess information about his/her prior criminal record, administrative or disciplinary charges, as well as his/her participation in administrative or disciplinary disputes.*

Considering the overwhelming public interest in ensuring that decent, qualified and honest candidates are chosen as judges, the State Inspector's Service concluded that purpose and the need of processing large volumes of data on candidates conformed to the Georgian legislation and served the purpose of assessing qualification and honesty of candidates.

Following types of violations have been identified in private and public sectors with regard to data processing in labor relations:

- In number of cases employee's data is made available to other colleagues, employees of other structural entities and/or to other persons, without any need;
- Digital systems that register employees' personal data do not have a function of registering all operations (including viewing/ scrolling of data) performed in relation to the data, which in the case of unlawful processing of personal data, makes it impossible to identify the offender;
- In addition, there are no differentiated levels of access to the electronic systems, in which employees' personal data are registered or the system is open to all users, regardless of their need and functions in the institution. We have also identified a case, where up to 250 employees all accessed the system using one username as they didn't have personalized user IDs. Thus, it was impossible to identify a person, who had performed any operation in relation to data;
- Audio-visual monitoring of employees is carried out in the workplace.

Audio-visual surveillance is a simple and effective way of monitoring employees. However, this form of personal data processing implies to be a harsh intervention in the employees' privacy.

✓ *The State Inspector's Service learnt about potentially illegal audio-video monitoring taking place in one of the insurance companies. As a result of inspection, it was established that the company monitored its employees with 40 cameras installed in the offices, in the kitchen and in the front-office where clients were served. Audio monitoring in the front office served the purpose of monitoring quality of customer services and assessing the content of communication with customers. This action was not considered legal and the company was found administratively liable. The company was tasked to ensure that through its video monitoring system it processed personal data only in volumes that would be proportional to legitimate purpose of such exercise (safety and protection of property). The company complied with the requirements of the State Inspector's Service and ended its practice of audio-video monitoring without a legitimate purpose.*

Many private and public entities have an established practice of using corporate telephone numbers. According to relevant legislation, in such case, the organization is considered to be a customer, and therefore, organization is entitled to receive transcripts of calls made from/to corporate numbers from the mobile operator.

✓ *An employee of one of the Ministries (Ministry of Agriculture of the Autonomous Republic of Ajara) applied to the Ministry with the request to obtain a telephone transcript (calls and sms-s) on his corporate number from a mobile operator. The employee received his transcript not directly from the mobile operator, but from his employer (the Ministry).*

According to the case law of the European Court of Human Rights, the calls and the correspondence made while performing official duties constitute a personal data of an employee and fall under the protection of Article 8 (Right to Respect for Private Life) of the European Convention on Human Rights. Therefore, the employee should have received the transcript directly from the mobile operator and not through the Ministry. The Ministry was given a recommendation to put in place a procedure through which it would request transcripts of the corporate mobile phone numbers used by its employees.

During the reporting period we also have had a case when the employer disclosed employee's personal data without the employee's consent.

✓ *The State Inspector's Service received an application of a citizen who stated, that the Casino, where he/she worked, had placed advertising photos on the banners in the city, which depicted the situation in the Casino and a close-up of his/her face.*

The company was unable to produce employee's consent to having his/her photo used for advertising purposes (which it was required to have under the law of Georgia on Personal Data Protection) and thus became a subject to administrative liability (It shall be noted that during the examination of this case, the company removed the photos of the employee from the banners).

8.1. RECOMMENDATIONS

The variety of cases examined in relation to personal data protection in labor relations confirms the relevance of this issue both in public and private sectors.

The interests of an employer and an employee may clash in the process of labor relations. Respectively, it is important to balance employee's right to private life / protection of personal data and the legitimate interests of an employer in order not to unreasonably restrict data subject's rights and, at the same time, protected interests of employers.

In order to have employees' personal data protected in the labor relations, public and private institutions shall:

- Only process the personal data that is necessary for its legitimate interests;
- Apply relevant organizational-technical measures;
- Limit the circle of persons having access to personal data of employees in line with its legitimate interests; The access shall be granted to those employees only, whose official duties include data processing;
- Assess whether processing personal data through audio-video monitoring serves lawful interests and whether it is possible to attain same goal through other measures;
- Put in place a procedure for requesting transcripts for corporate mobile phone numbers used by their employees that would ensure that the employer has no access to transcript.

9. DATA PROCESSING FOR DIRECT MARKETING PURPOSES

According to the law of Georgia on Personal Data Protection direct marketing refers to offering goods, services, employment or temporary jobs by mail, telephone calls, e-mail or other means of telecommunication.

9.1. OBTAINING DATA

According to the Law of Georgia on Personal Data Protection, the following data may be processed for direct marketing purposes: name (names), address, telephone number, e-mail address, fax number. Any other data may be processed on the basis of a written consent given by a data subject as determined by the Law.

Judging from the applications and complaints filed with the State Inspector's Service, during the reporting period citizens were interested in what were the sources of their personal data that the

companies used for direct marketing purposes, when, according to them, they had no relations of any kind with those companies.

When processing data, companies shall take all measures to establish proper mechanisms for registering sources of data and for providing this information to data subjects. This way, the rights of data subjects as guaranteed by the Law of Georgia on Personal Data Protection, would be upheld.

Through inquiry it was established that:

- Companies process data for direct marketing purposes that they have no right to process without a written consent of a data subject. Namely, they filter potential recipients of their messages using various criteria, including field of activity. They identify interest groups and offer their goods/services by SMSs.
- The companies do not register the sources of data they use for direct marketing purposes and thus, they are unable to provide this information to a data subject.

9.2. DATA PROCESSING BY A DATA PROCESSOR

The practice is that companies mainly send their offers through intermediary companies. According to the Law of Georgia on Data Protection, intermediary companies are authorized to process data, but they may process data only on the basis of relevant legal act or a written contract and only within a scope identified by the legal act or the contract.

Through the inspection it was identified that intermediary companies send advertising and informational messages not only to the telephone numbers handed over to them by the companies (which is stated in the contract between them), but to other numbers as well, despite the fact that the data processor is obliged to strictly and closely adhere to the instructions of the company, including the list of recipients of messages.

9.3. MECHANISM OF WITHDRAWAL

With each offer, a data controller is obliged to inform a data subject of his/her right to request at any time that a data controller stop using his/her data for direct marketing purposes. Data controller shall also establish accessible and adequate mechanisms for implementation of this right. The advertising message shall contain a clear reference to this right and to the mechanisms of its application.

During the reporting period, cases have been identified when such advertising messages didn't contain such a withdrawal mechanism, which is a violation of the Law of Georgia on Personal Data Protection. Respectively, the State Inspector's Service established the facts of administrative offenses.

In some instances, some data controllers considered advertising messages as informational and using this argument they tried to justified absence of withdrawal mechanism.

- ✓ *In response to one of the applications, the company argued that the SMS was of informational nature, not advertising. Therefore, it had not considered a mechanism to reject a message. Reviewing the content of the message, the State Inspector's Service did not share the arguments of the company and held it responsible for violating rules of direct marketing.*

In addition, a mere reference to a telephone number was not considered as accessible and adequate measure for requesting to stop usage of personal data for direct marketing purposes.

- ✓ *One of the companies had indicated a contact telephone number in its advertising SMS, however it was intended for contacting the company in case of interest in the offer. The message had not indicated that by calling that number a data subject could request to stop processing his/her personal data. The State Inspector's Service considered this fact as a violation.*

The State Inspector's Service also reviewed cases where the advertising SMSs contained a clear and effective mechanism for requesting to stop using personal data for direct marketing purposes, but the data processing was not discontinued for the reason of a data subject. In some cases, the data subject had no balance on his/her mobile phone to make a relevant call, while in some other cases, the mechanism was not properly used.

It shall be noted that employees of private institutions have no information on the procedures for personal data processing for direct marketing purposes and this often becomes the reason for a violation.

9.4. RECOMMENDATIONS

While processing personal data for direct marketing purposes public and private entities must:

- Register the sources of data (including in cases where data is obtained from publicly accessible sources) they use for direct marketing purposes;

- Obtain a written consent of a data subject in cases provided by law;
- Assess in every case whether a message is promotional or informational;
- When sending out promotional SMSs always include a rejection mechanism and/or establish other accessible and adequate measures for this purpose;
- Clearly and accurately describe the procedure for activating the rejection mechanism in the text of the message, to reduce risks of misusing it;
- In their contracts with processors prescribe the detailed obligations of processor; a processor on the other hand, shall ensure effective implementation of its contractual obligations;
- Ensure awareness-raising of staff on data processing procedures and on the rights of data subjects in this process.

10. PROCESSING BIOMETRIC DATA

The Law of Georgia on Personal Data Protection defines biometric data as any physical, mental, or behavioral feature which is unique and constant for each natural person and by which a person can be identified (fingerprint, footprint, iris, retina (retinal image), facial features).

According to legislation, it is only possible to process biometric data in exceptional cases, when processing such data is necessary to perform activities (except for public entities), for human security and property protection purposes, also to prevent disclosure of secret information, if these goals may not be reached by other means or if it would require disproportional efforts.

✓ *Based on an application the State Inspector's Service inspected a company, which processed biometric data (fingerprints) of customers of the gym at entry and exit. It was established that the company processed biometric data for the purposes of identification of its customers, and for prevention of entry by third parties and unauthorized use of company's services and facilities (this means that biometric data processing was used for the purposes of human security and protection of property). The company could not justify why it would be impossible to reach the same goal by processing lesser volumes of personal data. Therefore, the State Inspector's Service established a violation and ordered that the company stopped processing biometric data.*

It is to be noted that cases of processing biometric data in everyday life are increasing both in Georgian, as well as in international practice. Public and private entities are implementing number of new services, which can only be used through biometric data.

✓ *The JSC "Bank of Georgia" applied to the State Inspector's Service for a consultation. The bank wanted to introduce a face recognition system, through which the customer would be able to use the number of bank services (e.g. to withdraw money from ATM). The State Inspector's service examined the proposal, assessed its compatibility with existing legislation as well as organizational and technical measures applied and planned by the bank in order to ensure data security. Since the processing of biometric data (face) in the process of banking services would ensure a higher degree of security of banking operations and accurate identification of clients, it was assessed as compliant with the law.*

10.1. RECOMMENDATIONS

Biometric data is a unique and permanent data which does not change over time. Its unlawful disclosure may cause serious harm to the interests of a data subject. Thus, when processing biometric data, it is important to closely consider all circumstances for ensuring lawfulness of the process:

- Biometric data shall only be processed when it is necessary for reaching legitimate goals and when it is impossible to reach that goals by other means, or when it requires disproportional efforts;
- Specific and clear timelines shall be established for storing biometric data and after the time passes, data shall be automatically deleted (e.g. when an employer terminates data subject's access to a specific place, relevant biometric data used for accessing purposes shall be immediately deleted);
- It is important to define, establish and implement in practice organizational and technical measures for ensuring the security of biometric data (It is best international practice when a data controller has established clear and precise procedures for accessing data, registering data and for performing any other operations in relation to the data).

11. TRANSFER OF DATA TO OTHER STATES

The Order of the Personal Data Protection Inspector of 2014 defines a list of states (47 states) which have ensured proper guarantees for data protection. Therefore, it is allowed to transfer personal data to natural and legal persons of these states in the presence of legal grounds without consent by the State Inspector's Service. The list was compiled based on the assessment of data protection standards in respective countries (personal data protection legislation, activities of the supervising authorities, guarantees for human rights and freedoms). It is also possible to transfer personal data to other state or international organization, if it is foreseen by Georgia's international agreements and treaties.

Prior to transferring personal data to those states/international organizations, which fall short of ensuring data protection guarantees, respective entities are obliged to acquire permission of the State Inspector's Service.

During the reporting period the State Inspector's Service examined 14 applications for transfer of data. In 11 cases, the applications were filed by private entities, in one case – by a public entity and in 2 cases – by the branch offices of the international non-commercial legal entities. The applications concerned transfer of data to USA, Azerbaijan, Brazil and Turkey. Majority of cases concerned transfer of personal data of employees or clients to founding/donor organizations for reporting purposes, for assessing quality of services rendered, for providing consultancy and/or for using servers and software located in other countries.

In 9 cases permissions were granted; 4 applications were denied and 1 application remained unexamined as requested by the applicant (examination was terminated).

12. LEGISLATIVE DRAFTING ACTIVITIES

In 2019 the State Inspector's Service actively participated in the legislative drafting process.

12.1. DRAFT LAW ON PERSONAL DATA PROTECTION

The draft law on Personal Data Protection initiated in the Parliament of Georgia in 2019 was drafted by the State Inspector's Service. European experts participated in the law drafting.

The purpose of drafting the law was to approximate personal data protection legislation with European standards, implementation of Georgia's international obligations, introduction of internationally recognized principles and best practice, as well as addressing challenges revealed as a result of activities of the Service for the past several years.

In case Georgia develops a legislative base harmonized with the EU legislation, Georgia will have a chance to be "white-listed". This means that Georgian public entities, private organizations and physical persons would be able to circulate data within EU Member States, in the scope of different types of activities and for different purposes freely, without any prior examination[1].

It shall also be noted that upon the entry into force of the EU's new regulation on Data Protection (GDPR), a new principle of extraterritorial applicability has come into effect. According to this principle the scope of application of the regulation is extended not only to legal persons registered in the EU, but also to non-EU organizations offering goods or services to individuals in the EU. Respectively, for the Georgian companies that are active in the EU, it became especially important to operate based on legislation consolidated with that of the EU.

The draft law on Personal Date Protection initiated in the Parliament provides for number of important novelties. Specifically:

The rights of data subjects and guarantees for their protection are improved

- The right to receive information on data processing is extended. Organizations that process personal data will be required to provide the following information to data subject, in addition to information that is required by legislation in force: legal ground for data processing, data recipient, data transfer to another state, timelines for storing data, contact information of data protection officer, if applicable;
- The data subjects become entitled to be informed and to receive copies of personal data available at a private entity (according to legislation in force, this right extends to the data kept by public entities only);
- The data subject acquires a right to data portability/ data transfer (which means that the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller), with the right to refuse to be subject to profiling (which means that a data subject shall have the right not to be subject to

1 In addition to EUMS, the rules of free circulation of data also extend to Iceland, Norway, and Lichtenstein.

a decision based solely on automated processing, which produces legal or financial consequences for him/her or similarly significantly affects him/her);

- The draft contains more detailed mechanisms for regulating correction, renewal, completion, suspension of processing, deleting, destroying, blocking of data and issuing consent to data processing;
- If considering the category of data, its volume, data processing purposes, and means there is a high risk of human rights violation, the data controller becomes obliged to preliminarily assess the effect of data processing;
- When assessing the impact of data processing, the data controller becomes obliged to create a document that should describe: category of data, purposes of data processing, proportionality, process and grounds, assessment of possible risk of human rights violation and organizational-technical measures for ensuring data security;
- If data processing impact-assessment reveals a high risk of human rights violations, the data controller will be obliged to apply all necessary measures for mitigating risks (including having a consultation with the State Inspector's Service). If it is deemed impossible to mitigate risks of human rights violation through the application of additional organizational–technical measures, the data will not be processed.

The processing of the minors' data is improved

- The data concerning juvenile diversion is considered a data of special category and therefore it enjoys high standard of protection. Processing this data is only possible in cases specified in the law;
- The law specifically states that the supreme interest of a data controller cannot serve as a ground for data processing if supreme interests of a data subject (including children) is also present;
- The rule of issuing consent of a child to data processing and its conditions are an important novelty. The law grants this right to children from 14 years of age. At the same time the law specifies that during data processing the best interest of a child shall be considered and the consent shall be void if data processing threatens or harms child's rights;

- A special focus is made on the obligation to properly inform a child. Specifically, when information is obtained directly from a child, the data controller will be obliged to provide this information to him/her in a clear and plain language;
- Unlawful processing of a personal data of a child is considered as an aggravating circumstance, which would enable the State Inspector's Service to impose a harsher penalty in case of violation.

The rules of video surveillance are enhanced and audio-monitoring falls under a special legal regulation

- The grounds for the use of video surveillance are widened. Specifically, it becomes possible to apply this measure for the purposes of achieving public interest goals, however on a precondition that this would be adequate and proportional means for achieving the goal;
- When applying video surveillance, data controller becomes obliged to set forth in writing the purposes of video surveillance, its volume and duration, timelines of storing the record, rules and conditions for access, storage and destroying, as well as mechanisms for protecting data subject's rights;
- The standards for a warning sign on video monitoring are being established. Specifically, it shall bear relevant writing and/or a simple image about the ongoing video monitoring, as well as the name of a data controller;
- In addition to clock rooms and places of hygiene, video monitoring becomes inadmissible in the spaces, where a person has a reasonable expectation of privacy and where surveillance contradicts with established moral norms;
- A special article will regulate audio-monitoring establishing legal grounds for its application. At the same time, it becomes mandatory to warn a data subject of audio-monitoring prior to or immediately after the start of audio-monitoring.

Data processing rules for direct marketing purposes are being enhanced

- It becomes possible to process personal data for direct marketing purposes only with the consent of a data subject. In addition, processing data other than data subject's first name, last name, address, telephone number and an e-mail address requires a written consent of a data subject;

- Prior to obtaining data subject's consent and during engaging in direct marketing a data controller/ a data processor shall explain to the data subject his/her right to withdraw his/her consent at any time and the procedure to follow in a simple and plain language;
- A data controller/a data processor shall stop processing data for direct marketing purposes in a reasonable time, but no later than in 3 days after receiving relevant notification from a data subject;
- The mechanism for refusing data processing for direct marketing purposes shall be simple, clear and accessible;
- It becomes forbidden to request a fee or to establish other restrictions for withdrawal.

The draft law introduces a position of a personal data protection officer

- Public institutions (except for religious and political organizations), insurance companies, commercial banks, micro-finance organizations, credit offices, electronic communication companies, airlines, airports, and medical institutions that receive more than 10 000 patients a year, as well as data controllers/processors who process personal data of large number of data subjects or who carry out large-scale or systematic monitoring of their performance, become obliged to appoint or designate a personal data protection officer;
- Data protection officer shall have following responsibilities: to analyze applications and complaints related to data processing and to react to them within the scope of his/her mandate; to represent a data controller or a data processor in their relations with the State Inspector's Service; to ensure provision of data and documentation requested by the State Inspector's Service; to coordinate and monitor implementation of the requirements of the State Inspector's Service; in case of data subject's request, to provide information to him/her about data processing and his/her rights; to perform other important duties;
- The personal data protection officer shall possess sufficient knowledge in the field of data protection. He/she will enjoy relevant guarantees of independence in his/her activities and will be involved in making important decisions concerning personal data processing.

The responsibility for unlawful data processing is made stricter

The draft law provides for number of provisions concerning processing of cases by the State Inspector's Service. On one hand, they aim to establish necessary mechanisms for ensuring effective supervision over personal data protection and on the other – they aim to consider the interests

of data controllers and data processors. The proposed amendments will allow the State Inspector's Service to react to much more cases of unlawful processing of personal data and to more effectively implement its mandate:

- The draft law provides for specific aggravating and mitigating circumstances of administrative violations in the sphere of personal data processing;
- The statute of limitations for applying administrative penalties is being extended from 2 months to a year;
- In line with international standards, the administrative fines for violating personal data protection regulations are being raised which serves a purpose of prevention;
- The adoption of the draft law will significantly improve the situation with regard to protection of personal data in Georgia.

12.2. LEGAL EXPERTISE

Based on the requests of various institutions, the State Inspector's Service provided its legal opinion on 33 legislative packages, incorporating over 70 draft laws and by-laws. The reviewed legislative drafts mainly related to social, education, financial, taxation, money laundering, public security, trade and competition, and state procurement sectors.

The proposed draft laws and their explanatory notes, as a rule, did not contain justification as to why it was necessary to process personal data; why could the purpose not be achieved by means other than personal data processing or by depersonalizing data.

The proposed formulations were often general and too broad – the drafters made reference to the need of data processing for the purposes of "implementing the mandate granted by law". Considering a wide scope of powers/mandate of some public entities, such vague formulation of norms creates risk of using personal data for purposes other than those, originally defined and of processing disproportional volumes of data. Therefore, it was recommended that draft laws provided for specific purposes for data processing and that they indicated the need and the necessity of data processing, in order to avoid broad interpretation of those articles/norms.

The fulfillment of the recommendations and conclusion of the State Inspector's Service aimed at addressing shortcomings and limitations of the proposed draft laws, ensures establishment of high standard of personal data protection.

13. CONCLUSIONS

In parallel with activities carried out to monitor the lawfulness of personal data processing, the State Inspector's Service has also requested information from private and public entities on the measures applied by them for personal data protection purposes.

The information supplied by entities/organizations as well as the activities carried out by the State Inspector's Service revealed the following challenges:

- Proper realization of data subject's rights – providing him/her with information on his/her rights in a comprehensive, timely, clear and simple manner; ensuring fair balance between the interests of a data subject and other legitimate interests; restricting data subject's right to information without legal grounds;
- Lawful processing of data in electronic systems – insufficiency of organizational and technical measures applied for ensuring data security; unauthorized access to databases and use of personal data for non-official purposes; lack of established timelines for storing data in the databases and non-existence of mechanisms for automatically deleting or maintaining data in depersonalized form after expiration of defined terms;
- Audio-video monitoring through video surveillance systems in accordance with established legal requirements – violation of legal requirements when installing video monitoring systems at the residential buildings; audio-video monitoring of employees of private companies without relevant legal grounds; insufficient organizational-technical measures for ensuring security of data obtained through video monitoring;
- Protection of personal data of children – collection of more data than necessary on children; insufficient protection of documents containing personal data of children; disclosure of personal data of children;
- Protection of health data – insufficiency of measures for ensuring security of personal data collected and stored in the healthcare sphere by relevant data processing organizations; disclosure of information on patient's health condition by doctors and medical staff;
- Disclosure/ publication of personal data against legal requirements;
- Lawful processing of data in labor relations – disclosure of personal data of employees to third parties; unauthorized access to employees' personal data; audio-video monitoring at the workplace (in the offices);

- Lawful processing of personal data for direct marketing purposes – obtaining and use of personal data without data subject's written consent; inadequate assessment of the content of the message; failure to indicate how to reject data processing in the message and/or providing vague instructions;
- Insufficient effort by data controllers for raising qualification of their staff (the absolute majority of organizations have not carried out any training in personal data protection throughout 2019);
- Inefficiency of internal monitoring mechanisms of employees in public and private institutions (almost none of the organisations look proactively into data processing procedures);
- Low public awareness;
- Adoption of the law of Georgia on Personal Data Protection by the Parliament of Georgia.

MONITORING OF THE COVERT INVESTIGATIVE ACTIONS AND THE ACTIVITIES CARRIED OUT AT THE CENTRAL DATABANK OF THE ELECTRONIC COMMUNICATION IDENTIFICATION DATA

V. MONITORING OF THE COVERT INVESTIGATIVE ACTIONS AND THE ACTIVITIES CARRIED OUT AT THE CENTRAL DATABANK OF THE ELECTRONIC COMMUNICATION IDENTIFICATION DATA

1. GENERAL OVERVIEW

One of the functions of the State Inspector's Service is to control the covert investigative actions and activities carried out in the central databank of electronic communication identification data.

The State Inspector Service ensures 24-hour monitoring over investigative actions prescribed in articles 136-138 of the Criminal Procedure Code of Georgia, as well as over covert investigative actions set out in article 143[1].

- Requesting a document or information (Article 136);
- Real time collection of internet traffic data (Article 137);
- Obtaining content data (Article 138);
- Telephone tapping and covert recording of telephone communication (Article 143[1], Section 1, sub-section 'a');
- Removal and recording of information from a communications channel (by connecting to the communication facilities, computer networks, line communications and station devices), computer system (both directly and remotely) and installation of respective software in the computer system for this purpose (Article 143[1], Section 1, sub-section 'b');
- Real-time detection of geo-location (Article 143[1], Section 1, sub-section 'c'; shall enter into force on 30 March 2002);
- Monitoring of post and telegraphic communications (except for a diplomatic post) (Article 143[1], Section 1, sub-section 'd');
- Covert video and/or audio recording, photo shooting (Article 143[1], Section 1, sub-section 'e');

- Electronic surveillance through technical means, which do not endanger human life, health or the environment (Article 143[1], Section 1, sub-section 'f').

The central databank of electronic communication identification data is a database of the LEPL Operative Technical Agency of Georgia, in which electronic communication identification data obtained from various electronic communication companies are collected (specifically data that identifies: a consumer, trace of source of communication, recipient of communication, date, time and duration of communication, type of communication). Electronic monitoring system allows the State Inspector Service to have a real-time access to activities carried out in the central databank and to establish whether the activities were based upon relevant legal grounds (court order/ prosecutor's ruling).

2. MONITORING OF THE COVERT INVESTIGATIVE ACTIONS

Throughout 2018 first instance courts have granted 2 273 motions for covert investigative actions; the number was 2 279 in 2019. It is evident that the total number of court orders relating to authorization of covert investigative actions provided for by Article 143[1] of the Criminal Procedure Code has practically remained the same.

Majority of court orders concerned wiretapping and covert recording of telephone communications. Throughout 2019 the State Inspector's Service has received 1 362 court orders about permitting, prolonging, recognizing as lawful, partially granting and rejecting requests for telephone tapping and recording of telephone communication (1 397 in 2018).

During the reporting period wiretapping of telephone communication was mainly applied in cases of the following crimes (articles) established by the Criminal Code of Georgia: 180 (Fraud), 223[1] (Membership of a criminal underworld, "Thief in law"), 108 (Murder), 260 (Illegal manufacturing, production, purchase, storage, transportation, transfer or sale of narcotics, their analogues, precursors or new psychoactive substances), 338 (Bribe-taking), 210 (Manufacturing, sale or use of forged credit cards or charge cards).

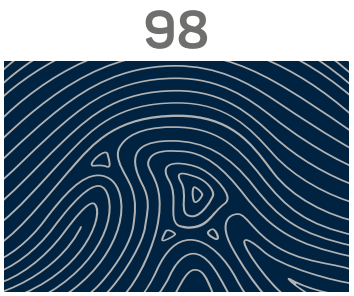
The State Inspector's Service is entitled to suspend an ongoing phone tapping of telephone communication in the following cases:

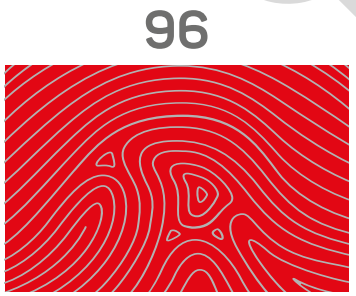
- It has not received an electronic copy of a judicial order permitting the investigative action;

- Within a deadline established by law, it has not received a paper copy of the judicial order authorizing the investigative action;
- It has not received an electronic copy of a prosecutor's ruling authorizing investigative action in case of urgent necessity;
- Within a deadline established by law, it has not received a paper copy of the prosecutor's ruling authorizing covert investigative actions in the case of urgent necessity;
- It is not supplied with requisites of a prosecutor's ruling through electronic system or on paper and/or its resolution section (ruling) is vague or inaccurate;
- Requisites of a prosecutor's ruling provided through electronic system differ from a hard (paper) copy of the prosecutor's ruing;

Throughout 2019 the State Inspector's Office has suspended 98 court orders/ prosecutor's rulings.

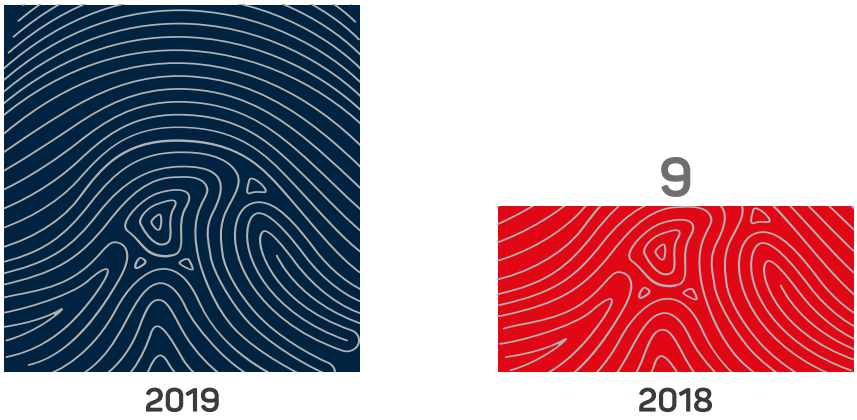
THE USE OF SUSPENSION MECHANISM BY THE STATE INSPECTOR'S SERVICE





In 2019 the State Inspector's Service reported 20 cases of ambiguity / inaccuracy in the court rulings to the relevant public bodies.

REPORTING OF AMBIGUITY/INACCURACY BY THE STATE INSPECTOR'S SERVICE



For effective enforcement of its monitoring powers granted by law in the area of covert investigative actions, the State Inspector's Service has carried out 10 inspections (6 – at the Operative Technical Agency; 2 – at the General Prosecutor's Office, 1 – at the State Security Service and 1 – at the Ministry of Internal Affairs of Georgia) based on citizen's applications, as well as on its own initiative. Among them, inspected activities included monitoring of lawfulness of data processing in cases of actions provided for in sub-sections "b" and "e" of article $143^{1}.1$ of the Criminal Procedure Code of Georgia (Namely, removal and recording of information from a communications channel (by connecting to the communication facilities, computer networks, line communications and station devices), computer system (both directly and remotely) and installation of respective software in the computer system for this purpose and Covert video and/or audio recording, photo shooting).

4 administrative offenses have been established as a result of inspections. The Operative-Technical Agency and the Prosecutor's Office have been held administratively liable. In addition, 11 requirements and 4 recommendations have been issued for eradication of shortcomings identified during the inspection.

3. MONITORING OF THE ACTIVITIES CARRIED OUT AT THE CENTRAL DATABANK OF THE ELECTRONIC COMMUNICATION IDENTIFICATION DATA

In 2019 data were processed at the central databank of electronic communication identification data on the basis of 81 court orders that is by 42% less than in 2018.

Throughout 2019 the State Inspector's Service without an interruption studied and analyzed information/documentation reflecting the provision of electronic communication identification data to law enforcement authorities by electronic communication companies as prescribed by Article 20 of the Law of Georgia on Personal Data Protection. In case of relevant grounds, it also reviewed lawfulness of transmitting data to law enforcement authorities by electronic communication companies.

Based on documentation/information analysis and inspections it was established, that electronic communication companies have significantly improved their practice of notifying the State Inspector's Service when transferring electronic communication identification data to the law enforcement authorities. It is noteworthy that throughout 2019 no incidents related to processing data without relevant legal grounds or in violation of data processing principles have been revealed.

It is also to be mentioned that the Constitutional Court of Georgia in its judgment No 1/1/650,699 of 27 January 2017 declared unconstitutional normative content of Article 136 of the Criminal Procedure Code of Georgia, according to which defendant was not entitled to file a motion with the court requesting a court order on a provision of document or information stored in a computer system or in a computer data carrier. Respectively, as of publication of the Constitutional Court Judgment on 27 January 2017, criminal defense party has become able to file relevant motions with the court. Due to this important legal development the State Inspector's Service examined the lawfulness of electronic communications identification data by electronic communication companies. Namely, 3 companies have been inspected to assess lawfulness of data processing carried out on the basis of court rulings issued on the motions filed by criminal defense party.

The cases of processing data without relevant legal grounds or in violation of data processing principles have been revealed, however, shortcomings in terms of observing in practice legal requirements for ensuring data security have been identified. Not all operations carried out in relation to data on the request of the defense party (in line with article 136 of the Criminal Procedure Code of Georgia) were registered, which increased the risk of accidental or unlawful processing of personal data. Therefore all 3 companies were found to have violated the law and became subject to administrative responsibility as defined by law. It should be noted that one of the companies eradicated

improper practices prior to finalization of the inspection. The other two companies were requested to address shortcomings identified in the course of inspection, which they did, within deadline set by the State Inspector's Service.

4. RECOMMENDATIONS

When carrying out covert investigative actions or investigative actions related to computer data, law enforcement authorities process personal data and significantly interfere in privacy of data subjects. Therefore, in order to ensure protection of the data subject's rights, it is of vital importance to closely observe requirements of the law. Besides, in order to effectively monitor covert investigative actions by the State Inspector's Service, it is necessary that all authorized bodies thoroughly adhere to their legal obligations:

- Common Courts, prosecution service, law enforcement bodies and electronic communication companies should provide the State Inspector's Service with full documentation/ information provided for by the Law of Georgia on Personal Data Protection and the Criminal Procedure Code of Georgia within deadlines established by the above legal acts; For ensuring security of data, LEPL Operative –Technical Agency of Georgia – legal entity with an exclusive authority to carry out covert investigative actions under article 143^1.1, sub-sections "a" and "d" – shall apply all necessary practical measures and technical solutions; this shall include registering all operations performed in relation to data collected through covert investigative actions and assigning unique identification numbers to technical means through which these operations are carried out;
- Electronic communication companies shall register all operations carried out with regard to data registered in relevant software, when transmitting electronic communication identification data to law enforcement authorities. In addition they shall make a full record of information concerning transfer of data to law enforcement bodies (which data had been disclosed, when and on which legal grounds).
- In case of delivering a ruling on termination of covert investigative actions, prosecutors of the General Prosecutor's Office should take all necessary measures to provide this information immediately to the relevant body (including Operative-Technical Agency);
- When transferring electronic communication identification data to the law enforcement bodies, the electronic communication companies should make a record of all the actions carried out in respect of the data registered in software tools for this purpose. At the same time, they should register rigorously the information related to the transfer of the data to the law enforcement bodies (which data was disclosed, to whom, when and what were the legal grounds).

INVESTIGATION OF CRIMES COMMITTED BY REPRESENTATIVE OF LAW ENFORCEMENT AUTHORITIES, AN OFFICIAL OR A PERSON EQUAL TO AN OFFICIAL

VI. INVESTIGATION OF CRIMES COMMITTED BY A REPRESENTATIVE OF LAW ENFORCEMENT AUTHORITIES, AN OFFICIAL OR A PERSON EQUAL TO AN OFFICIAL

1. GENERAL OVERVIEW

International organizations and independent experts for many years discussed the need of establishing an independent investigative mechanism in Georgia.

In his report – "Georgia in Transition", published in 2013, Thomas Hammarberg – the former High Commissioner for Human Rights of the Council of Europe and the former EU Special Adviser on Constitutional and Legal Reform and Human Rights in Georgia – noted lack of effective investigation of cases of torture and ill-treatment committed by law enforcement bodies and referred to the need of establishment of an independent investigative mechanism[1].

European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment also noted cases of impunity for ill-treatment in Georgia in its report of 2019 and called on the authorities to apply measures that would ensure investigation of alleged cases of ill-treatment in conformity with the standards established by the European Court of Human Rights[2].

An Independent human rights expert – Maggie Nicholson, in her assessment of 2017 of the implementation of 2014-2020 Human Rights National Strategy, called on establishment as a matter of priority of an independent investigation mechanism to look into cases of misconduct by law enforcement officers, stating that this would be the best indication of the government's commitment to fight impunity[3].

On 21 July 2018 Parliament of Georgia adopted the Law of Georgia on "State Inspector's Service". This law transformed the Personal Data Protection Service into the State Inspector's Service. In addition to previous functions, the Service became responsible for investigating specific crimes committed by a representative of a law enforcement body, an official or a person equal to an official.

1 Thomas Hammarberg, Georgia in Transition (September 2013)

2 Report to the Georgian Government on the visit to Georgia carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) published on 10 May 2019

3 Report of Progress in the Implementation of the National Strategy for the Protection of Human Rights in Georgia 2014-2020, and Recommendations as to Future Approaches by Maggie Nicholson.

The State Inspector's Service has been mandated to investigate crimes committed by a representative of a law enforcement body, an official or a person equal to an official as of 1 November 2019.

Relevant crimes committed after 1 November 2019 fall under the investigative jurisdiction of the State Inspector's Service.

2. ACTIVITIES CARRIED OUT BY THE SERVICE PRIOR TO ENACTMENT OF ITS NEW POWERS

ACTIVITIES CARRIED OUT BY THE SERVICE PRIOR TO ENACTMENT

- THE STRATEGY AND AN ACTION PLAN WERE DEVELOPED
- AMENDMENTS TO THE LAW OF GEORGIA ON "THE STATE INSPECTOR SERVICE" WERE ADOPTED
- THE STRUCTURE OF THE INVESTIGATIVE DEPARTMENT WAS DETERMINED
- THE OFFICES WERE EQUIPPED WITH COMPUTERS, OFFICE TECHNOLOGIES AND SURVEILLANCE SYSTEMS
- THE STAFF OF INVESTIGATIVE DEPARTMENT WAS RECRUITED THROUGH TRANSPARENT, MULTI-TIER SELECTION PROCESS
- MANUAL ON INVESTIGATIVE METHODOLOGY WAS DEVELOPED
- CODE OF ETHICS WAS DRAFTED
- THE RULES FOR DISCIPLINARY PROCEEDING WERE ELABORATED
- HOTLINE SERVICE WAS INTRODUCED
- INVESTIGATORS OF THE SERVICE WERE GRANTED ACCESS TO THE ELECTRONIC CRIMINAL CASE MANAGEMENT SYSTEM
- NEW LOGO WAS CREATED

2.1. DEVELOPING STRATEGY AND AN ACTION PLAN

For effective and unimpeded implementation of its mission and powers, in 2019 the State Inspector's Service developed a Strategy and an Acton Plan for 2020-2021 for its investigative functions with the support of the EU and the UN Office of High Commissioner for Human Rights (OHCHR).

Establishing a system for effective investigation of crimes falling under jurisdiction of the service was identified as a strategic goal of the Service.

For reaching the above strategic goal 4 main objectives were identified: institutional development, effective investigation, enhancing effectiveness and professionalism of employees, ensuring accountability and cooperation.

The Action Plan spells out in detail specific activities to be carried out under each strategic objective.

Strategic planning – a process directed at organizational development of the Service – ensures effectiveness, proper distribution of priorities and resources, internal coordination and result-oriented operations of the State Inspector's Service.

2.2. ADOPTED LEGISLATIVE AMENDMENTS

Expanding the mandate of the Service called for the need to develop legislative amendments and internal legal acts (by-laws).

Amendments to the Law of Georgia on "State Inspector's Service"

The State Inspector's Service worked closely with the Parliament of Georgia. As a result of coordinated work of the two institutions, on 20 September 2019, prior to enactment of a new mandate of the Service, the Parliament adopted amendments to the Law of Georgia on the State Inspector's Service, with respective package of amendments.

Following amendments have been introduced:

- Several categories of investigators have been defined for career development purposes: senior investigator of especially important cases, investigator of especially important cases, junior investigator and intern investigator;

- For the effectiveness of the Investigative Department, the positions of operative and forensic expert have been introduced;
- Selection criteria and transparent recruitment procedures have been established for management level positions at the Investigative Department, similar to those available for recruitment of investigators (qualification requirements, participation of criminal justice and human rights experts in the selection procedure);
- Additional barriers for recruitment of investigators at the State Inspector's Service have been removed for persons having worked in other spheres of criminal justice: persons having passed qualification exams for judges, prosecutors or a bar exam in the criminal justice field are exempt of the duty to pass a unified qualification exam at the Training Centre of Justice (having passed above qualification exams, they had demonstrated equivalent or higher qualification than what has been requested for passing unified qualification exam for candidates of investigators of the State Inspector's Service);
- The State Inspector was entitled to regulate the recruitment and the service for the employees of the Investigative Department and the General Inspectorate (Department) with its normative act different from the rules established by the Law of Georgia on Public Service. As a result, it has become possible to recruit employees of the Investigative Department and the General Inspectorate (Department) through a transparent competition in a limited period of time;
- A special metal badge and a uniform have been introduced for the employees of the State Inspector's Service since the service identification document was not considered sufficient for identifying a person authorized by a State Inspector;
- The circle of persons entitled to special state ranks has been broadened to include not only investigators of the State Inspector's Service, but also the Deputy State Inspector responsible for Investigations, operatives, forensic experts and the employees of the General Inspectorate (Department);
- In order to examine expediency of carrying out investigative or procedural actions restricting inviolability of private property, ownership or the right to privacy on the basis of a judicial order, corresponding deputy State Inspector may apply to the supervising prosecutor not later than 14 days prior to pre-trial hearing (instead of 20 days requested in the old version). Such application may be needed any time prior to pre-trial hearing (prior to submitting the case to court);
- The 20-day time limit before the pre-trial hearing for a Deputy State Inspector to apply to a supervising prosecutor for inclusion of specific evidence in the list of evidence submitted to

Court - was abolished. The above rule used to restrict deputy State Inspector for presenting his/her opinion concerning the inclusion of specific evidence obtained within final 20 days of pre-trial hearing in the list of evidence submitted to court.

Drafting Subordinate Normative Acts (by-laws)

Prior to enactment of investigative powers, the State Inspector's Service drafted amendments into 6 Governmental Decrees, as well as six proposals for amending legal acts of various entities.

In order to ensure conformity of by-laws with the law of Georgia on State Inspector's Service, 6 subordinate normative acts (Orders) of the State Inspector were issued:

1. *Approving Statute of the State Inspector's Service – which defined a new structure of the service and functions of its structural units (approved on 22/05/2019; it was subsequently amended three more times);*

2. *About the Rules of Service for the employees of the Investigative Department and the General Inspectorate (Department) of the State Inspector's Service, which defined: the rules of recruitment, service and conditions of the employees of the above two departments; types of disciplinary offenses by the employees of the Investigative Department and the General Inspectorate (Department), measures of disciplinary responsibility, rules of their application and lifting, as well as the rules of disciplinary proceedings (adopted on 26/09/2019);*

3. *Approving the Rule of Payment and Amount of Wages of Employees of the State Inspector's Service - which regulates issues related to payment of salaries of staff, including payment rules and amount of wages of officers with special ranks (adopted on 26/05/2019);*

4. *Approving the Emblem of the State Inspector's Service – which approved the emblem of the State Inspector Service (adopted on 18/10/2019);*

5. *Approving the Rules of Granting Special State Ranks to the Employees of the State Inspector's Service, which defines the rules for granting special ranks to the employees of the Service, as well as rules and conditions for depriving of the special ranks in accordance with the requirements of the Law of Georgia on Special State Ranks (adopted on 28/10/2019);*

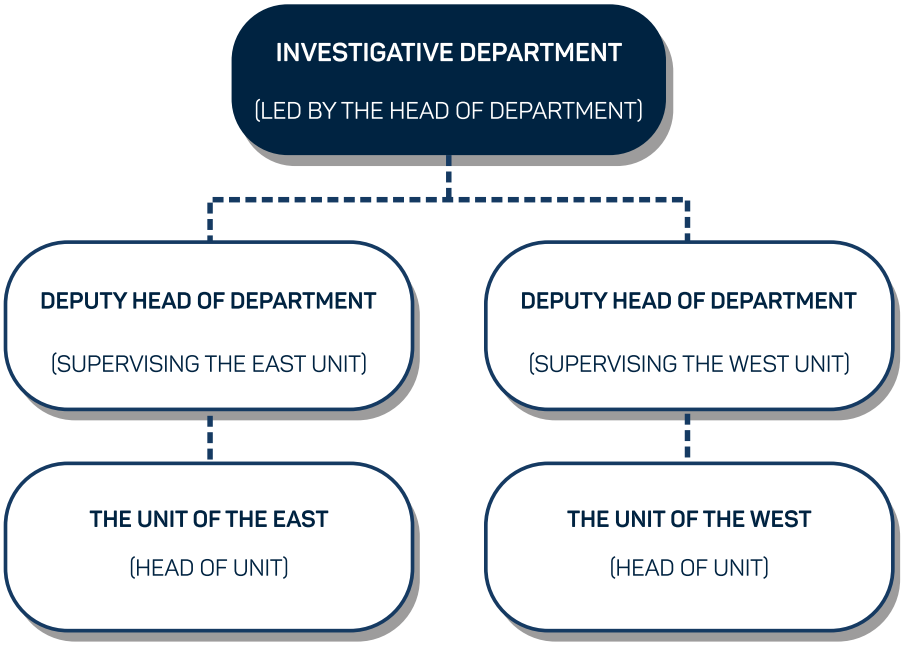
6. *Approving the Code of Ethics for the employees of the Investigative Department of the State Inspector's Service, which sets standards of conduct for the employees of the*

Investigative Department, including main principles of their conduct, issues related to their cooperation with colleagues, relations with the parties to criminal proceedings and the public, as well as issues of conflict of interest (adopted on 01/11/2019).

2.3. STRUCTURE AND OFFICES OF THE INVESTIGATIVE DEPARTMENT

The Investigative Department is made up of 2 Units – the East Unit and the West Unit. The East Unit investigates crimes committed on the territory of the Eastern Georgia; while the West Unit– deals with those, committed on the territory of the Western Georgia.

The East Unit is located in Tbilisi; the West Unit is located in Kutaisi.



The State Inspector's Service was technically / logistically ready to deal with the new investigative function when it came into force: network and server infrastructure are installed in both offices; the offices are equipped with computers and office equipment, video surveillance systems, software (internal case management system, criminal case management programme);

2.4. RECRUITMENT OF EMPLOYEES OF THE INVESTIGATIVE DEPARTMENT

The effectiveness of any service depends first and foremost on professionalism and qualification of employees. Proper selection and development of human resources is of critical importance.

The main challenge of the service in 2019 was to recruit employees who would ensure impartial and effective investigation of cases.

The qualification requirements, as well as legal and social guarantees of the investigators of the State Inspector's Service are defined by law. A citizen of Georgia with no previous record of criminal conviction, who has a higher legal education, has at least one-year experience of working as a judge, a prosecutor, an investigator or a lawyer, has appropriate business qualities and high moral reputation, a command of the language of proceedings and has passed the unified qualification examination at the Training Centre of Justice of Georgia in the following disciplines: Constitutional Law, International Human Rights Law, Criminal Law, Law of Criminal Procedure, Law on Corrections, and Principles of Operative-Technical Activities in Criminal Procedure, shall be appointed as the investigator of the State Inspector's Service. The candidates having passed judicial, prosecutorial or bar qualification examinations in general specialization or in the field of criminal law – are exempt of the duty to pass a unified qualification examination.

Prior to announcing a competition for the investigators and in line with the requirements of the law of Georgia on State Inspector's Service, the Training Centre of the Ministry of Justice administered 3 qualification examinations for the investigators of the State Inspector's Service. 135 candidates registered for the examination. The 75 participants successfully passed a 75% threshold. The registered candidates mainly came from the prosecution service, various investigative bodies and defense bar.

The investigators of the Investigative Department were selected through open and multi-staged competition. After screening of written applications, the candidates passed through written tests and an interview. In the process of recruitment of employees, candidates' education, qualification, work experience, professional skills, personal qualities and motivation were considered. In order to ensure openness and transparency of the competition, representatives of non-governmental organizations and academia participated in the work of the competition committee together with the representatives of the State Inspector's Service.

Up to 190 persons applied for the position of investigator. The competition committee selected 16 candidates for the position of investigator of especially important cases and 6 operatives. The candidates had different backgrounds. 2 of the investigators were former defense lawyers, 7 – had worked at the prosecutor's office, 5 – at the Ministry of Internal Affairs and 2 – at the Investigative Service of the Ministry of Finance.

6 Operatives and 2 forensic experts have also been recruited through a similar open and multi-staged competition. They support investigators in carrying out investigative and procedural actions.

The process of recruitment of employees of the Investigative Department was launched on 1 October 2019. Despite short deadlines and heavy workload, the service managed to successfully recruit investigators and attract professional human resources.

2.5. DEVELOPMENT OF MANUAL FOR INVESTIGATIVE METHODOLOGY

In order to ensure high quality investigations compliant with international standards and oriented at protection of human rights and freedoms, as well as the establishment of uniform investigative practices, the State Inspector's Service developed a manual on investigative methodology in co-operation with the EU and the OHCHR.

The manual is made for investigators of the service and it incorporates following issues: international regulations for effective investigations, qualification of crimes, standard for starting an investigation, specificities of investigative actions, rules of communication with parties to proceedings, cooperation between an investigator and a prosecutor, participation of a victim in the investigation process.

2.6. DEVELOPMENT OF ETHICS CODE AND RULES FOR DISCIPLINARY PROCEEDINGS

One of the aims of the State Inspector's Service is to fight official misconduct. Considering the types of crimes under the jurisdiction of the Service, this aim can only be achieved through abiding by high ethical standards by the employees.

Thus, the Service developed a Code of Ethics for the employees of the investigative department, which sets forth standards of conduct of employees, main principles of their activities – such as lawfulness, protection and respect of human rights and freedoms, political neutrality, impartiality, objectivity, fairness, professionalism, non-disclosure and confidentiality, protection of personal data. The Code also establishes standards for relations with colleagues, parties to criminal proceedings and the public.

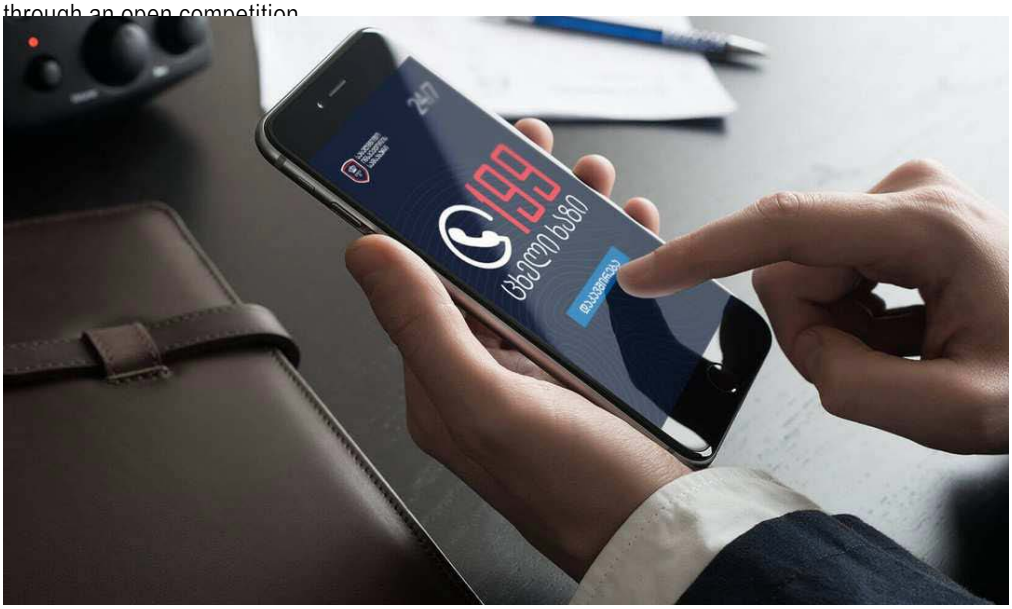
The Code of Ethics aims to establish norms to support fair, impartial, effective, comprehensive and professional investigations, as well as protection and respect of human rights and freedoms in the process of investigation.

In parallel with the Code of Ethics the rules for disciplinary proceedings have also been drafted. They define types of administrative misconduct, principles for selecting types of disciplinary measures, grounds for launching and timelines for disciplinary proceedings.

2.7. INTRODUCTION OF CRIME REPORTING MECHANISM ON POSSIBLE CRIMES

Prior to 1 November 2019, the State Inspector's Service with the support of the Ministry of Internal Affairs launched a mechanism for crime reporting on possible crimes without any delay from any point in Georgia – a 24-hour hotline (number - 199) and an electronic notifications management system (emergency assistance management system). The hotline operators were recruited

through an open competition.



The Hotline operator was assigned a cell phone number. The state institutions (for example, the temporary detention units, penitentiary service, etc.) send information on possible crimes via SMS to this number during 24 hours.

2.8. ENROLLMENT IN THE ELECTRONIC CRIMINAL CASE MANAGEMENT SYSTEM

Prior to enactment of an investigative mandate, with the assistance of the Prosecutor's Office of Georgia and the LEPL "Smartlogic" of the Ministry of Justice of Georgia, investigators of the State Inspector's Service became users of the Electronic Criminal Case Management System and underwent through respective training.

An Electronic Criminal Case Management System makes it possible to electronically process a criminal case (launching investigation, assigning number to a criminal case, carrying out and registering investigative/procedural actions).

All investigators of the Service (as well as the supervisor of investigations) have been issued individual usernames and passwords, granting them access to the system. Management level staff

of the Investigative Department and supervising prosecutors have access to criminal cases registered in the system (ensuring effective quality controls and speeding up communication between the investigator and the prosecutor, saving financial and human resources).

Besides, the Electronic Criminal Case Management System has a statistical module, which makes it possible to retrieve specific statistical data on criminal cases.

The State Inspector's Service is one of the first investigative entities, which started to operate within the updated version of the Electronic Criminal Case Management System.

2.9. CREATING A LOGO

A new logo of the Service was developed with the assistance of the EU and the OHCHR. The Logo was approved by the State Council of Heraldry. After assuming new functions, the Service presented itself to a public with this new logo.

The logo of the State Inspector Service is made up of three symbols:

- Iveria crown of state coat of arms – a historic symbol of united Georgian state, reflecting its strength and security;
- Protection shield – historic symbol denoting self-defence, internal balance and constant readiness;
- Support pole – a main founding symbol of European civilization, symbolizing sustainability, strength and a strong foundation;

The symbol in its entirety signifies the following: "Strong legal institution of a unified state".

3. INVESTIGATIONS

THE INVESTIGATIVE DEPARTMENT RECEIVED 351 NOTIFICATIONS

68 CRIMINAL INVESTIGATIONS WERE LAUNCHED

THE CRIMINAL CASES CONCERN 75 POSSIBLE VICTIMS

1190 INVESTIGATIVE AND PROCEDURAL ACTIONS WERE CARRIED OUT

718 PERSONS WERE INTERVIEWED

74 FORENSIC EXAMINATIONS WERE APOINTED

158 REQUESTS WERE FILED TO PUBLIC AND PRIVATE ENTITIES TO HAND OVER THEIR AUDIO/VIDEO RECORDINGS

148 MOTIONS WERE FILED IN THE COURT

INVESTIGATION WAS TERMINATED IN 8 CRIMINAL CASES

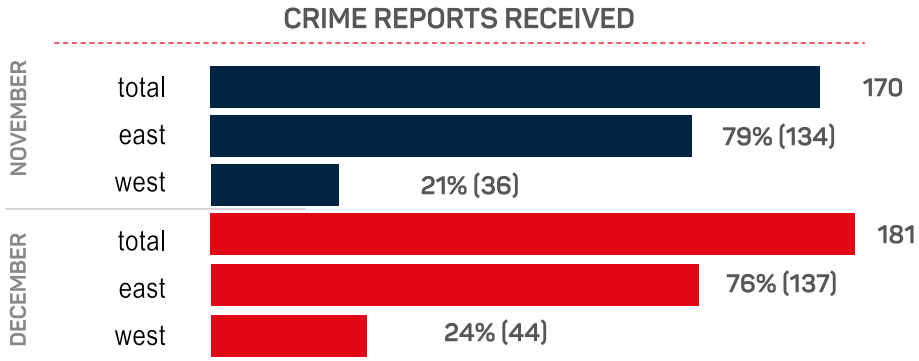
PROSECUTIONS WERE INITIATED AGAINST 1 PERSON

DEPUTY STATE INSPECTOR APPLIED TO THE GENERAL PROSECUTOR ' S OFFICE WITH 13 SUBSTANTIATED PROPOSALS

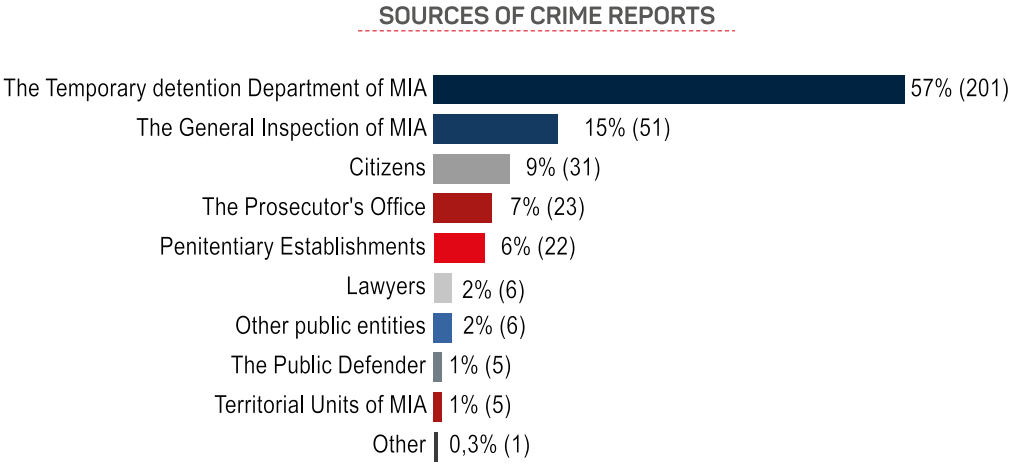
3.1. CRIME REPORTS RECEIVED

From 1 November 2019 (since gaining the investigative powers) to 31 December 2019 the Investigative Department of the State Inspector's Service received 351 crime reports (170 – in November and 181 – in December).79% of reports received in November were examined by the East Unit of the Investigative Department, and 21%, were dealt by the West Unit.

76% of reports received in December were examined by the East Unit of the Investigative Department, while 24% - were examined by the West Unit.



73% of reports were received from the Ministry of Internal Affairs; 9% - for the citizens; 7% - from the Prosecutor's Office; 6% - from the Ministry of Justice; 2% - from defense attorneys; 2% - from other public institutions; 1% - from the Public Defender's Office.



The Temporary Detention Department of the Ministry of Internal Affairs sends reports to the State Inspector's Service without any delay during 24 hours (by SMS). This information is transmitted to the Investigative Department by medical doctors, employed at the Temporary Detention Isolators, who carry out medical examination of persons detained for criminal or administrative violations. If there are no doctors employed at the detention isolators, the heads of the facilities send report.

The reports are sent when:

- A detainee has physical injuries and a doctor employed at the isolator suspects that he/she had been subject to torture or ill-treatment;
- A detainee has new marks/ traces of violence on his/her body;
- A detainee placed in isolator alleges violence against him/her from representatives of law enforcement bodies.

The General Inspectorateof the Ministry of Internal Affairs also submits crime reports on possible cases of violence and other crimes under jurisdiction of the State Inspector's Service, committed by the representatives of the Ministry during 24 hours. The Ministry of Internal Affairs obtains the information through its hotline (126) or citizen's applications.

The information about possible traces of violence on the bodies of inmates are provided to the State Inspector's Service by the doctors, employed at the Penitentiary facilities or by the General Inspectorate of the Ministry of Justice of Georgia.

The penitentiary establishments send reports when:

- The inmate has physical injuries and a doctor suspects that he/she had been subject to torture or ill-treatment;
- The detainee alleges violence against him/her from a representative of the law enforcement body (despite presence of any physical marks).

The penitentiary establishments of the Ministry of Justice also submit inmates' applications who allege possible acts of violence to the State Inspector's Service. The information on inmate's death is also provided to the State Inspector's Service immediately throughout 24 hours.

If in the process of investigation or prior to launching investigation during the interview with an inmate the General Inspectorate of the Ministry of Justice identifies features of crime falling under jurisdiction of the State Inspector's Service, it immediately submits the inmate's application and the case materials to the State Inspectors' Service.

The reports from the Prosecutor's Office of Georgia are mainly written (rarely provided through

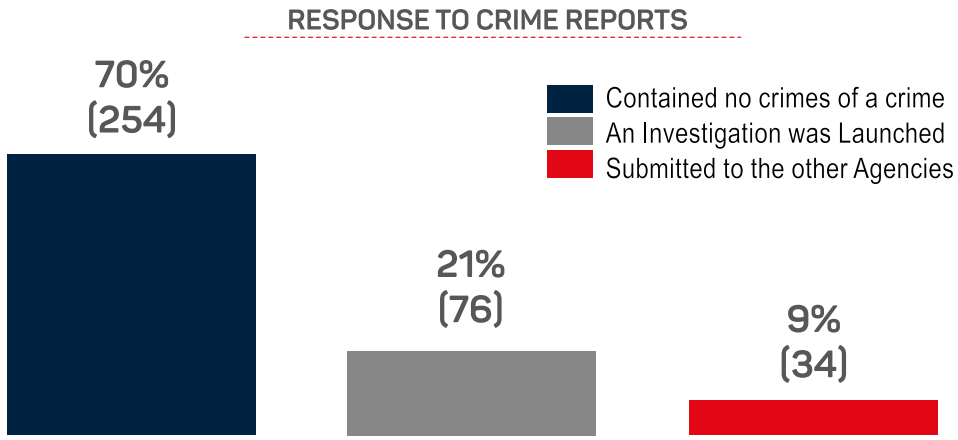
means of telecommunication). They concern the statements of defendants made during the first appearance, pre-trial hearing or during the trial, concerning signs of crimes falling under jurisdiction of the State Inspector's Service. The Prosecutor's Office also refers to the State Inspector's Service applications that concern possible crimes falling under the State Inspector's jurisdiction.

The court submits reports, if at any stage of a court hearing, a judge has a suspicion that a defendant might has been subjected to torture, ill-treatment, degrading or inhuman treatment or if a defendant claims he/she has been subject to such treatment. It shall be noted that these types of notifications from courts are rare. There has only been 1 such report from court in 2019. As it has been noted above, the notifications concerning defendants' claims about ill-treatment made at the court hearing are mainly communicated to the State Inspector's Service through the Prosecutor's Office.

3.2. LAUNCHING INVESTIGATION

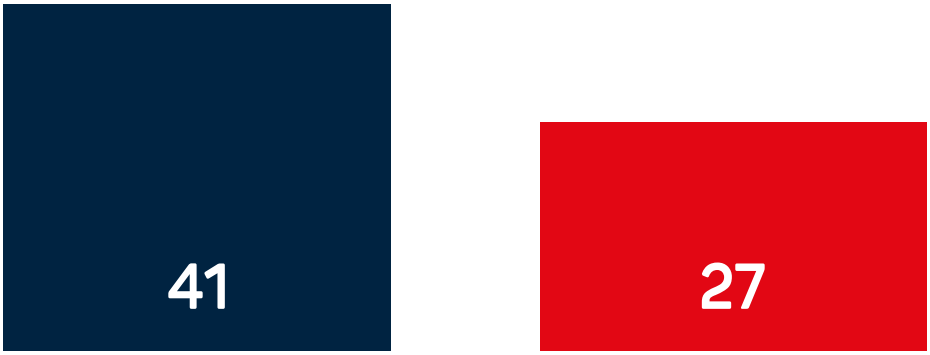
The 251 crime reports received throughout 2019 concerned 364 potential victims. Reports about 254 victims indicated no signs of crime. Investigation was launched into cases of 76 possible victims. 34 cases that concerned actions falling outside the mandate of the State Inspector's Service, were referred to other agencies.

In 2019, 68 criminal investigations were launched into cases concerning 75 possible victims (few cases concerned potential crimes committed against more than one person). The investigation on the case of 1 victim was launched in 2020 (the information on investigations carried out in 2020 will be reflected in subsequent reports).



In 2019 (from 1 November to 31 December 2019) the Investigative Department of the State Inspector's Service launched 68 criminal investigations: 41 cases were launched in November (35 of them were investigated by the East Unit; 6 – by the West Unit) and 27 – in December (23 of them in the East and 4 – in the West).

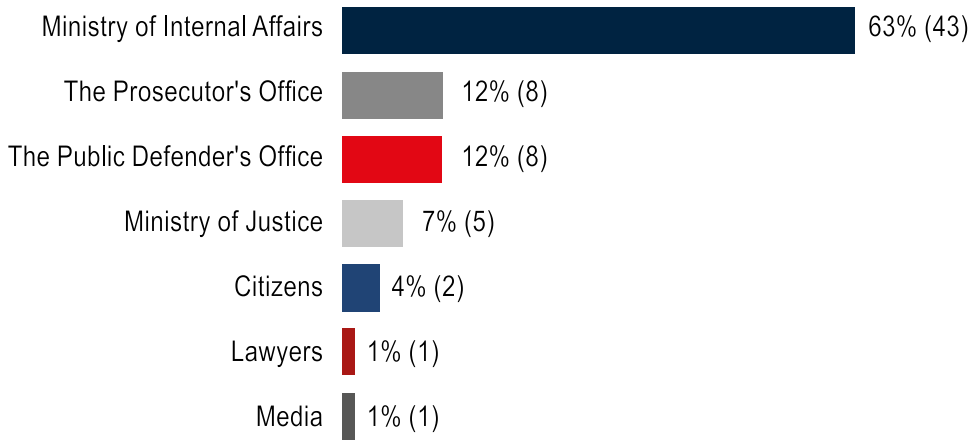
NUMBER OF LAUNCHED INVESTIGATIONS



In parallel with launching investigations, 2 criminal cases were transmitted from the Ministry of Internal Affairs to the Investigative Department of the State Inspector's Service by the decision of the General Prosecutor's Office. One of the cases was joined with another criminal case under investigation at the East Unit. In total the Investigative Department of the State Inspector's Service had 69 cases under investigation during November-December 2019.

63% of cases on which criminal investigations had been launched were based on reports received from the Ministry of Internal Affairs (Department for ensuring Temporary Detentions, General Inspectprate, territorial units); 12% - were based on the reports of the Prosecutor's Office; 12% - on the reports of the Public Defender's Office, 7% - on the reports of the Ministry of Justice, 4% - on the basis of the citizens' complaints, 1% - on the report filed by the defense lawyer and 1% - on the information provided by media.

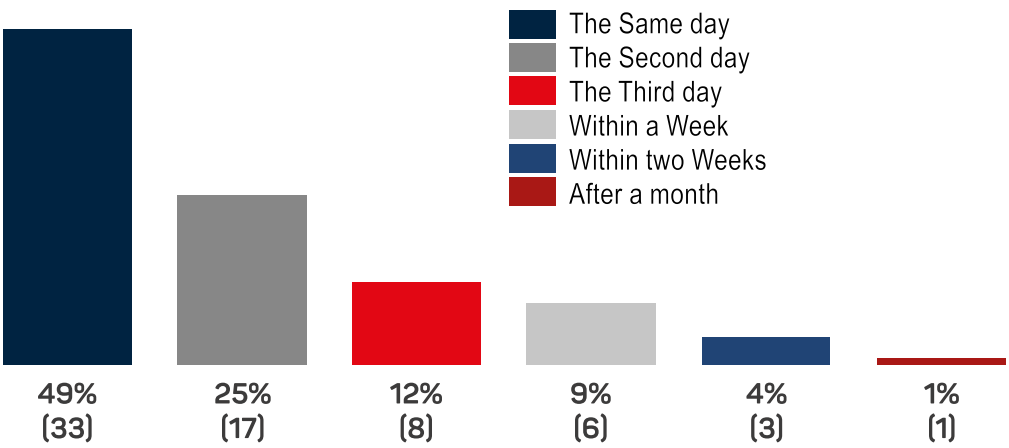
AUTHORS OF REPORTS INDICATING SINGS OF CRIME



Regrettably, some crime reports arrive not immediately after the alleged crime is committed but with a certain delay, which makes it impossible and/or significantly impedes collection of evidence and the establishment of factual circumstances.

In 68% of cases reports on possible crimes were received within 3 days, while in 14% of cases it took a week or longer to have crime reported. Reports with a week or a longer delay were submitted both by State institutions as well as the citizens.

THE TIME FROM THE COMMITMENT OF AN ALLEGED CRIME TO RECEIVING CRIME REPORT BY THE STATE INSPECTOR'S SERVICE



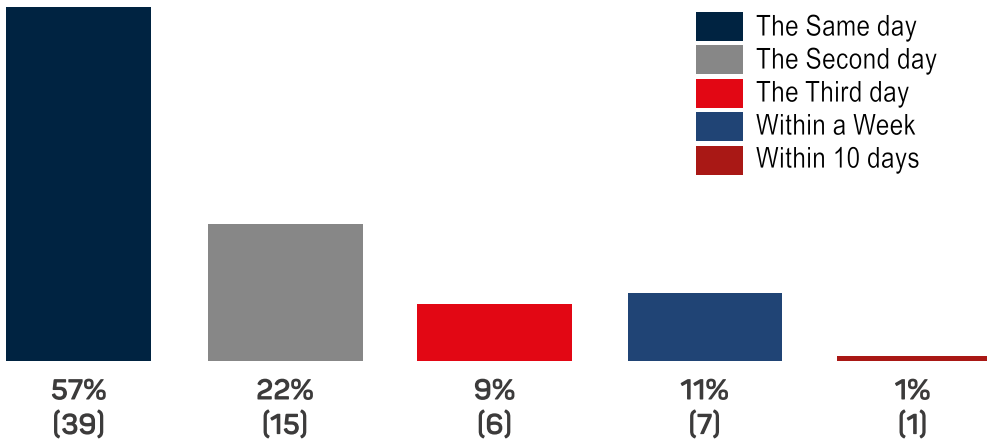
Timely response to crime reports, immediate launch of investigation and carrying out investigative actions in limited period of time are a key to effective investigation.

The State Inspector's Service launches investigation on the day it receives a report unless the report is unclear and it is impossible to start investigation without clarifying details with the applicant.

The State Inspector's Service launched investigations on the day it received respective report in 57% of cases; in 22% - investigations were launched on the second day; in 9% of cases – on the third day, on 11% of cases – within a week and in 1% of cases – in 10 days period.

The reasons for a week's and longer delay in launching investigation were the vagueness of facts/ circumstances indicated in the report and the fact that the applicant failed to timely report to the State Inspector's Service for clarifying content of a report in spite of numerous communications.

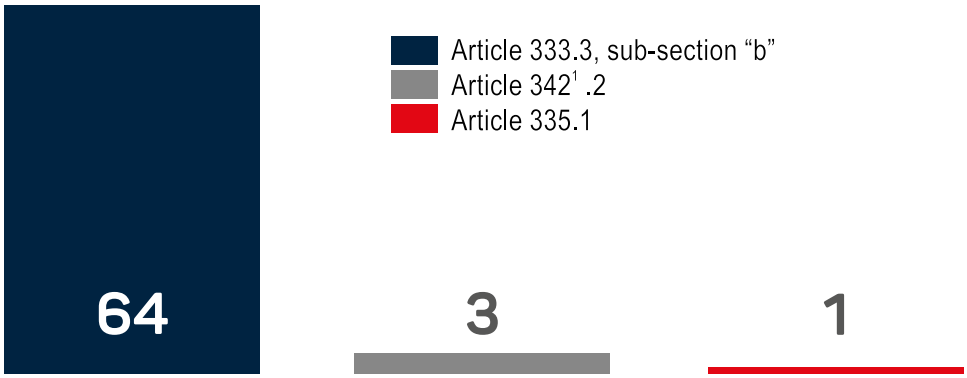
THE TIME OF LAUNCHING INVESTIGATION INTO REPORTS INDICATING SINGS OF CRIME



Due to a rather general content of crime reports in most cases it is difficult to properly identify qualification of the committed act at an early stage. Therefore, investigations mainly are launched on the basis of Article 333.3, sub-section "b" of the Criminal Code of Georgia (Exceeding official powers, committed with violence).

In 2019 the Investigative Department of the State Inspector's Service launched 64 criminal investigations on the basis of Article 333.3, sub-section "b" of the Criminal Code of Georgia (Exceeding official powers, committed with violence), 1 criminal investigation on the basis of Article 335 (Providing explanation, evidence or opinion under duress), and 3 criminal investigations – based on Article 342[1].2 (Violation by an employee or person equated to him/her of the internal regulations of the Special Penitentiary Service).

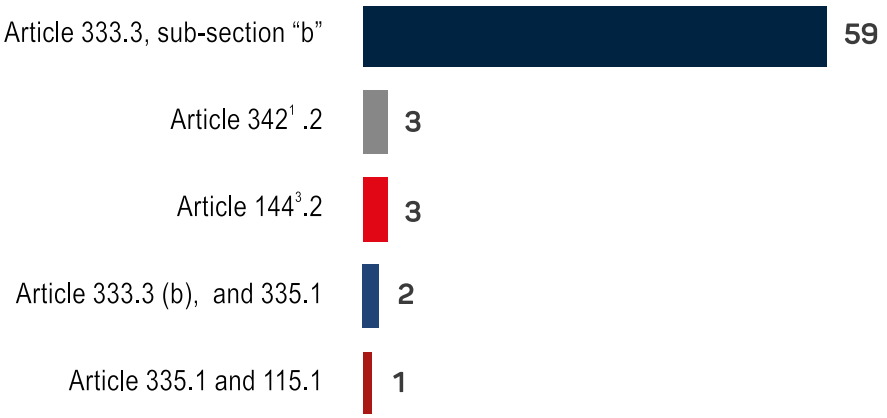
QUALIFICATION OF THE CRIMES IN THE BEGINNING OF THE INVESTIGATION



The qualification is often changed based on the interview with an applicant/ an alleged victim and the evidence obtained through other investigative actions. In the course of these actions, more precise qualification is chosen that better matches factual circumstances of the case.

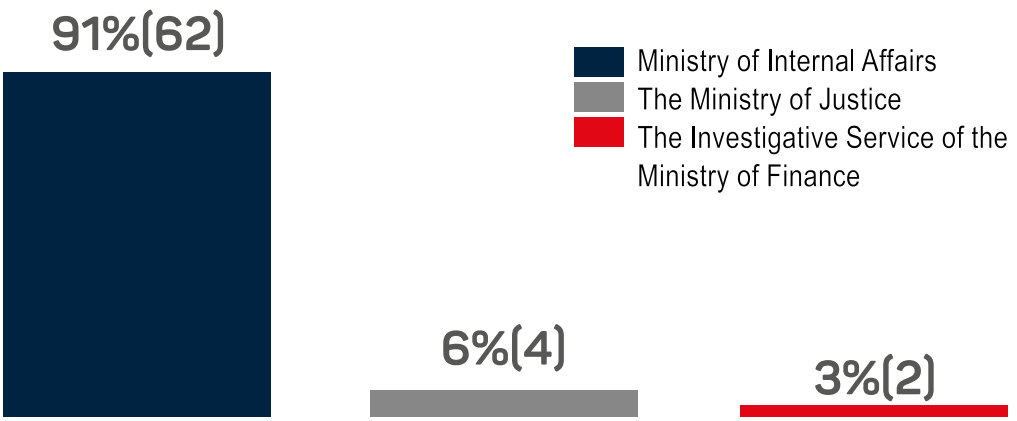
Out of cases launched on the basis of Article 333.3, sub-section "b" of the Criminal Code of Georgia (Exceeding official powers, committed with violence) criminal qualification of 3 cases was changed into Article 144[3] of the Criminal Code (Inhuman or degrading treatment); on 2 cases additional charges were pressed under Article 335.1 of the Criminal Code (Providing explanation, evidence or opinion under duress), 1 criminal case, into which investigation was launched under Article 335.1, was joined with another investigation referred from another investigative agency and the investigation continued under Articles 335.1 (Providing explanation, evidence or opinion under duress) and 115.1 (Incitement to Suicide).

QUALIFICATION OF CRIME DETERMINED IN THE COURSE OF INVESTIGATION



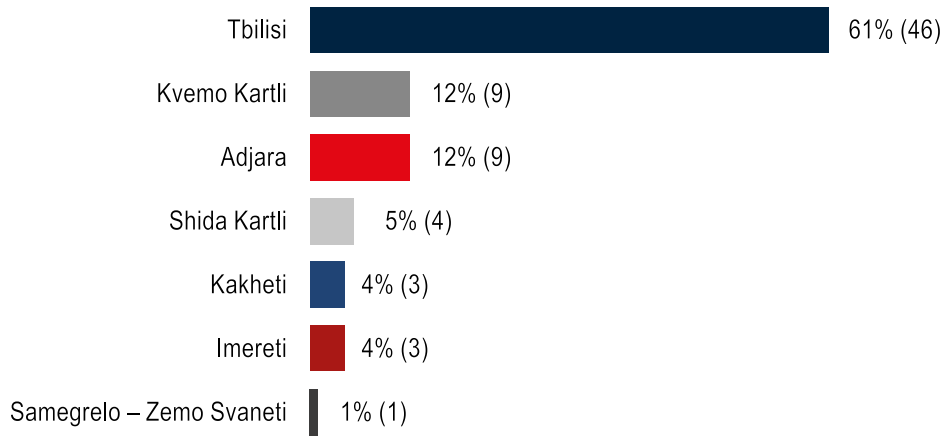
In 91% of cases, into which the State Inspector’s Service launched investigation, alleged victims identify employees of the Ministry of Internal Affairs as potential offenders; in 6% of cases – victims point at the employees of the Special Penitentiary Service of the Ministry of Justice and in 3% of cases – at the employees of the Investigative Service of the Ministry of Finance.

THE ENTITIES INDICATED BY POSSIBLE VICTIMS



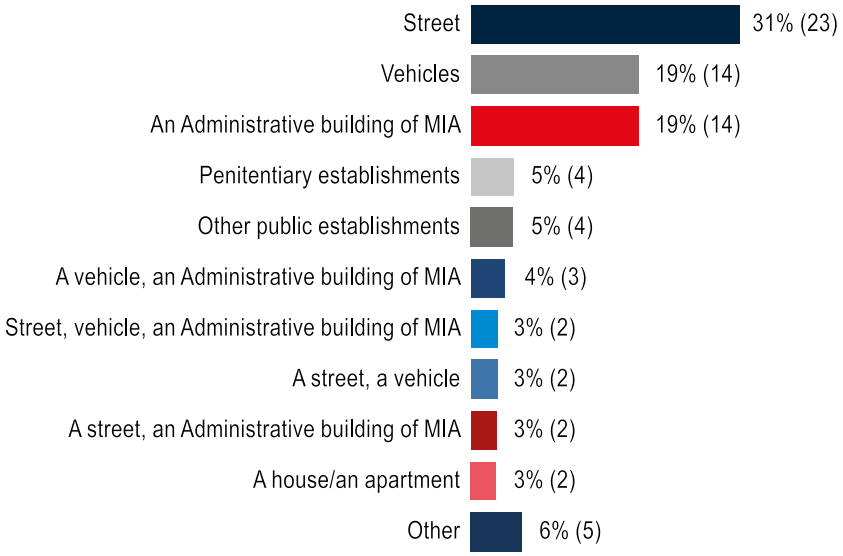
61% of victims identified Tbilisi as a place of alleged crime. Relatively high figures also identified Kvemo Kartli (12%) and Ajara (12%) as places of possible crimes.

GEOGRAPHIC AREA OF COMMISSION OF POSSIBLE CRIMES AS INDICATED BY VICTIMS



40% of victims stated that the alleged crime was committed in the street; 29% - identified a car as a place of crime; 29% - stated the alleged crime was committed at the administrative building of the Ministry of Internal Affairs; 5% - referred to penitentiary establishments, 5% - mentioned other public institutions; while 3% - stated it occurred in the house/apartment. In some cases, victims identified several places as places where alleged crime had been committed.

SPECIFIC PLACES OF ALLEGED CRIME AS INDICATED BY VICTIMS

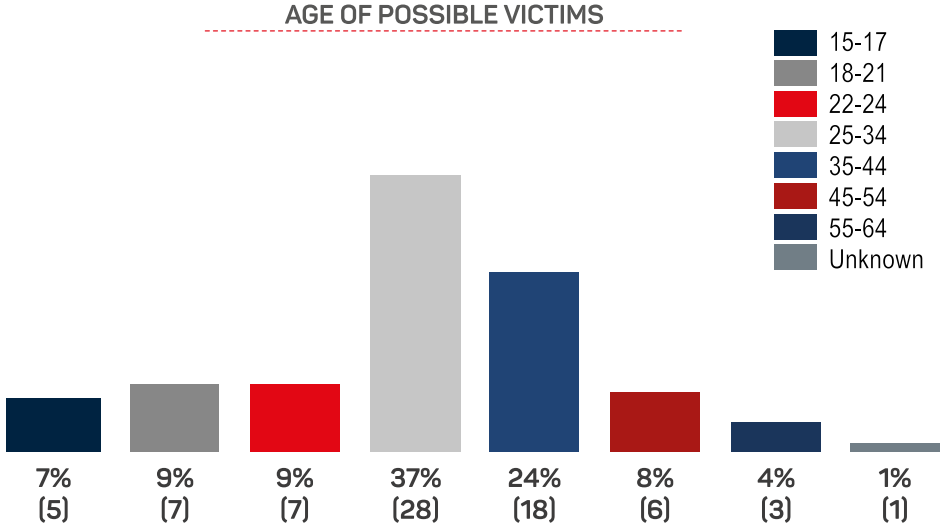


3.3. POSSIBLE VICTIMS

68 Criminal Cases launched in 2019 involved total number of 75 possible victims. Their absolute majority (96%) were males and 4% - were females.

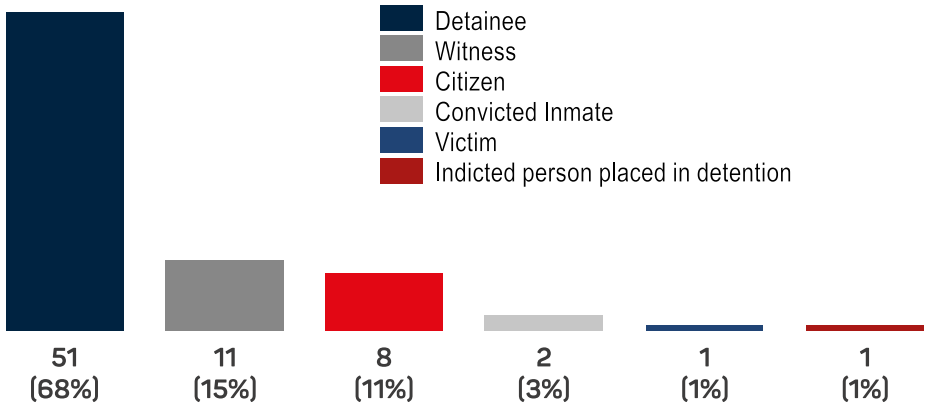
92% of possible victims were adults, while 7% were minors. The age of one victim could not be established as it had not been possible to identify and interview him/her.

AGE OF POSSIBLE VICTIMS



68% of possible victims were persons detained through administrative (32 persons) or criminal (19 persons) proceedings; 15% were witnesses; 12% - other persons; 3% - convicted prisoners; 1% - a victim and 1% - a pre-trial detainee.

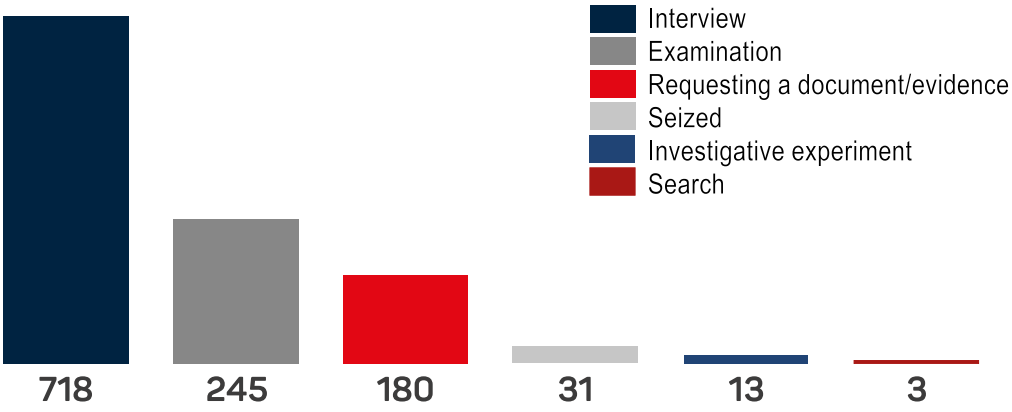
PROCEDURAL STATUS OF POSSIBLE VICTIMS



3.4. INVESTIGATIVE AND PROCEDURAL ACTIONS CARRIED OUT

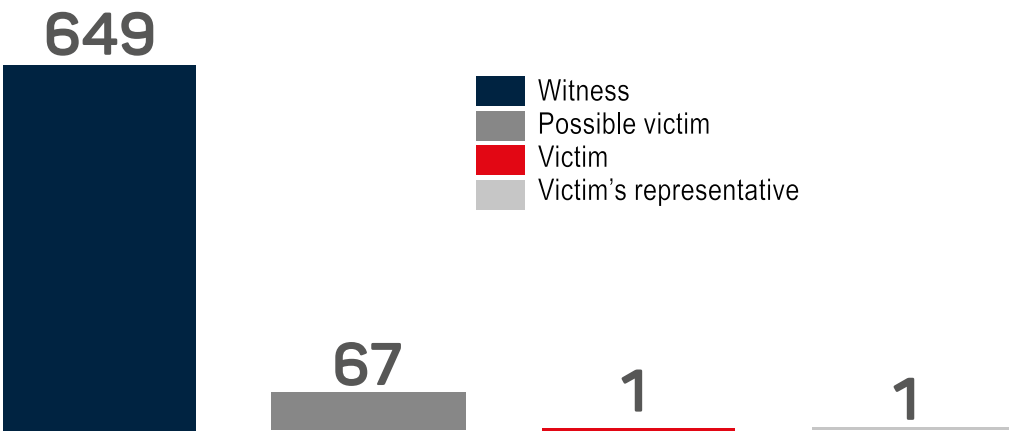
In 2019 the State Inspector's Service carried out 1190 investigative and procedural actions on criminal cases under its jurisdiction:

INVESTIGATIVE ACTIONS CARRIED OUT



In 2019 total of 718 persons (649 - witnesses), 67 – possible victims; 1 – victim; 1 – victim's legal representative) had been interviewed.

PERSONS INTERVIEWED



Out of total number of witnesses interviewed, 181 had been representatives/ employees of the law enforcement bodies and 46 – minors.

It should be noted that in criminal cases that are processed by the State Inspector's Service, victims or potential victims are mainly persons detained either through administrative or criminal procedure. Respectively, the persons directly or indirectly involved in imposing criminal or administrative sanctions against them, are alleged offenders. Due to this, victims often refrain from testifying against those who had committed acts of violence against them.

10 possible victims did not cooperate with the investigation (they do not share information with the investigation on the facts of the case; they provide information radically different from the content of their own report or contradictory to other solid evidence collected by the investigation on the case; they fail to hand over material evidence in their possession to the investigation).

In the cases investigated by the State Inspector's Service eye witnesses are mainly the representatives of the law enforcement bodies. From 114 persons interviewed none of them confirm unlawful actions by him/her or by his or her colleague/co-worker. As a rule, they appeal to completely different circumstances.

During 2019 the State Inspector's Service received only one crime report from a third party, while in 31% of cases, victims claimed that crime took place in the street.

The criminal cases processed by the State Inspector's Service rarely have neutral witnesses (bypassing citizens). In case there is one, he/she usually states that despite their presence, they saw or heard nothing.

With regard to the cases processed by the State Inspector's Service 9 witnesses completely refused to testify (it was possible to interview only 3 of them in the court; 6 of them didn't respond to telephone calls and were not found at their places of residence). One person later changed a testimony against a police officer that he had given to investigation.

The State Inspector's Service interviews child witnesses/ possible victims in mandatory presence of a psychologist. It is challenging for investigative bodies to find/procure child psychologists and to have them involved in investigative actions; this often becomes a reason for postponing investigative actions.

Forensic Examination

In criminal cases falling under jurisdiction of the State Inspector's Service, the applicants mainly refer to possible violence committed by representatives of the Ministry of Internal Affairs. For this reason the Service mainly applies to Levan Samkharauli National Bureau of Forensic Examination,

in order to avoid speculations on impartiality and objectivity of forensic examination.

The investigative mandate of the State Inspector's Service expands over specific violent crimes committed by a representative of law enforcement authorities, an official or a person equal to an official. Therefore, forensic examination represents one of the main procedural actions in those cases (the forensic expert responds to questions related to existence/ absence of injury, its degree, location, age and severity of injury).

74 forensic examinations have been appointed throughout 2019 (among them 59 forensic medical examinations).

The State Inspector's Service faces three main challenges when appointing and carrying out forensic examinations: a) some possible victims refuse to undergo forensic examination; b) experts are unavailable during weekends and after working hours; c) the forensic examination reports arrive with a delay (insufficient human resources are cited as reasons for points under 'b' and 'c'). It shall be noted that a positive trend of submitting forensic examination results on time has been observed since March 2020.

As noted above, there are 75 possible victims registered in connection of criminal cases initiated in 2019. The State Inspector's Service appointed / requested forensic medical examination of 59 persons (on 55 criminal cases).

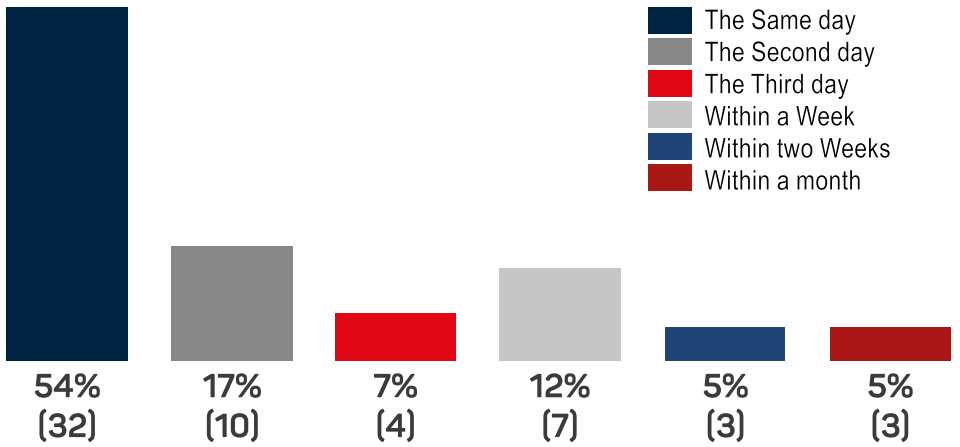
From the abovementioned 59 persons, 76% reported to a medical expert for examination; 20% failed to appear (their forensic medical examination was carried out based on medical documen-

tation obtained by the investigation); 4% - failed to appear and there were no medical documents pertaining to their cases.

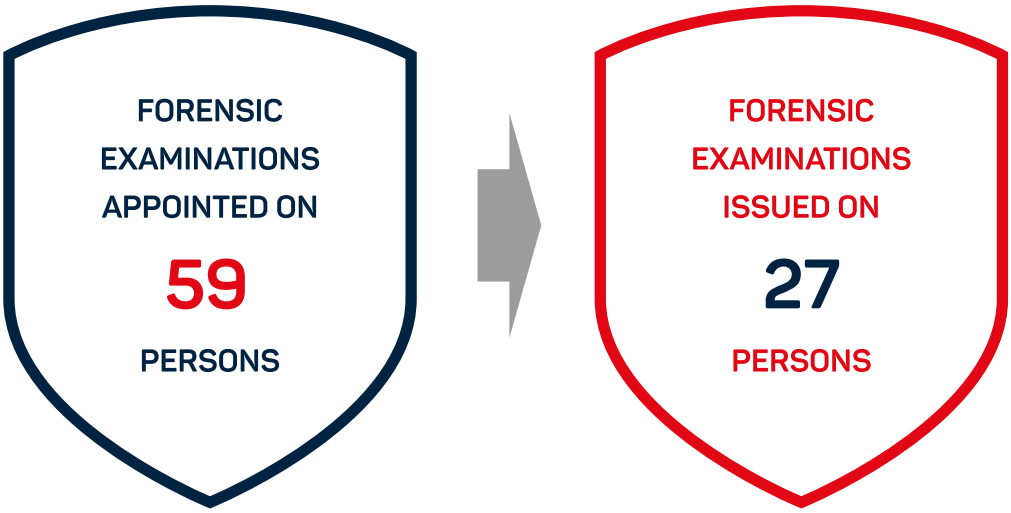
No medical forensic examinations were appointed in 13 criminal cases (on 16 persons), since many victims (10 persons) refused to undergo examination as according to them, there were no signs of injury on their bodies (in addition, there were no medical documents on their cases and therefore it was impossible to carry out forensic medical examinations). In other cases, long time interval between the alleged incident and disappearance of traces of injury (this concerns delayed notifications), as well as refusal to cooperate with investigation, were cited as reasons for not having medical examinations.

Since timely forensic examination is very important for determining the degree of injury, forensic examinations of 54% of victims were appointed on the day the investigations were launched; of 17% - on the second day of starting investigations; on 7% - on the third day and on 22% - between one week and a month. The latter concerned cases where it proved to be impossible to submit a person to an expert for forensic examination and where it became necessary to obtain medical documentation.

TERMS OF APPOINTING FORENSIC MEDICAL EXAMINATIONS



The State Inspector's Service received 27 (46%) forensic examination results out of 59 submitted for forensic examination. 45% of examination results out of forensic examinations appointed in 2019 were submitted to the Service during February-Mach 2020. Forensic examination results on the cases under the jurisdiction of the State Inspector's Service are directly connected with the adoption of the final decisions on those cases.



Requesting Information about Audio-Video Recordings

Audio-video recordings placed at alleged crime scene represent important evidence on criminal cases investigated by the State Inspector's Service. Respectively, public and private entities are requested to hand over the audio-video recordings to the investigation.

The Investigative Department filed 158 requests in respect of 58 criminal cases to public and private organisations to hand over their audio/video recordings baring importance for investigations. 34% of the requests were addressed to the Joint Operations Centre of the Ministry of Internal Affairs (currently – A Public Security Management Centre '112')[1], 6% - were addressed to the Temporary Detention Department of the Ministry of Internal Affairs[2], 5% - from the Patrol Police Department of the Ministry of Internal Affairs[3], 3% - from the Special Penitentiary Department[4], 41% - from natural and legal persons.

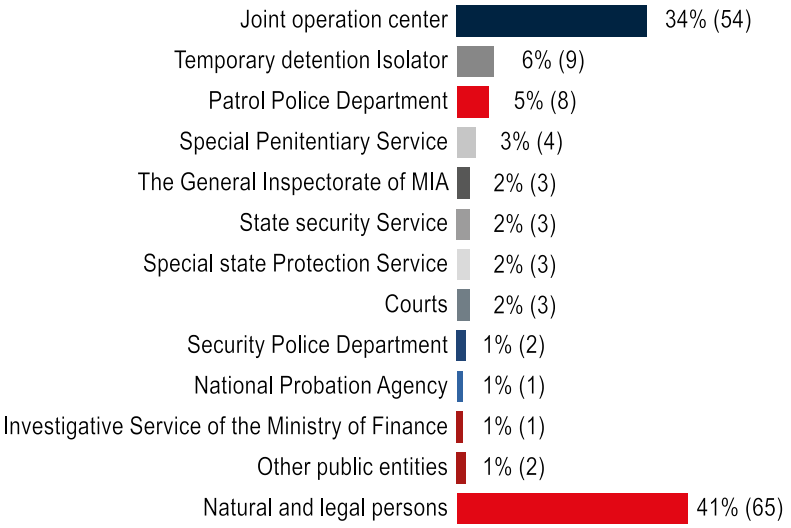
1 Video recordings of surveillance cameras installed at the administrative building of territorial units (police departments) of the Ministry of Internal Affairs as well as shoulder cameras of patrol police officers are stored at the Joint Operations Centre of the Ministry of Internal Affairs

2 Video recordings of video surveillance cameras installed at the temporary detention isolators are stored at the Temporary Detention Department of the Ministry of Internal Affairs

3 Recording made by patrol police Dash Cams are stored at the Patrol Police Department of the Ministry of Internal Affairs;

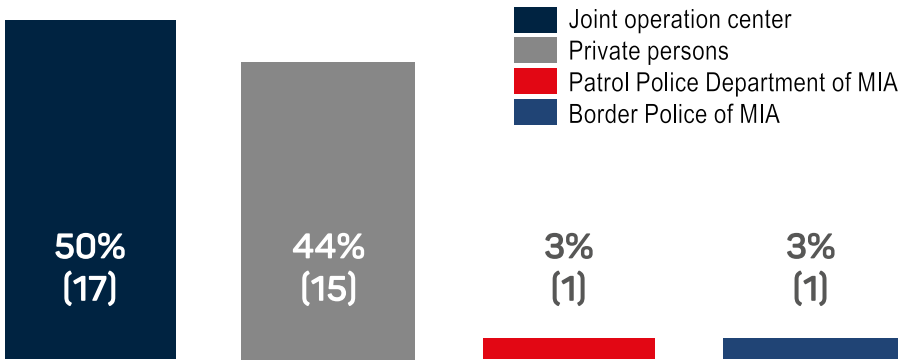
4 Video recording of surveillance video cameras installed at the penitentiary establishments are stored at the Special Penitentiary Service

ENTITIES FROM WHICH AUDIO-VIDEO RECORDINGS HAVE BEEN REQUESTED



In 34 cases, when the State Inspector's Service based on the court ruling requested audio-video recordings, the State Inspector's Service was told that the recording was not found. The following persons/ organizations were not able to/did not provide the requested recording: Joint Operations Centre of the Ministry of Internal Affairs/ Public Security Management Centre '112' (17 cases); private persons (15 cases), Patrol Police Department of the Ministry of Internal Affairs (1 case), Border Police of the Ministry of Internal Affairs (1 case).

REJECTING THE REQUEST FOR PROVISION OF AUDIO/VIDEO RECORDINGS



Failure to provide requested information by the institutions, the employees of which may have been involved in criminal activities, raises questions (especially, when the request is made immediately after committing an alleged crime, within few hours).

It should be noted that in 30% of cases it was stated that the alleged crime took place in the police car. The interior of the police car is not monitored. Respectively, it is impossible to collect recordings of these types of facts.

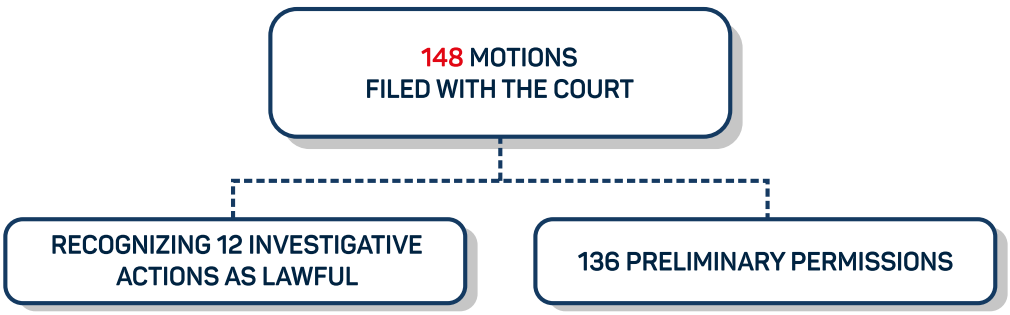
In many cases the quality of video recordings placed in the administrative buildings of the law enforcement bodies is rather low. The low quality of the recording makes it difficult to identify specific individuals and their actions. At the same time, the visibility of video cameras does not reach all those places where participants of procedure move around.

3.5. MOTIONS FILED WITH THE COURT

In the process of investigation the State Inspector's Service closely cooperates with the General Prosecutor's Office.

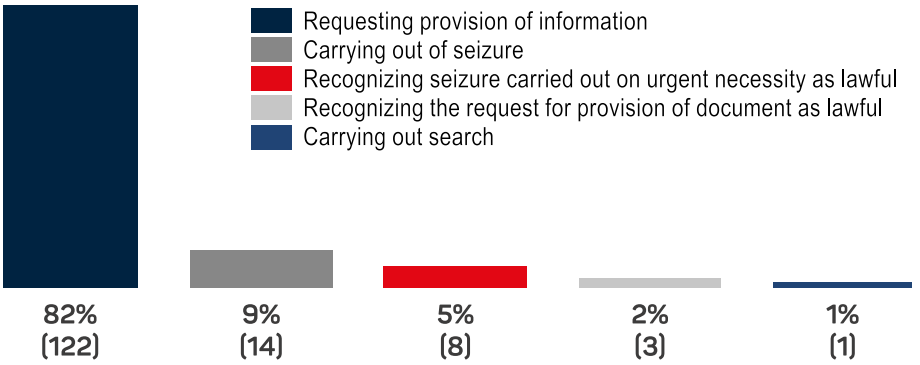
The General Prosecutor's Office has filed 148 motions with the court on the criminal cases investigated by the Investigative Department of the State Inspector's Service. All of them were granted (In number of cases permission for carrying out multiple investigative actions was requested by a single motion).

92% of investigative actions infringing upon the rights to private property, ownership and privacy were carried out with a prior judicial authorization. Only 8% of the 148 motions concerned the request to recognize as lawful investigative actions that had already been carried out due to urgent necessity.



The majority of the 148 motions (82 %) submitted to the court concerned requesting information.

MOTIONS FILED BY PROSECUTORS WITH THE COURT



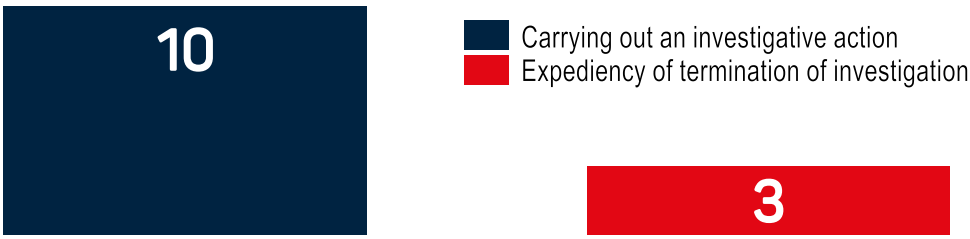
3.6. SUBSTANTIATED PROPOSALS SUBMITTED TO THE GENERAL PROSECUTOR'S OFFICE

According to the Law of Georgia on "State Inspector's Service" the deputy State Inspector, in charge of the investigative direction may apply to the supervising prosecutor in writing with a substantiated proposal.

Throughout 2019 the Corresponding Deputy State Inspector applied to the General Prosecutor's Office with 13 substantiated proposals, 9 of which concerned the request to file a motion with the court requesting provision of information / documentation; 3 concerned the expediency of terminating investigation; and 1 concerned the seizure of medical files from a medical facility.

The General Prosecutor's Office took all the proposals into consideration.

PROPOSALS SUBMITTED BY THE DEPUTY STATE INSPECTOR TO THE PROSECUTOR GENERAL'S OFFICE



FINAL DECISIONS ADOPTED

The General Prosecutor's Office adopted 9 final decisions on the cases investigated by the Investigative Department of the State Inspector's Service.

Specifically, 8 criminal investigations launched in 2019 were terminated (including 1 case handed over to the State Inspector's Service from another investigative service in line with the rules of procedural jurisdiction). The grounds for terminating investigation in each case had been the lack of an act provided for by the criminal law, as provided for in Article 105.1, sub-section "a" of the Criminal Procedure Code of Georgia. 7 cases were qualified as crimes provided for by Article 333.3 sub-section 'b' of the Criminal Code of Georgia (Exceeding official powers with use of violence), while on one case investigation proceeded on the basis of Article 187 of the Criminal Code of Georgia (Damaging an Object).

The criminal prosecution was initiated against 1 person on the basis of Article 335 of the Criminal Code of Georgia (forcing someone to provide evidence) (2 episodes). The case is currently tried in the court.

4. THE ACTIONS IMPLEMENTED IN ORDER TO IMPROVE THE ACTIVITIES OF THE SERVICE

METHODOLOGY ON PROCESSING STATISTICS DEVELOPED

WEB-PAGE FOR INVESTIGATIVE DEPARTMENT

AN ELECTRONIC SYSTEM FOR RECEIVING CRIME REPORTS WAS INTRODUCED

THE WORKING MEETING WITH THE REPRESENTATIVES OF THE PUBLIC DEFENDER'S OFFICE WAS HELD

COMMUNICATION STRATEGY WAS DEVELOPED

4.1. DEVELOPING A METHODOLOGY FOR PROCESSING STATISTICS

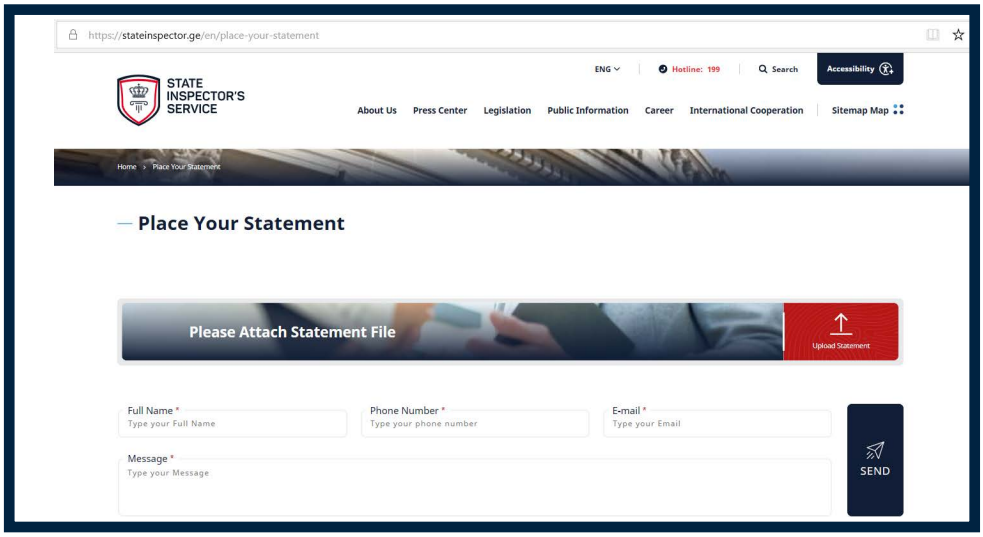
With the assistance of Council of Europe expert and for comprehensive processing and analyzing of statistical data, the Service has developed a unified methodology for collecting and producing statistical data.

According to the methodology the Analytical Department of the service shall collect detailed statistical data on reports filed with the State Inspector's Service, as well as on criminal investigations under its jurisdiction. The data is collected on the basis of specifically developed tables; in parallel it is planned to develop a respective electronic programme. Some statistical data are also collected through the statistical module of the Criminal Case Management System.

Processing and periodical analysis of statistical data using various parameters helps the Service in identifying existing trends, challenges and in developing effective measures for addressing them.

4.2. INTRODUCING AN ELECTRONIC SYSTEM FOR RECEIVING CRIME REPORTS

The citizens can electronically report to the State Inspector's Service of possible crimes using a web-page of the Investigative Department of the State Inspector's Service (https://stateinspector.ge/ka/place-your-statement). Considering that the Service is physically present in the 2 cities only, the possibility of electronically filing a notification from any place in Georgia is very important.



5. CHALLENGES

The State Inspector's Service has accumulated a few months of experience of conducting investigations and this experience makes it possible to make preliminary conclusions and identify challenges the Service is facing.

It can be stated without modesty that the Investigative Department of the Service has become institutionally operational. The Service employs qualified investigators, is equipped with sufficient technologies and financial resources. The Service adequately responds to everyday challenges and constantly strives for improvements.

The analysis of cases investigated by the Investigative Department of the State Inspector's Service, as well as of its activities point at a number of challenges (including legislative) that the Service faces:

- The state institutions and the citizens often notify the State Inspector's Service of a possible crime with a considerable delay, which gets on the way of collecting evidence and effective investigation of the case. Therefore, coordination with respective state institutions and awareness raising of potential victims (e.g. inmates at the penitentiary establishments) shall be stepped up;.
- For investigating crimes falling under jurisdiction of the State Inspector's Service it is important to procure engagement of non-involved persons (so-called "impartial third parties"). The cases of third parties reporting to the State Inspector's Service of a possible crime are very limited even when 31% of applicants state that crime was committed on the street;
- The cases investigated by the State Inspector's Service rarely have neutral witnesses (the by passers). Even when they are present, they claim that despite being there at the time of the incident, they saw or heard nothing. This trend points at the need for public awareness raising;
- The victims/ potential victims of cases under jurisdiction of the State Inspector's Service mainly are persons under criminal or administrative detention. Respectively, the persons directly or indirectly involved in imposing criminal or administrative sanctions against them, are alleged offenders. Due to this, victims often refrain from testifying against those who had committed acts of violence against them;
- It is difficult to find and engage child psychologists in the investigative actions; this often becomes a reason for postponing investigative actions. At the same time, the Service at this

stage does not have a special space for interviewing children (the relevant funds could not be allocated from last year's budget);

- In many cases the Investigative Department of the Service fails to obtain neutral evidence. The video recordings made by shoulder cameras of police officers, patrol police car Dash Cams and by the video monitoring systems installed at the administrative buildings of the law enforcement institutions represent a significant neutral evidence. The analysis of established practice indicates that in some criminal cases video recording has not been provided, citing as a reason unavailability of such recordings on a hard disc. Failure to provide requested information by the institutions, the employees of which may have been involved in criminal activities, raises questions (especially, when the request is made immediately after committing an alleged crime, within few days). Since reports on potential crimes arrive at the State Inspector Service with a certain delay, the State Inspector Service immediately appeals to the Ministry of Internal Affairs, prior to obtaining a court ruling, requesting the Ministry to temporarily store/archive video recording of possible crime, however the Ministry does not consider these requests. Besides, in 30% of cases police car is mentioned as a place where crime has been committed and interior of police cars is not monitored. Therefore, it is impossible to obtain video materials on those cases. In many cases, the quality of video recordings carried out at the administrative buildings of the law enforcement bodies is rather low. Low quality of the recording makes it difficult to identify specific individuals and their actions. At the same time, the visibility of video cameras does not extend to all those places where participants of procedure move around. In order for the State Inspector's Service to ensure effective investigations, the law enforcement bodies must apply special measures to eradicate potential cases of deleting video recording; They should also ensure that video surveillance system encompasses fully the space within their administrative buildings, where participants of proceedings are held/or where they are able to move. In addition, the Ministry of Internal Affairs should take steps to mount video cameras in the police cars and to replace/upgrade low quality video cameras at its administrative buildings; the period of time during which the recording is kept should be prolonged or a mechanism for temporarily archiving the material should be put in place;

- Carrying out forensic examination is problematic. Experts are unavailable during weekends and after working hours, which makes it impossible to present a victim to a forensic expert and to immediately record existing injuries. The forensic examination reports / expert opinions also arrive with a delay, which hinders scheduling other investigative actions on the case and the adoption of final decisions. The issues related to forensic examinations are crucial for the service, as they are directly correlated with timely and effective investigations;

- The State Inspector's Service which is an independent investigative body accountable to the Parliament of Georgia and which is responsible for effective and impartial investigation, is not entitled to independently (without engagement of the Prosecutor's Office) decide on carrying out important investigative actions, such as search, seizure, in many cases – examination, witness examination at the court during investigation, carrying out investigative actions related to computer data (including requesting provision of documents and information) and to covert investigative actions. The Service can also not decide independently on carrying out operative-investigative activities. At the same time, a prosecutor is entitled to issue a mandatory instruction to an investigator concerning the conduct of investigative activities, including those that, according to current legislation are carried out by the decision of an investigator independently. Such dependency on another institution cannot fully guarantee institutional independence of the Service. Therefore, the State Inspector's Service finds it very important that the reform initiated by the Ministry of Internal Affairs on separation of investigative and prosecutorial functions be finalized in a timely manner, especially, in respect of the State Inspector's Service (The Service employs highly qualified investigators who have been recruited through an open, transparent and multi-stage competition; they have passed qualification examinations equal to the level of judicial and prosecutorial examinations, therefore they can ensure to independently carry out effective investigation);[1]

- According to the Law of Georgia on the State Inspector's Service the State Inspector and the Deputy State Inspector are entitled to submit substantiated proposals to the General Prosecutor's Office on various issues (this could concern handing over a case for investigation, familiarization with case materials, initiation of criminal prosecution, the expediency of termination of criminal prosecution or a criminal investigation, carrying out investigative activities infringing upon private property, ownership or privacy or procedural actions). However, the law does not provide for the right to appeal the refusal of a prosecutor in the court. Granting such a right to the State Inspector's Service and subjecting this process to judicial review, would increase trust into final decisions adopted by the State Inspector's Service;

- The Law does not provide for the right of a State Inspector to address the General Inspectorates of the relevant services with substantiated proposals, in case disciplinary violation by an employee is confirmed. The Law provides for neither responsibility of institution receiving such proposal nor a procedure for its review. During the reporting period the Service addressed one institution with such a proposal, but due to absence of respective procedures, the decision made by the institution is still unknown;

1 The reform for delineating investigative and prosecutorial functions was positively assessed by the Venice Commission in its opinion of March 2019 https://www.venice.coe.int/webforms/documents/?pdf=C-DL-AD(2019)006-e#

- It is a challenge to raise public awareness on the functions of the State Inspector's Service. The Service is often addressed regarding the incidents that do not fall under its jurisdiction or that have been committed prior to 1 November 2019. The citizens also most often report possible crimes committed by the police officers to the General Inspectorate of the Ministry of Internal Affairs, instead of reporting them directly to the Service;

- Another challenge for the Service is the lack of adequate infrastructure. The East Unit of the Investigative Department is still located at rented premises, for which the Service makes considerable monthly payments from the state budget. In spite of numerous requests, it was still not possible to find adequate space/premises for the Service;

- It is difficult to cover the entire territory of the country from the two offices of the Investigative Department (in Tbilisi and in Kutaisi) and it is impossible to appear at crime scene immediately. The cases, when possible victim and/or persons to be interviewed live far away from the administrative buildings of the Service, create difficulties in practice. On the one hand, this often delays timely reporting by a witness and, on the other hand, it complicates investigative actions to be carried out in respective territorial units due to lack of infrastructure.

COOPERATION WITH THE PUBLIC DEFENDER'S OFFICE AND NON-GOVERNMENTAL ORGANISATIONS

VII. COOPERATION WITH THE PUBLIC DEFENDER'S OFFICE AND NON-GOVERNMENTAL ORGANISATIONS

The State Inspector's Service cooperates with the Public Defender's Office and with non-governmental organisations both on issues related to personal data protection, as well as on those related to implementation of its investigative function.

The State Inspector periodically meets with representatives of the Public Defender and non-governmental organisations, organizes joint working meetings, provides them with information on the activities of the State Inspector, and carries out research and awareness campaigns with them.

Throughout 2019 NGOs applied to the State Inspector on 7 facts of violation of personal data protection. The cases mainly concerned violation of data subject's rights and disclosure of information.

As for the investigative function, during November-December 2019 the State Inspector received 12 letters (5 reports on alleged crime, 5 requests for provision of information on actions carried out in relation with specific incidents/facts, 2 – requests of statistical data) from the Public Defender's Office. NGOs submitted 6 letters (4 of them concerned information on a possible crime which did not fall under the jurisdiction of the State Inspector's Service, 1 – requested information concerning ongoing investigation of a criminal case, 1 – requested information on applications received for the position of investigator at the State Inspector's Service). Comprehensive and substantiated responses were sent on all of them within deadlines provided for by law.

The State Inspector's Service provides information (in writing or through meetings) to the Public Defender about ongoing investigations of criminal cases and, in case of request, makes materials of criminal cases accessible to the Public Defender.

The representatives of NGOs are involved in various criminal cases that are processed by the Investigative Department of the State Inspector's Service. The Service regularly shares the information on the development in the investigation process with them and listens to their opinion with regard to conducted and planned investigative actions.

PUBLIC RELATIONS

VIII. PUBLIC RELATIONS

The image and the reputation of any institution greatly depends on correct and effective public communication. The activities of the State Inspector's Service are founded on the principles of public accountability, openness and transparency. Despite a solid reputation within informed circles of the society, public awareness raising remains a challenge. High expectations towards the Service increases the importance of accurate communication with target groups. This issue became even a greater concern in 2019 since the expansion of the mandate of the Service, enactment of a new investigative function and rebranding of the Service.

Public communication through mass and social media was being actively used during the reporting period. The State Inspector's Service aimed at sharing information proactively. The Service appeared in media 2947 times, including 1705 times in television, 842 times in print media; 310 times in internet and 90 times in radio broadcasting (the information is provided by a research company "IPM").

The Service makes active use of social media for informing society timely and for awareness raising. The number of visitors of the official Facebook page of the State Inspector's Service was expanded in 2019. The number of visitors of a Facebook page increased from 9 892 in 2018 to 23 890 in 2019.

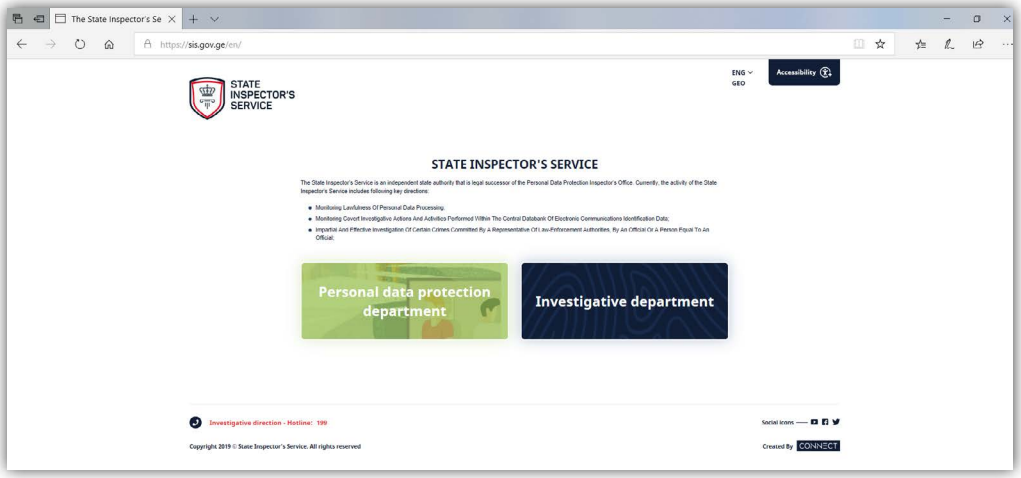
The Service has been keen to cooperate with media and to answer questions of the public. The public has been regularly informed about criminal cases of high public interest. Throughout 2019 the Service has issued 15 press releases for this purpose. In addition, the State Inspector has had direct contact with the representatives of media through briefings and press conferences and has provided them with detailed information on the issues falling under the State Inspector's competences. Besides, the State Inspector organized two thematic meetings for journalists: one – concerning the enactment of an investigative function and the other – on the importance of personal data protection in journalistic work.

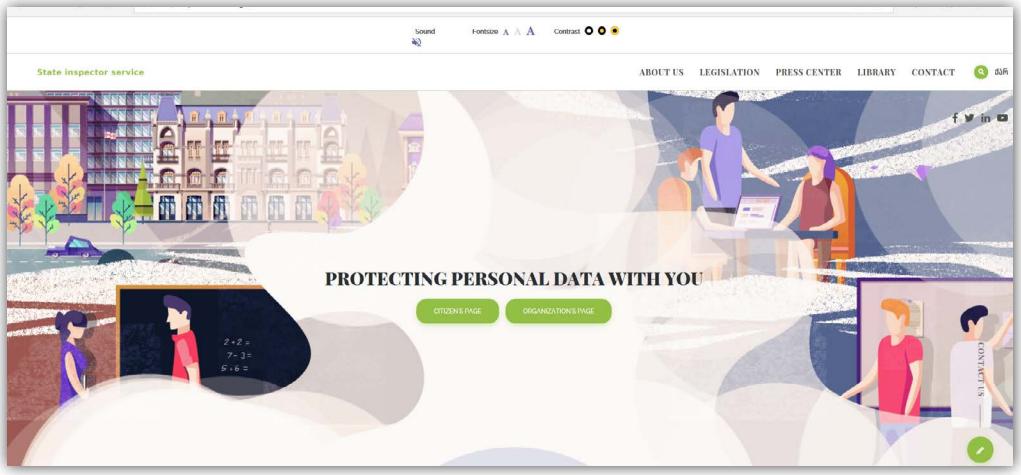
1. CREATING A NEW WEB-PAGE

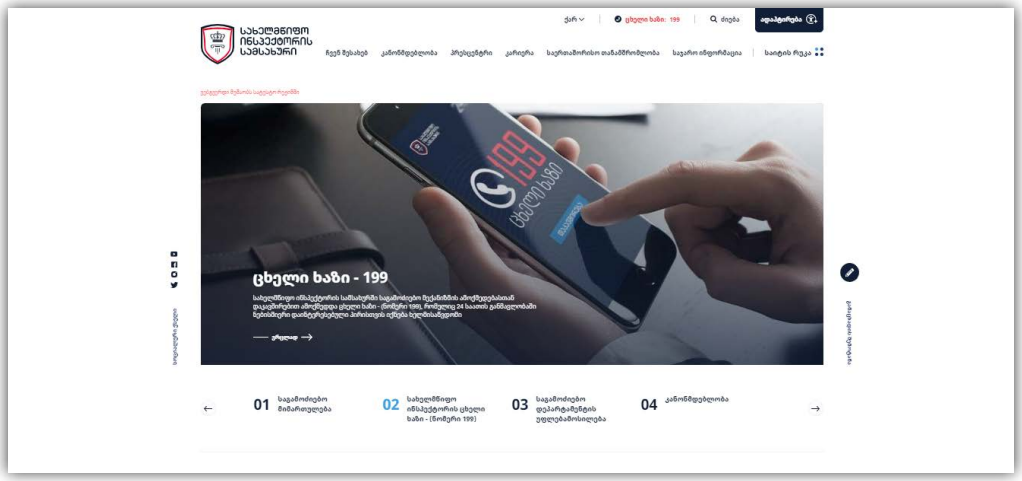
In order to improve public communication and information on personal data protection issues a new web-page was launched in 2019 (www.personaldata.ge). Considering diverse nature of personal data protection and investigation the Service decided to launch a new (additional) web-site. The web-page on personal data protection (www.personaldata.ge), which was renewed in January

2019, maintained its outlook and information; while, for ease of access to information on investigative function, a new web-page was set up - www.stateinspector.ge. Both pages have been merged under the main web-page of the Service (www.sis.gov.ge).

The web-pages have been developed with the assistance of the European Union (EU) and the United Nations Development Program (UNDP). It represents a modern, interactive and user-friendly digital space, fully adapted for visually impaired citizens. All new developments and statements of the State Inspector are published on the web-pages. Besides, any interested party can electronically apply to the State Inspector's Service during 24 hours.







2. DEVELOPING COMMUNICATION STRATEGY

The Communication Strategy of the State Inspector's Service aiming at raising public awareness, building trust and effective public communications was developed last year with the support of the Council of Europe.

The document defines the directions and goals of communication, target audience, means of communication and the impact of positive communication. The document describes in detail the potential risks, challenges, strength and opportunities of the Service. Broad circles of society are identified as a target audience, including students and youth; law enforcement bodies; other public institutions; international organisations; civil society; the Public Defender's Office; representatives of legal community and academia; national and regional media. The communication strategy foresees specific activities and active information campaigns for each target group.

The aim of activities foreseen under the Communication Strategy is to raise public awareness on the activities of the Service, to promote relevant attitudes and expectations towards the Service, to establish effective communication with media and to support the establishment of the image of the State Inspector's Service as a highly competent, impartial, trustworthy and independent human rights institution.

3. RAISING PUBLIC AWARENESS

In 2019 the priority of the Service was to raise public awareness on issues of personal data protection. As a result, over 600 representatives of public and private sectors, including local self-governments, schools, universities and medical facilities were enabled to learn and improve their knowledge of the personal data protection.

During the reporting period, number of educational and awareness raising activities have been carried out on the means and importance of personal data protection, as well as concerning the activities of the State Inspector's Service, including:

- In 2019 the working meeting concerning protection of personal data of children under the state care was held for the first time. Representatives of the State Inspector's Service provided detailed information to children/minors about their rights related to protection of personal data and mechanisms of protection of those rights;
- The State Inspector's Service continues to offer free training courses on personal data protection to interested citizens. The training courses were held every month. Up to 150 interested persons received information on their rights in relation to protection of their persona data.
- In 2019 the State Inspector's Service continued to have workshops for the local self-governance bodies. Over 80 representatives of local self-governance were trained;
- During the reporting period, the State Inspector's Service developed a training module on processing personal data in the healthcare sector, which is specifically designed for this sector with due respect to its specificities. The training module aims at ensuring high standard of personal data protection in the healthcare sector and at eradicating existing shortcomings. The training module will be actively used in training during 2020;
- In cooperation with the National Bank of Georgia, the State Inspector's Service developed recommendations for "Personal data processing by commercial banks". The document aims to assist commercial banks in complying with existing legislative requirements when processing their clients' personal data. While presenting recommendations jointly to the public the State Inspector's Service and the National Bank also signed a Memorandum of Cooperation;

- In cooperation with the CoE distance learning platform (HELP) a training course on Personal Data Protection and the right to Privacy was implemented in Georgia for the first time in 2019. The course is made for practicing lawyers and consists of 10 modules. The first 3 modules address the basic legal mechanisms in Europe, institutions working on personal data protection and privacy issues and main legal concepts in this area. Following 7 modules deal with medical data, media, new technologies, digital communications, surveillance at a workplace, enforcement mechanism and cross border transfer of data. The employees of the State Inspector's Service are trained in the first place. Later the course will be available for representatives of other institutions and interested persons;

- As a result of active cooperation of the State Inspector's Service with the Council of Europe a manual of European Law on Personal Data protection and "Guidelines for Protection of Privacy in the Media Space" were published in 2019. The translation and publication of these resources aim at raising public awareness, as well as improving practice and putting in place high standards of protection of personal data. The manuals are being distributed to target groups and interested persons;

- In the beginning of 2019, the Service developed a public service announcement on the importance of personal data protection. The PSA was disseminated through TV channels and social media. It was viewed by 163 000 users only on the webpage and on Facebook;

- Thematic leaflets (on video surveillance, direct marketing, healthcare, etc.) have been developed and published on the official Facebook page of the Service.

INTERNATIONAL COOPERATION

IX. INTERNATIONAL COOPERATION

One of the priorities of the State Inspector's Service in 2019 was an effective cooperation with international organisations and its counterparts in foreign states.

The State Inspector's Service participated in various international platforms and conferences. The Service was also actively engaged in the process of development of various types of international documents. Specifically, the Service was involved in the development of the Guidelines on Artificial Intelligence and Personal Data Protection by the consultative committee of the Convention 108 of the Council of Europe. The State Inspector's Service also represented Georgia in Strasbourg at the first meeting of the Ad hoc Committee on Artificial Intelligence (CAHAI). The Committee is made up of experts from CoE member states, representatives of various international organisations and observer states. Based on the CoE standards on human rights, democracy and the rule of law, the Committee shall examine the feasibility of a legal framework for the development, design and application of artificial intelligence.

In 2019 the State Inspector's Service organized and hosted the Spring Conference of European Data Protection Authorities, which is the most prominent international forum on personal data protection issues. Up to 100 high level delegates participated in the conference, including the leaders of the European data protection authorities. The participants of the conference discussed challenges such as implementation of the EU General Data Protection Regulation (GDPR), protection of child's data, the role of international organisations in data protection.

The draft law on Personal Data Protection was developed and submitted to the Parliament of Georgia based on the legislative proposals drafted in cooperation with international experts. The draft law aims to ensure compatibility of Georgian legislation with the European standards, compliance and fulfillment of commitments under the EU-Georgia Association Agreement and enhancing the standards of personal data protection in Georgia.

In 2019 the Service organized a translation into Georgian of one of the most important European legal documents in the area of data protection - Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (the so-called – "police directive"). The document was translated with the support of the EU and the

OHCHR. The Georgian version of the police directive has been published on the web-page of the State Inspector's Service and is accessible for all interested parties.

In addition, the State Inspector's Service provides legal expertise on international agreements and treaties to be signed by Georgia in order to ensure high standard of personal data protection. In 2019, 22 draft international agreements have been examined and 14 recommendations have been issued.

The State Inspector's Service, within the scope of its competences, participated in the process of fulfillment of various commitments of Georgia under the EU-Georgia Association Agenda and other international obligations.

The State Inspector's Service actively supports acceleration of the process of signature of the Convention 108+, a modernized version of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and hopes that in 2020 Georgia signs its third additional protocol. Signing it, Georgia will be making an additional step towards implementation of international human rights standards. A new draft law fully complies with the modern requirements of the Convention 108+ which will significantly speed up and facilitate implementation of the modernized Convention on the national level.

In parallel with the election of the new State Inspector and the expansion of the Service's mandate, there were number of meetings held with the local representations of the international organisations. Meetings were held with the representatives of the CoE, EU, UN OHCHR, UNICEF, US Embassy and the World Bank. The priorities, challenges, needs and prospects of future cooperation were discussed at the abovementioned meetings. The special emphasis was put on the enactment of the investigative function and the need for proper implementation of the draft law presented to the Parliament concerning personal data protection.

FUTURE PLANS

X. FUTURE PLANS

In 2020 the State Inspector's Service aims at improving the situation in terms of protection of personal data, developing further the investigative activities of the Service and increasing the quality of work of the Service.

In order to improve the personal data protection and to carry out an effective control over personal data processing the Service plans to implement following activities:

- Support the process of adoption of the Law of Georgia on "Personal Data Protection" – initiated at the Parliament of Georgia;
- Organise thematic meetings with data controllers from different sectors;
- Establish criteria for carrying out planned inspections (for identifying high-risk areas), which shall serve as a basis for developing a Plan for 2021;
- Intensify inspections carried out in the regions;
- Improve mechanisms for monitoring the fulfilment of recommendations and instructions issued by the Service;
- Enhance coordination mechanisms with the other agencies having control over data controllers;
- Develop commentaries on the Law of Georgia on "Personal Data Protection";
- Design thematic training programmes for the representatives of different sectors;
- Develop thematic compilations of the final decisions adopted by the State Inspector's Service;
- Organise a training of trainers (TOT) for the employees, who in turn will support data controllers in re-training their staff;
- Develop a methodology for statistics and relevant documentation;
- Define and introduce standards for rendering consultations on the issues of personal data protection;
- Develop a methodology for assessing the protection of personal data;

- Organise awareness raising campaigns on personal data protection in all regions of Georgia, with active engagement of "Personal data protection Ambassadors";
- Cooperate with educational institutions and introduce training courses on the topic of personal data protection;
- Support the process of signature of the modernized 108+ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

For improving effectiveness of investigations, the State Inspector's Service plans the following:

- Active cooperation with other investigative authorities for crime prevention and enhanced co-ordination in the process of investigation;
- Draft amendments to the Law of Georgia on "the State Inspector's Service" to address legislative shortcomings faced by the Service;
- Active participation and support of the process of reform aimed at delineation of investigative and prosecutorial functions;
- Improve territorial accessibility of the Service. In 2020 the Service will have at least one additional office in Batumi which is the third place after Tbilisi and Kutaisi in terms of number of applications. Respectively, the number of investigators will also increase;
- Arrange a child-friendly space at the premises of the State Inspector's Service (this time in Kutaisi) for upholding of the best interest of a child;
- Signing contracts with child psychologists for ensuring their availability and participation in the investigation process;
- Introduce an appraisal system for investigators, which is important for effective investigation;
- Raising qualification of investigators (including in victim, witness interviewing technics) in order to ensure that investigations are carried out in line with international standards;
- Introduce an internship system, which would enable the Service to grow new professionals for the Service;
- Familiarise with the best practice of independent investigative mechanisms.

For improving quality of Service's operations, its development and enhanced transparency, the State Inspector's Service plans the following activities:

- Setting up a consultative council with participation of non-governmental organisations, to which the State Inspector would present its activity reports in order to receive their feedback and recommendations;
- Developing an internal communication system;
- Raising qualification of staff/employees;
- Introduction of performance appraisal system;
- Setting up a collegial body that would decide on the punishment, encouragement and promotion of the employees of the Investigative Department;
- Actively work on raising public awareness (including through developing information materials and their dissemination in relevant organisations (law enforcement authorities, penitentiary establishments));
- Using multiple channels and means for communicating with public (including at local level);
- Developing indicators for assessing results of the public awareness activities carried out by the Service;
- Carrying out a survey to assess public attitudes towards the Service;
- Develop a strategy for international relations;
- Active cooperation with international organisations and engagement in international platforms.

www.sis.gov.ge