PERSONAL DATA
PROTECTION SERVICE

2022 ACTIVITY REPORT OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

PERSONAL DATA
PROTECTION SERVICE

2022 ACTIVITY REPORT OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

This report is prepared in compliance with Paragraph 1 of Article 40^{10} of the Law of Georgia "On Personal Data Protection" according to which the President of Personal Data Protection Service shall present the report on the status of data protection in Georgia, as well as on the monitoring of the conduct of covert investigative actions, and the activities carried out in the electronic data identification central bank, to the Parliament of Georgia once a year, no later than March 31. Accordingly, the report encompasses the information about the activities conducted by the Service during the reporting period from March 1, 2022 up to December 31, included.

2022 activity report of the Personal Data Protection Service of Georgia consists of four parts:

THE PERFORMANCE REPORT OF THE SERVICE, which reviews the activities carried out by the Service during the year. On the one hand, it brings together the topical issues of controlling the lawfulness of data processing and, on the other hand, it represents the measures implemented in terms of raising public awareness as well as in the educational direction. In addition, for the purpose of international institutional acknowledgement of the Service, the report presents the activities performed on the basis of analytical function and the strategic development of different sectors and considers the key role of the Service in the development of law on personal data protection as a separate branch of law. The statistical data with relevant indicators reflecting the activities conducted by the Service during the year are provided as an annex.

THE INTERNAL ORGANIZATIONAL REPORT, that deals with the issues related to the Service management and presents the activities performed at the internal institutional level during the year. The organizational structure of the Service, the certain issues regarding the management of human resources, and the internal organizational documents adopted to improve the quality of the Service are also presented in it.

THE FINANCIAL REPORT that offers the financial situation of the Service and the budget utilization rate.

THE CONCEPT OF STRATEGIC DEVELOPMENT AND THE FUTURE PLAN FOR STRENGTHENING THE SERVICE, which briefly outline the concept of institutional development of the Service.

CONTENTS:

FORWARD OF THE PRESIDENT OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

On behalf of the Personal Data Protection Service of Georgia, I have the honour to present my first report to the public. It encompasses the collection of salient decisions and activities of the Georgian data protection authority from March the first to December 2022. Additionally, in order to ensure the protection of the fundamental right to personal data, it analyses the challenges facing us and the trends singled out in practice.

The report reviews particular pressing issues related to controlling the lawfulness of data processing, such as: the accessibility of natural person to their own data; the protection of children's personal data; the protection of personal data in labour relations; video surveillance; personal data processing in the sphere of health care; personal data processing in the financial sector; data security. At the same time, the report comprises the precedential decisions of the Personal Data Protection Service of Georgia, important legal definitions as well as the recommendations developed as a consequence of evaluating the process of personal data processing by the representatives of the public and private sector and law enforcement bodies, which aim at the increase in efficiency of personal data protection. The report reflects the scientific or informational events implemented by the Service for the purpose of raising public awareness as well as presents the statistical data of activities of the Service, which along with the other indicators evidence the increase in public referral to the Service, the scalability for the study of the lawfulness of personal data protection and its results. This report will familiarize society with a number of issues relating to the internal organization management of the Personal Data Protection Service of Georgia, the rate of utilization of its financial resources and the information regarding the future vision of institutional advancement and particular priorities of the Service.

The maintenance of an utmost balance between the interests of privacy and public safety represents the fundamental value of a democratic society and the rule of law. The data protection supervisory bodies play a crucial role, on the one hand, in determining the appropriate balance between legitimate interests and, on the other hand, in strengthening the appropriate safeguards to protect the rights of data subjects. Digital identity and personal data processing by means of artificial intelligence are

only a part of the modern processes of the digital age, the epicentre of which represents the data subject and the protection of their fundamental rights. It is thus clear that a number of challenges accompanying the digital transformation increasingly demonstrate the modernized institutional role of the data protection supervisory bodies in relation to the right to privacy and the protection of personal data. Consequently, nowadays, the cognizance of civil society, data subjects, and data controllers as well as raising public awareness of the significance and the best standards of personal data protection have now become an integral part of the strategic objective of data protection supervisory authorities. With the mentioned trend in mind, the Personal Data Protection Service of Georgia intends to improve the culture of privacy and betterment of the quality of personal data protection in the country by adhering to European values.

The European integration of Georgia, the institutional development of the Georgian Law "On Personal Data Protection" and the Personal Data Protection Service of Georgia, as well as the implementation of the effective supervisory function are the primary objectives of me and the staff of the Service.

In order to achieve the above-mentioned, it is the absolute priority for us to bring the activity of the Service in line with European standards, improve the national legislation, and develop the Law of Georgia "On Personal Data Protection".

Our commitment to our work is the main guarantee that the Personal Data Protection Service of Georgia will hold its worthy place in the European family among other counterpart supervisory bodies.

Professor, Dr. Dr. Lela Janashvili

President of the Personal Data Protection Service of Georgia
Professor at Ivane Javakhishvili Tbilisi State University
Visiting Professor at the Autonomous University of Barcelona

PART I

PERFORMANCE REPORT OF THE SERVICE

1. INTRODUCTION

In the modern democratic society governed by the rule of law, the institutional protection of personal data is conceptually dependent on the effective implementation of the mandate of the national data protection authority.

Today, the role of data protection supervisory bodies is not limited only to the consistent oversight of observing the legislation regulating the personal data protection and the adequate response to offences. The public-law function of the data protection supervisory body also includes raising public awareness of rectitude and consciousness and improving the culture of personal data protection in the country.

In Georgia the institutional control over the lawfulness of personal data processing by the data protection supervisory authority was initiated in 2013, while the monitoring of the covert investigative actions and the activities carried out in the central bank databank was launched in 2015. According to the current legislation, from 1 March, 2022 the mentioned function was performed by the Personal Data Protection Service of Georgia as an institutionally independent supervisory body in the field of personal data protection.

In order to control the lawfulness of personal data processing, the Service examines the lawfulness of personal data processing by private and public institutions and law enforcement bodies on its own initiative for the planned or unplanned inspections as well as on the basis of notifications of persons concerned and the applications of citizens. When responding to unlawful data processing, the Service focuses not only on imposing administrative penalties, but also on eliminating the shortcomings identified during the data processing. Accordingly, the Service issues recommendations and mandatory instructions to rectify the deficiencies identified.

In order to monitor the covert investigative actions and the activities conducted in the electronic data identification central bank, the Personal Data Protection Service of Georgia is in a round-the-clock mode provided with the court judgments authorizing such actions, the prosecutor's resolutions on conducting covert investigative actions due to urgent necessity and the resolutions drawn up by law enforcement agencies on conducting the covert investigative actions as well as the notifications from

the electronic communication companies about the transmission of identifiable communication data to law enforcement bodies. The Service verifies the documents received, compares the information displayed in electronic systems, enters the data into the internal electronic system for recording the covert investigative activities and analyses it. It is worth noting, that the Service systematically takes preventive measures including the consultations held with the persons concerned, cares about raising public awareness, organizes informational meetings and training sessions, issues recommendatory documents, and prepares the annual report on the status of data protection as well as on the implementation of covert investigations and monitoring of the activities carried out in the central databank of the electronic communication identification data.

MISSION

The mission of the Personal Data Protection Service of Georgia is to establish the culture of respect for privacy in society, to raise public awareness of personal data protection and to implement the European standards for protection of human rights and fundamental freedoms. In order to harmonize national legislation with international legal instruments and to adopt the best practices, the Service actively cooperates with foreign counterpart supervisory bodies, international organizations and strives to deepen the relationships with them.

VALUES

The activities of the Personal Data Protection Service of Georgia are based on the following values and principles: lawfulness, protection of human rights and freedoms, independence and political neutrality, objectivity and impartiality, professionalism, secrecy and confidentiality.

VISION OF FUTURE DEVELOPMENT

The Personal Data Protection Service of Georgia strives to strengthen and protect the common European values. On the path of European integration, the Service is furthering its institutional advancement, the approximation of the national legislation to the European standards, the improvement of the quality of personal data protection, the enhancement of cooperation with international partners and introduction of the best practices, so as to hold its rightful place among European supervisory bodies of personal data protection.

2. SCHEMATIC OVERVIEW OF ANNUAL ACTIVITIES (MAIN EVENTS)

MARCH

The establishment of the Personal Data Protection Service of Georgia.

The official meeting between the President of the Service and the First Deputy President of the Service with the staff of the authority.

The meeting of the President of Service and the First Deputy President with the Chairman of the Human Rights and Civil Integration Committee of the Parliament of Georgia, as well as with the Heads of various state authorities.

APRIL

The meeting of the President of the Service and First Deputy President with the Chairman of the Legal Issues Committee of the Parliament of Georgia.

Meetings of the First Deputy President of the Service and the staff of the authority with the representatives of the British and US embassies, as well as, USAID/Georgia.

A three-day training on the inspection methodology for the Service staff within the framework of the EU project (TAIEX).

Opening of the cycle of public lectures on personal data protection at Ivane Javakhishvili Tbilisi State University.

MAY

The speech given by the President of the Service at the panel session of the 30th Spring Conference of European Data Protection Authorities.

Signing the memorandum of cooperation between the Personal Data Protection Service of Georgia and the Croatian Personal Data Protection Agency.

The participation of the First Deputy President of the Service and the staff of the authority in various events, including the business meeting relating to the draft law on the amendments to Children's Code as well as in the presentation of the research findings on the "Assessment of Interaction of the Parliament of Georgia with Independent Institutions and Regulatory Bodies".

Conducting the informational training and public lecture on the issues about personal data protection with the employees of the Service participating in it.

The establishment of the first bilingual scientific periodical publication – "Journal of Personal Data Protection Law" by the Service.

JUNE

The Participation of the President of Service in the Global Security Forum (GlobSec) in Bratislava.

The publication of information about the Service in the Global Privacy Assembly (GPA) newsletter.

The publication of the handbook produced by the Service - "Protecting Child's Personal Data in the Digital Environment".

The publication of statistics on the activities of Service for 4 months - 152 applications/ notifications; 38 inspection of lawfulness of data processing; 36 cases of illegal data processing; 18 people were levied with administrative fines and 15 people were issued warning; 49 instructions and recommendations; 1084 consultations; 13 meetings for 490 people; utilization of the suspension mechanism of covert wiretapping and recording of telephone communications in 53 cases.

JULY

Meeting of the President of Service with the Chairman of the Human Rights and Civil Integration Committee and the Chairman of the Legal Issues Committee of the Parliament of Georgia.

Launching the cycle of regional meetings - in the Autonomous Republic of Adjara, Samegrelo and Imereti.

The completion of the training cycle for notaries resulting in 270 notaries having upgraded their qualification in data protection.

The training for the representatives of Special State Protection Service of Georgia.

The participation of Service in the submission of 5th Periodic Report of Georgia on the implementation of International Covenant on Civil and Political Rights to the UN Human Rights Committee.

The Service became the beneficiary of the project of agency "Federal Ministry for Economic Cooperation and Development" (BMZ), German Society for International Cooperation (GIZ) - "Improving public services in the Eastern Partnership countries".

AUGUST

In order to work on further institutional strengthening of the Personal Data Protection Service of Georgia, the participation of the President of Service and the First Deputy President in the first sitting of working group of the Legal Issues Committee of the Parliament of Georgia.

The introductory meeting of the President of Service with the President of Georgia.

Meetings of the President of Service and First Deputy President with the representatives of the non-governmental sector.

The informational meeting in Mtskheta-Mtianeti region within the cycle of regional meetings.

The publication of statistics on the activities of Service for 6 months — 244 applications/ notifications; 76 inspection of the lawfulness of data processing; 70 cases of illegal data processing; 41 persons were levied with administrative penalties, 24 persons were issued warnings; 78 instructions and recommendations; 1646 consultations; 17 meetings for 610 persons; utilization of the suspension mechanism of covert wiretapping and recording of telephone communications in 84 cases.

SEPTEMBER

The presentation made on the 6-month activity report of the Personal Data Protection Service by the President of Service to the highest legislative body, diplomatic, academic corps and representatives of non-governmental sector.

Meeting of the President of Service with the Commissioner for Spanish affairs.

Launching the campaign 'Make it a habit' for the purpose of raising public awareness.

Continuing the cycle of regional meetings in Shida and Kvemo Kartli, Guria region.

OCTOBER

The assignation of the building to the Service to open its representative office in Batumi.

Signing of the Memorandum of Cooperation between the Service and the Italian Data Protection Supervisory Authority.

The working meeting of the President and First Deputy president of Service and the representatives of the Embassy of Georgia in Italy.

The introductory meeting between the President of Service and the Head of International Committee of the Red Cross delegation to Georgia.

The participation of the President of Service in the annual conference of Global Privacy Assembly in Istanbul and meetings with representatives of foreign supervisory bodies.

The publication of the article by the President of Service in GPA newsletter on data protection and gender-sensitive privacy issues in Georgia.

The participation of the First Deputy President of Service in Kishinev in the first regional working meeting held within the project: "Regional Projects on Re-engineering of Public Services and E-governance and Digitalization in the EaP".

NOVEMBER

Conducting the "European Case Handling Workshop" ("ECHW") organized by the Service.

Meetings between the President of Service and the Head of the Supervisory Authority for Personal Data Protection of Bosnia and Herzegovina and the First Deputy President of the Croatian Agency.

The visit of the delegation from the Private Law Research Institute of Kazakhstan.

Holding the training sessions and public lectures on the protection of personal data by the Service.

The publication of statistics on the activities of Service for 9 months - 399 applications/ notifications; 130 inspections of lawfulness of data processing; 129 cases of illegal data processing; 72 persons were levied with administrative penalties, 32 persons were issued warnings; 175 instructions and recommendations; 2868 consultations; 32 meetings for 909 persons; utilization of the suspension mechanism of covert wiretapping and recording of telephone communications in 147 cases.

ECHW

DECEMBER

Awarding the students having won the blog contest.

Granting the Service, the status of observer to the International Conference of Information Commissioners.

Holding the international conference on data protection in the digital world: 'Protecting Personal Data in the Digital World' organized by the Service.

Meeting of the President of Service, the First Deputy President and the Deputy president with the Chairman and representatives of the Business Association of Georgia.

The public lecture -'The Rule of Law and Human Rights' conducted by the First Deputy President of Service at Winter School of the Institute for Development of Freedom of Information in the framework of International Human Rights Week.

The meeting of Service staff with the representatives of Georgian employers, the associations of microfinance and insurance companies and the companies existing in the insurance association.

The informative meetings of Service staff held in public bodies and educational institutions.

3. SPECIFIC TOPICAL ISSUES OF CONTROLLING THE LAWFULNESS OF DATA PROCESSING

3.1. INDIVIDUALS' ACCESS TO THEIR PERSONAL DATA

A natural person's access to his/her own data represents one of the main aims of the data protection legislation and represents the precondition for the exercise of a number of human rights[1]. Despite the fact, that apart from the presence of consent, personal data processing is permitted on the other grounds[2] as well, the individual is often less informed about the actions taken to his/her data. The lack of the mentioned information conditions the ineffectiveness of the data subject's right to appeal in the process of correcting, updating, adding, blocking, deleting and destroying his/her own data as well as, in a number of cases, against the specific facts of data processing[3]. It is worth noting, that the access to one's own data is an important tool for supervising data controllers and bringing the privacy–related processes into the legal realm[4].

One of the effective and efficient measures for exercising the rights of a data subject represents such a legal framework that ensures the access of a natural person to his/her personal data to the maximum. From this point of view, it is worth noting that the national legislation provides a number of clear and predictable provisions. The right to informational self–determination is regulated by Paragraph 2 of Article 18 of the Constitution of Georgia and is echoed by a number of rulings of the Constitutional Court. "The familiarization with the information available in a public entity is an important prerequisite for informational self–determination and the individual's right to free development..." The Constitution of Georgia provides more guarantees for freedom of information and imposes not only the negative obligation on the state not to prevent a person from obtaining information, but the positive duty to provide the information available to him as well.

[1] CJEU, C-434/16, Nowak [2017]; combined cases C-141/12 and C-372/12, YS and Others [2014].
[2] The basics for data processing is lied down in Article 5 and 6 of the Law of Georgia on "Personal Data Protection" and including the consideration of Data protection by Law, the necessity of data processing for the data controller to fulfill the duties imposed by Law, the need to process data in accordance with the Law to protect the salient pubic interests, etc.
[3] Case of Cemalettin Canli v. Turkey, [2008] ECHR App. No. 22427/04, §§ 35, 41-42.
[4] EDPB, Guidelines 01/2022 on Data Subject Rights - Right of Access Version 1.0, 2022, §10.

The Constitution of Georgia restricts the mentioned right only in case the information requested contains the state, professional or commercial secrets [5]." According to the assessment of Constitutional Court: "a person's right to obtain the information about him/her in the public entity does not intend only to read the information or to visually inspect the relevant document. Its purpose is to provide the mechanism that will allow the person concerned to properly and carefully examine the information, investigate its veracity, analyse it and draw conclusions, disseminate and/or utilize it for various legitimate aims"[6]. A person's right to get to know the information held about him/her by a public authority implies the opportunity to become effectively acquainted with that information, which, if necessary, may also include obtaining a copy of the document containing such information.[7]"

The significance of accessibility to one's own data is also referred to in the General Data Protection Regulation (GDPR)[8]. In addition, it is also reinforced by Article 8 of Convention[9] of the Council of Europe from 28 January, 1981 on the "Protection of Individuals with Regard to Automatic Processing of Personal data", in which the entry referred to in Subparagraph "b" clarifies that the Convention recognizes the right of a person to obtain the data concerning him /her in any objectively understandable, perceptible, accessible form at reasonable intervals and without undue delay or expense. The basic norms and principles developed to ensure the exercise of the right recognized by constitutional and international acts are stipulated in Articles 15, 21 and 24 of the Law of Georgia on Personal Data Protection. Besides, Article 18^1 of the Civil Code of Georgia is noteworthy, according to which an individual has the right to get familiar with his/her personal data and records regarding his/her financial or property status or other personal affairs and receive the copy of this data, unless otherwise stipulated by Georgian legislation.

The issues regarding the access to personal data is also regulated by the legal acts of various fields, for example: Article 18 of the Law of Georgia "On Patient's Rights" grants the patients the right to receive the complete, objective, timely and understandable information from the relating to specific

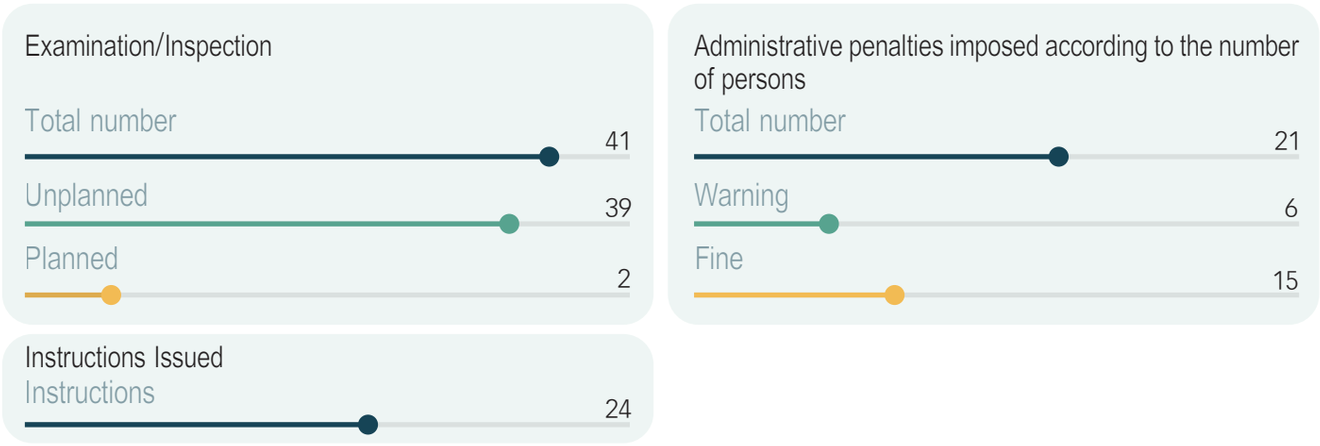
[5] The judgment of the Constitutional Court of Georgia from 14.07.2006 No. 2/3/364 in the case of "Georgian Young Lawyers Association and a citizen Rusudan Tabatadze v. the Parliament of Georgia"
[6] The judgment of the Constitutional Court of Georgia from 18 December, 2020 No. 1/3/1312 in the case "Konstantine Gamsakhurdia v. the Parliament of Georgia", II-10.
[7] Ibid, II-13.
[8] Regulation No. 2016/679 of 27 April, 2016 of the European Parliament and of the Council of the European Union on the protection natural persons with regard the processing of personal data on the free movement of such data (Which repeals the directive 95/46/EC Directive).
[9] Ratified by Parliament Decree No. 2010-II of 28 October 2005.

services and diagnoses. According to Article 71 of the Law of Georgia on "Public Service", a civil servant has the right to get to know his/her personal file and the amendments to it, in case of changing the factual circumstances.

The activities of each individual play the vital role in setting the high standards for the protection of personal data. Accordingly, raising the awareness of individuals and data controllers, and, consequently, ensuring the exercise of data subjects' rights as well as the introduction of effective mechanisms related to informing individuals and their effective use, was one of the main challenges of the Service during the reporting period.

PROCESSES STUDIED

In 2022 the Personal Data Protection Service of Georgia studied 41 (forty-one) cases about the lawfulness of informing a natural person by various authorities, among which 2 (two) of them were conducted on the initiative of Personal Data Protection Service of Georgia and 39 (thirty-nine) of them — on the grounds of citizens' applications/notifications. Based on the cases examined by the Personal Data Protection Service of Georgia, 21 (twenty-one) persons were imposed the administrative liability for committing 21 (twenty-one) offences, (6 (six) of them - for repeated offences). In case of 6 (six) persons the warning was applied as a sanction and 15 (fifteen) persons were fined. In order to improve the course of data processing in public and private entities and ensure their compliance with the Law of Georgia on Personal Data Protection, the Service issued 24 (twenty-four) mandatory instructions in parallel to the administrative fines.



In 2022, the Personal Data Protection Service of Georgia, on its initiative as well as on the grounds of citizens' applications, examined/inspected the facts about the lawfulness of informing natural persons by various public or private entities, in particular:

• *One of the banks.* The institutions frequently use other companies in the course of personal data processing. It is clearly and unambiguously necessary to regulate the relationship between the mentioned institutions so that the data subjects can enjoy their rights in an effective and timely manner. On the basis of an individual's application the Personal Data Protection Service of Georgia, having evaluated the said issue, revealed the administrative offence related to the legitimacy of informing the data subject by one of the banks and the private institution associated with it.

Within the examination, it was established that according to the request of the company rendering postal service, the applicant confirmed the delivery of the message of the bank by a physical as well as electronic signature, then demanded from the same private entity to provide the information in writing about the purpose of processing the electronic signature on the delivery of the document. The investigation revealed that the postal service provider was the data processor of the bank and processed the applicant's data on the basis of the service contract. The inspection did not confirm the fact of notifying the bank about the applicant's demand by the company. At the same time, neither the company nor the bank provided the applicant with any information about the purpose of processing his/her signature in the above-mentioned process.

The Service focused its attention on the content of the service contract, which did not specify the instructions on how the data processor (postal service provider) could act in case of the request for information submitted by a data subject. The bank did not provide any evidence for giving the company such an order or instruction outside the contract. When assessing the case, the Service referred to the definition of the European Data Protection Board (EDPB) that "the data controller is responsible for fulfilling the data subject's request. The contract concluded between the data processor and the data controller shall contain the record of the data processor's obligation to facilitate/encourage the data controller through taking the appropriate technical and organizational measures, to the extent possible". Article 15 of the General Data Protection Regulation (GDPR) was taken into account within the assessment, which defines the data controller's obligation to inform the data subject and consider the obligations of the data processor in the contract concluded with the data processor. The Office also referred to the definition of the "EU Working Party on Personal Data Protection" (so-called "Article 29 Working Party"), according to which the data controller must determine who is responsible for the rules on data processing and how the data subject can exercise their rights in practice.

It should be noted, that Article 21 of the Law imperatively stipulates the data controller's obligation to employ all the possible measures for ensuring the exercise of rights of a data subject including the identification of the risks that may arise in the case of direct relationship between the data processor and data subject, where the request may be submitted to the data processor by an individual, as it happened in this case. Since the requirements laid down in Article 21 of the Law applies directly the data controller and not on the data processor, the failure to provide information to the applicant in the prescribed time limits and in the form requested was regarded by the Service as a negligent breach committed by the bank. Accordingly, by the decision of the President of Service, the fine was levied on the offender who was instructed to immediately inform the data subject, as well as to take such measures which, in the future in case of the data subject(s) making a request for information from the data processor, would ensure the provision of information within the time limit and rule prescribed in the Law of Georgia on Personal Data Protection.

- *LEPL — Levan Samkharauli National Forensics Bureau.* In a number of cases, on the basis of objective circumstances, the natural persons assume that in the public institutions there exist the

materials containing their data, e.g. they personally witnessed the fact of taking photographs or detected the audio-protocol being made during administrative proceedings. However, in the case of making request for materials, they are often provided with ambiguous information and cannot ascertain their own assumptions. The Personal Data Protection Service of Georgia examined the similar case of Levan Samkharauli National Bureau of Forensic Examinations on the basis of a citizen's appeal.

The investigation revealed that the Bureau had conducted the medical examination of the applicant within which the expert had taken photographs of him, which had subsequently been removed. The individual later applied to the Bureau for the copies of photographs showing the injuries existing on his body at the time of medical examination. The response letter from the Bureau, which was forwarded to the data subject within 26 (twenty-six) days, did not notify him/her about the photos requested, but the fact of availability of expert opinion. He was also provided the requisites (date and number) and explained that the Bureau could not give the copy of the said conclusion and the attached documents to any other person without the written consent of the investigating authority that had appointed the examination. The same letter stated that as the expert opinion was one of the pieces of evidence in a criminal case, the applicant could apply to the investigating authority for the transfer of necessary documents or submit to the Bureau the written consent of such authority to hand over the requested documentation. As part of the examination, the Bureau explained to the Service that (based on Article 24, paragraph 1, clause C of the Law of Georgia on Personal Data Protection) the applicant's right to receive information about the photos had been restricted because of the assumption that providing the information would harm the interests of the investigation. In addition, at the time of preparing the letter, the Bureau was informed that the requested photographs had been removed, but in the interests of the investigation the applicant was not informed of this. The examination demonstrated that the Bureau had relied only on its own assumptions in assessing the circumstances of the investigation. Furthermore, there was obtained the response and clarification from the investigating authority having appointed the examination, according to which the applicant was notified that the photographs he had requested had not been attached to the examination report and that providing information about them would not prejudice the interest identified by the investigating authority and the legal benefit. In assessing the case, the Service focused its attention on the fact that the information provided by the Bureau to the data subject did not correspond to the applicant's request for the transfer of

photographs. Furthermore, the said letter to the applicant, who might have had the objective expectation of the availability of documentation containing his data at the office, was not sufficiently informative to determine the existence or otherwise of that documentation. Furthermore, it could not be clear to the applicant whether his right of access to the requested documentation had been restricted because there was a reference to the expert opinion which appeared to lack photographs.

It should be noted that the natural person's right to access documents containing his /her data, guaranteed by Article 21 of the Law, also implies the obligation of the data controller to notify the data subject that the relevant documentation is not available at the institution, or it is deleted due to the expiry of its retention period and/or others. Obtaining the said information helps the data subjects to identify and protect their own legitimate interests. On the basis of Article 24 of the Law, the mere fact of conducting the investigation cannot be regarded as the prerequisite for the automatic restriction of the right. It is important that the data controller's position on the expectation of possible prejudice to the interests of the established investigation is based on the available evidence/information to justify the mentioned restriction. At the same time, the Service considered the time limit used to inform the applicant (26 (twenty-six) days) as unreasonable, since the applicant had submitted the request to the Bureau for specific, identifiable documents. In addition, the response of the Bureau was based only on its own assumption - that the data subject's right to information is restricted due to the ongoing investigation. Thus, the Bureau has violated the requirements laid down in Article 21 of the Law and the data controller has been imposed the liability for the administrative offence envisaged by Article 50(1) of the Law of Georgia on "Personal Data Protection". In addition, in case of missing the documentation containing data, the Bureau was instructed to inform the data subjects within the reasonable period of time, at his/her request for them. Also, pursuant to Article 24, paragraph 1, sub-paragraph C of the Law of Georgia on Personal Data Protection, the Bureau was instructed not to rely solely on assumptions in case of restriction of the data subject's right and thoroughly examine the available information and all the evidence, including the possibility to contact to the relevant investigative authority on the matter, so as to assess the relation between the requested documentation or information and the interests of the investigation.

- *LEPL — Animal Monitoring Agency.* The applications presented to the Service often relate to the facts of informing data subjects in the unreasonable time and/or incomplete form, which

should be regarded as the violation of statutory standard. Based on a citizen's application, the Personal Data Protection Service of Georgia investigated the similar case regarding the lawfulness of informing the applicant by LEPL –Animals Monitoring Agency.

Based on the analysis of evidences obtained, it was established that the applicant had not requested the information about processing the video recordings in general, but about the fact of viewing the video recordings and/or transcribing the copy by the representatives of the Agency, to which the detailed response was not provided by the Agency in its letter. In addition, it was revealed that the case materials preserved by the Agency contained the video recordings reflecting the applicant's data, which had not been provided to the data subject despite his/her request (the Agency submitted the said material to the data subject later, in response to the repeated request). Thus, it was found that the Agency had provided the incomplete information to the applicant. Pursuant to Article 21 of the Law, the data subject is conferred the right to receive the requested information within ten (10) days. Although the same rule does not specify the time limit for providing the natural person with copies of documents containing his/her data, it was clarified in the course of evaluating the case that the data controller must act within a reasonable time frame in each case. Taking into account the circumstances of the case, the request and the amount of material (one sheet and five audio files), the time limit used by the Agency to respond to the applicant's request, moreover, the provision of requested information/documentation in the incomplete form was assessed as unjustifiably long period – unreasonable term. It is worth mentioning, that the untimely provision of information/documentation of one's own data may inflict the considerable damage to the data subject, as after a certain period of time the information loses its value and the data subject loses interest in obtaining this information. Thus, the Agency violated the requirements laid down in Article 21 of the Law, for which the data controller was imposed the fine for administrative offence under Paragraph 1 of Article 50 of the Law of Georgia "On Personal Data Protection".

- *NNLE — National Youth Palace.* There are trendy cases when parents make a request for the information about minors' data from various institutions, and apply the Service for the evaluation after having been responded. Every decision concerning minors, including the transfer of personal data about a child to his/her legal representative, must be made with the best interests of a child in mind. In order to protect the child's privacy, family life, dignity, well–being, safety and other rights, the requirements of

the law must be strictly observed. On the grounds of a citizen's application the Personal Data Protection Service of Georgia assessed the similar case while examining the lawfulness of informing the applicant by NNLE – National Youth Palace.

The evidences obtained about the case demonstrated that the child's parents were divorced and the child lived with the mother. The days and hours for visitation of the child's father was determined by the enforceable court decision, however, its annulment was disputed in court by the minor himself. In addition, the act of conciliation approved by Court regulates the mother's obligation to provide the father with information about the minor's school activities. However, it should be noted, that the information requested by the applicant from the public entity concerned the extra-curricular activities. Within the examination, the explanations of the juvenile data subject, his mother and lawyer as well as the representative of the National Youth Centre confirmed, that the applicant's request for obtaining the information did not coincide with the data subject's will and that the child himself was against forwarding the information and documentation containing his data to the applicant. In this case, it was also revealed that the applicant requested the data on his son in order to exercise his parental right, however, the dispute over the child-parent relationship was ongoing in court on the child's initiative. In addition, the issue of providing a number of details of the child to the parent was regulated by the act of conciliation approved by the court.

In the decision made on the case, the attention was focused on the circumstances according to which the parent and the child represented the individual data subjects. At the same time, the parent is the legal representative of the child, however, the data of the minor cannot be considered as the data about a parent. As a consequence, the investigation revealed that the interests of the data subject to be informed is protected by the Law of Georgia on Personal Data Protection, accordingly, it stipulates the obligation of data controller – to provide the personal information to a data subject or a representative acting in defence of his/her interests. But in the said case it was not singled out whether the request for information served the purpose of the minor to be informed about the data processing. Consequently, the application to the public authority as that of the legal representative of the child was not equated to the application of the data subject (the child) himself/herself. Upon taking decision the will of the data subject (the child), who refused to provide the parent with his/her data, was taken into consideration as well. Occasioned by the fact that the request made by the juvenile data subject under Article 21 of the law was not identified, no

restriction of the right to provide the information by the public entity was demonstrated.

- *LEPL — International Education Centre.* Frequently, the prerequisite for the first exercise of a data subject's right to be informed is the correct assessment of the information requested in relation to the data subject, and it is especially important that the restriction of the right to information is not the rule, but the exception, on which the Service targeted the particular attention. On the basis of a citizen's application, the Service assessed the mentioned circumstances when examining the lawfulness of the provision of applicant with information by the International Education Centre.

During examining the application, it was stated that the contestant had requested from the Center the information on the scores awarded to him, as a participant in the scholarship program, according to the evaluation criteria by each member of the competition commission, indicating their identity. In response, the Centre provided the applicant with the specified information, but the identity of the assessors was concealed in the document. The contestant pointed out, that the identity of commission members was the part of the decision taken about him, accordingly, it represented his/her personal data and he/she was entitled to receive it. Furthermore, the scores given to him/her by the different members of the commission varied significantly from one another allowing the applicant to assume that the commission members were biased and incompetent. From the applicant's viewpoint, the identity of each member of the evaluation panel, considering that person's background and reputation, would clarify whether the commission's assessment was competent and impartial.

As part of examination of the application, the Centre indicated the protection of the interests of other individuals as the grounds for restriction of the data subject's right to information (Paragraph 1(e) of Article 24 of the Law). He noted that in case of disclosure of requested information there existed the possibility to use and publicly disseminate (e.g. via social media) the abusive, humiliating and/or threatening messages towards the commission members having given a low assessment by the contestants who were dissatisfied with scores. This, in turn, could have had an undesirable impact on the objectivity of the competitive evaluations and on the ability of commission members to openly and honestly express their assessments. Within the inspection, it was revealed, that the applicant could obtain full information about the names, areas of work and positions of the members included in the competition commission

via the website of the Centre, which would allow him/her to gain insight about the fairness, competence, and impartiality of the commission. In addition, according to the rules of the commission, the immediate identification data of a contestant must not be available to the commission members/evaluators.

Upon assessing the case, the Service shared the interpretation of Centre on the risks relating to disclosing the identity of particular commission members to the contestants and considered that in this case the failure to provide personal data did not constitute the breach of the law. However, the Centre was instructed that the applicant should be provided with clearer and more detailed information on the reasons for restricting the right than they were reflected in the relevant letter. Thus, by the decision of the President of the Service, on the grounds of preventing the violation of rights of other persons, in case of restricting the right envisaged by Article 21 of the Law of Georgia on Personal Data Protection, the Centre was instructed to provide the data subject with all the information about the factual and legal grounds for the decision on restriction of the right, whose transfer to the data subject will not prejudice the purpose of its restriction.

- *Office of the public defender of Georgia.* There exist occasions when data subjects make a request for the documentation containing their personal data in the form they like, such as in digital or paper format, certified in the manner prescribed by the legislation, and others. It is worth noting that the documentation is often voluminous and data processing agencies are free to choose the clear form and method of submitting materials. The Personal Data Protection Service of Georgia assessed the mentioned issue within a citizen's appeal submitted to the Ombudsman's Office.

The review of the case stated that the files placed on CDs were not damaged, they were readable and could be opened on the personal computer that was not equipped with any special, hard-to-reach software. In the decision of the President of Personal Data Protection Service there is pointed out that Article 21 of the Law does not provide the data subject with freedom to choose the form, in which the copies of documents containing personal data are obtained. The obligation imposed on the public authority shall also be considered as duly performed if the data subject is provided with copies of the documents containing his/her data in any accessible, perceptible form and within the reasonable time. Thus, no breach of law was found in this case.

- *LTD "Centre for Mental Health and Prevention of Addiction".* There are occurrences when the institutions restrict the access of natural persons to their own personal data on the grounds that the material has been provided periodically or previously and in another context. The misuse of grounds to restrict the data subject's right to be informed is also common. Exactly the similar issues were examined by the Personal Data Protection Service of Georgia on the basis of a citizen's application when assessing the case of informing the data subject by the Centre for Mental Health and Prevention of Addiction.

In consequence of inspection it was stated, that in the case at hand, the applicant's request served his/her interest to obtain information about the still unknown process (the response to violence against him) to him/her related to processing of his/her own data, which was important for familiarizing himself with the content of the specific document containing the data. Although a part of the case file reflected the correspondence with the applicant at various periods, which was periodically provided to the data subject, the case in question should not have been equated with the data subject's repeated requests for documents containing the data made at unreasonable intervals. In the decision of Service, it was pointed out, that the access to material containing one's own data also extends to the internal departmental documentation, which may be made available to the data subject with masking the data of other individuals. As regards the limitation of the right referred to in Article 24 of the Law, the data controller should importantly verify the existence of the relevant grounds through using the available means. For example, if there is possibility that transferring of the requested document to the data subject may interfere with the detection and investigation of a crime. The mere fact that he /she lacks the sufficient competence to assess the issue should not become the legal ground for restricting the right, as the mentioned can be clarified, for example, by contacting the relevant investigative body. The Service assessed the reasonableness of the period used to reply the applicant and deemed that, given consideration to the activities carried out by the institution as well as based on the purpose of the data subject to be informed, the time interval to reply (105, 75 and 26 days) could not be considered as the reasonable period needed to reply. It is worth noting that the law does not set the specific time limit for documents containing data, however, in each case, the data subject's interest and need for the information to be accepted as well as the entry of Subparagraph "b" of Article 8 of the Council of Europe Convention of 28 January 1981 for "Protection of Individuals with regard to Automatic Processing of Personal Data" shall be taken into account in

determining the time limit. The Convention indicates the obligation of the data controller to inform the data subject without undue delay. By the decision of the President of the Service, given the untimely informing of the data subject, the Centre was levied the fine and instructed to provide the applicant with the documentation containing his/her data.

- *Tbilisi City Hall.* The data controller's statutory obligation to provide relevant information to the data subject also applies the cases where the applicant's request concerns the specific data that is not processed by the agency, although the agency processes other data about the applicant. The Personal Data Protection Service of Georgia inspected the similar issue on the basis of a citizen's application within the scopes of reviewing the lawfulness of informing the applicant by Tbilisi City Hall.

In the course of examination, it was stated that the applicant lodged the statement against the construction of unauthorized boom barrier to the Town Hall. And then, on the ground of the additional application he/she asked for justification of the disclosure of his personal data included in the notification (according to the applicant, the fact that he had submitted the notification to the Town Hall had been disclosed with the Home Owner Association (HOA)). The Mayor's office responded to the applicant's appeal by the letter, but provided the information about the measures taken in connection with the construction. According to the Mayor's office, their letter did not provide the specific response, because no disclosure of the data had occurred, so it was not obliged to indicate any circumstances.

According to the assessment of the Service, it is important that even if the data controller does not process the applicant's data in a specific way, the data subject must be informed about it within the statutory deadline. The mentioned is informative for the individual because he/she gains the insight into how lawfully his/her data is being processed, who has the possibility to access it, and helps to identify and protect his/her own legitimate interests. Thus, even if the release/disclosure has not occurred, ignoring the data subjects' request deprives them the opportunity provided by Article 21 of the law to obtain the specific response from the data controller about the actions taken with respect to their data and to assure themselves of the validity or otherwise of their own assumption. Considering the above mentioned, the Mayor's Office was held to be in breach by the decision of the President of the Service.

- *One of the companies.* During the reporting period, there was a case where on the basis of ongoing court proceedings the data controller considered to be exempt from the obligation to inform the data subject.

Within the examination it was stated that the applicants had requested the company for information about processing their data. The company sent them the response letter within the statutory deadline, but informed them that the applicants' data were being processed for litigation purposes, due to which the law did not apply the company pursuant to Article 3, Paragraph 3, Sub-paragraph – b of the Law of Georgia on Personal Data Protection.

The review of the application revealed that the company had been processing the applicants' data as part of ongoing proceedings. Accordingly, their data was processed in another form (through submitting it to the Ministry of Finance of Georgia). Having regard to the above mentioned, under Article 21 of the Law, the company was obliged to provide the applicants with details of processing their data or under Article 24 of the Law to notify the applicants of the restriction of their rights, in case of existing its ground envisaged by Article 21. Accordingly, the position of company regarding the scope of application of the law was not shared. By the decision of the President of Service, the institution was found to be in breach of the requirements laid down in Article 21 of the Law and the fine was imposed on it. In addition, the company was instructed to inform the applicants of processing their data within one (1) week following the submission of the decision.

MAIN TRENDS AND RECOMMENDATIONS

The Service carried out a lot of activities to implement the access of natural persons to their personal data, including training sessions for different target groups (children, students, professional representatives, civil servants, etc.) and also dealt with a number of applications regarding the lawfulness of informing the data subject. Within the framework of the applications and inspections, in the process of providing access to personal data for natural persons, the facts of failure of performance or the improper performance of the duties imposed on them by law were identified in both public and private entities, which were responded to, and along with the arrangement of cases there were clarified the salient issues for the future practice of data controllers, namely:

✓ There have been singled out the facts of handing over the documentation to the data subject within the unreasonable period. It is true that personal data protection legislation does not envisage the specific time limit for the transfer of documentation, but the absence of legal regulation cannot be used as the means of misusing and making the right illusory on the part of data controllers. Thus, it is important that when transferring documents containing information, data controllers take into account the nature and volume of the material requested and transfer it within the time frame that is objectively necessary to process the documentation of relevant specificity;

✓ The examined processes highlighted the tendency towards the violation of the 10-day deadline for transferring the requested information envisaged by law. It is worth noting that the 10-day period set by law for the proper exercise of the right is the reasonable and objective timeframe to collect even a large amount of data and transfer it to the applicant. In order to comply with the term, it is important for data controllers to delegate power between the employees in such a way that the lack of human resources does not become the reason to limit the rights of the data subject. In addition, in case of transferring several independent information of large volume requested by a single application, with the aim to ensure a timely response, it is expedient to allocate these requests to the relevant actors, so that each request is processed within the time limits prescribed by law;

✓ One of the problems identified is informing a person about the unavailability of the requested information/documentation for the data controller. The Service emphasizes that informing the data subject of the presence or absence of information/documentation in various institutions is the right with the same significance and guarantees of legal protection as the data subject's availability of information and documentation about him/her preserved in the relevant institution. Thus, it is essential for data controllers to approach the issue of informing data subjects about the lack of information/documentation in the institution with the appropriate standards and try sympathetically to inform the applicants about the actions related to their own data;

✓ It is important that data controllers do not use the vague statements provided by individuals as a means of evading their legal obligations. The controller's obligations related to informing the subject inherently include the duty of institution to provide the reasonable assistance to individuals in exercising the right to informational self-determination and to enable the clarification of unclear requirements;

✓ In some cases, the rights envisaged by Article 21 of the Law are restricted without providing sufficient information to data subjects. The existence of appropriate grounds for restricting the right at the legislative level does not mean that they can be used arbitrarily and formally. Even in case of existing the relevant grounds for refusing the transfer of information/documentation, it is important for the data controller to take into account the current situation, ensure that the data subject is informed as much as possible about the grounds for the restriction in such a way, that the interest of the restriction itself is not harmed;

✓ The processes studied demonstrated that in a number of cases, when the data subject makes request for the information/documentation of his/her data, the data controllers refuse to meet the request despite the fact, that the mentioned information has been in full or in part submitted to the data subject some time before. Most importantly, data controllers must not automatically refuse to satisfy data subjects when evaluating their request for the retransmission of information/documentation. They should first examine the timing of the last delivery of the information/documentation requested

and make the appropriate decision following the reasonable assessment of the time passed and changes in circumstances;

✓ In order to ensure access to personal data for individuals, the importance is attached to the proper perception and evaluation of the concept of personal data and its content on the part of data controllers. When regarding any information as personal data, the controller must be guided by several specific elements of the concept of personal data and not interpret them so narrowly as to be detrimental to the protection of rights. When attributing the information to an individual's personal data, the means of constantly developing modern technologies must also be taken into account;

✓ In the course of inspecting the cases of lawfulness of informing, the Service identified the shortcomings in the distribution of rights and responsibilities between data controllers and processors, that make it difficult for them to duly fulfil their obligations towards data subjects. In each case it is important that the data controller adequately ensures the risks associated with the submission of requests to data processors by data subjects. This can be implemented, for example, through the agreement on detailed instructions between the institutions.

In the legal literature, the concept of modern state implies "new qualitative attributes, new aspects of governance and it is not perceived only as a hierarchical system..." [10] "In the governance process, the focus is shifted to the quality of the service and the extent to which the citizen is satisfied with that service.[11] " The public administration starts exactly with making decisions towards every member of society. In terms of the transparency of its activities, the institution is accountable not only to the public, but also to each individual. Accordingly, in the case of access for each member of society to the data processed about him/her at the institution, the data subject is given the opportunity, if necessary, to contribute to the process of the effective exercise of not only his/her individual, but also to the rights granted to each member of society, through the appropriate legal response. For

[10] *Khubua G., Kalichava K.,* Handbook of the Administrative Sciences, the Issues of the Institute of Administrative Sciences at TSU, Volume IV, 2018, 38, Ref.: Benz, Kooperative Verwaltung. Funktionen, Voraussetzungen und Folgen, 1994.
[11] Ibid, Knorr, Ökonomisierung der öffentlichen Verwaltung: einige grundsätzliche ordnungstheoretische Anmerkungen, 2005.

the proper exercise of the right, it is important that data controllers act responsibly for the obligations imposed on them and do not use the exceptional cases envisaged by the law as the way to avoid them [12]. In some cases, the achievement of necessary standards requires data controllers to develop the work plan, structure or instruction regarding the request for information or documentation, so as to minimize the risks of inefficient and untimely responses to the data subject [13]. In addition, data controllers should ensure training and raising awareness of those persons responsible for providing information, so that the request submitted by a data subject for the transfer of information or documentation is followed up with an adequate and timely response in each case.

[12] Case of K.H. and others v. Slovakia, [2009] ECHR App. No. 32881/04, §§ 44-47.
[13] Case of Roche v. The United Kingdom GC, [2005] ECHR App. No. 32555/96, § 167.

3.2. PROTECTION OF MINORS' PERSONAL DATA

The right to privacy of minors necessitates particular protection[14]. Under the conditions of technological advancements, the protection of this right has even more grown in salience as the dangers of unlawful interference with the right to privacy increases in line with the new opportunities[15] . And children have less information about the negative consequences of processing personal data and are often unable to utilize the mechanisms of data protection on their own to protect their rights. The violation of the right to privacy can cause irreparable harm to a child's psyche, development, social relationships and further life [16]. Therefore, in terms of protecting the personal data of minors, the considerable responsibility falls on those institutions and entities which collect a large amount and sensitive category of data on them.

The 1989 UN Convention on the Rights of the Child and the 2019 Georgian Code of Children's Rights oblige the state to have regard to the best interests of the child within its decision-making process. Protecting the interests of minors is a matter of the utmost importance in the EU legislation and practice on personal data protection. The General Data Protection Regulation (GDPR) emphasizes, that minors need special protection because they may not have sufficient information about the rights, risks and consequences associated with their data processing. It should be noted that the draft Law of Georgia on Personal Data Protection [17], initiated in the Parliament of Georgia, ensures the higher standard of protection of the rights of minors as compared to legislative acts in force. Accordingly, the adoption of this law is of paramount importance to ensure the high level of personal data protection, including the improvements in minors' data protection.

One of the priorities of the Personal Data Protection Service of Georgia in 2022 was the protection of personal data of minors. Occasioned by the mentioned, minors have been considered as one of the target groups in "The 2022 Plan for the Planned Examination (Inspection) of lawfulness of

[14] Case of Söderman v. Sweden GC, [2013] ECHR App. No. 5786/08, § 81.
[15] UN Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to the Digital Environment, 2021, § 67.
[16] Case of N.Š. v. Croatia, [2020] ECHR App. No. 36908/13, § 99.
[17] The Draft Law of Georgia on Personal Data Protection, N07-3/353/9, 22.05.2019.

Personal Data Processing" approved by Order № 01/23 of the President of Personal Data Protection Service from April 7, 2022. Consequently, the Personal Data Protection Service of Georgia examined a number of cases of minors' personal data processing and implemented various activities (including seminars, trainings etc.) within the planned audits as well as on the basis of citizens' requests, which intended to raise public awareness and that of the persons responsible for children's data processing.

PROCESSES STUDIED

In 2022, the Personal Data Protection Service of Georgia examined 39 (thirty-nine) cases of processing personal data of minors, 27 (twenty-seven) of which were initiated by the Personal Data Protection Service of Georgia and 12 (twelve) of them were carried out on the basis of applications/notifications from citizens. The applications submitted to the Service mainly concerned the unlawful disclosure of the personal data of minors by the medical institutions, the breach of rules on video surveillance, the irregularities occurred in data processing for direct marketing purposes and other facts.

Based on the cases examined by the Personal Data Protection Service of Georgia, 19 (nineteen) persons were held administratively liable for committing 20 (twenty) offences. Warning was applied to 9 (nine) persons and 10 (ten) persons were levied a fine in the form of sanction. In parallel to administrative penalties the Service issued 2 (two) recommendations and 44 (forty-four) mandatory instructions with the aim to improve data processing in public and private entities and ensure their compliance with the Law of Georgia on Personal Data Protection.

Examination/Inspection

Total number	39
Unplanned	12
Planned	27

Administrative penalties imposed according to the number of persons

Total number	19
Warning	9
Penalty	10

Instructions and recommendations issued

Total Number	46
Recommendations	2
Instructions	44

In 2022, the Personal Data Protection Service of Georgia on its initiative as well as on the grounds of citizens' applications examined the various cases of children's data processing within implementing the entrepreneurial activities by public and private entities as well as by individuals. During the reporting period, in order to examine the lawfulness of processing of minors' personal data, the Personal Data Protection Service of Georgia conducted the inspections both in Tbilisi and in the regions. The Personal Data Protection Service of Georgia examined /inspected:

- *Vake District Administration of Tbilisi Municipality.* It is worth noting, that a large volume and sensitive category of information about minors is processed by the district administrations of the municipality during recruiting the conscripts for the military registration. In line with the mentioned the risk of illegal processing is increasing. Thus, on its own initiative the Personal Data Protection Service of Georgia examined Vake District Administration of Tbilisi Municipality, which comprised the examination on the lawfulness of minors' personal data processing by the Administration for the purpose of recruitment of conscripts for military registration.

The inspection on the lawfulness of personal data processing stated that for the purpose of the initial registration of minors Vake District Administration of Tbilisi Municipality performs the manual processing of personal data of minors – through obtaining "questionnaires" filled in by students/legal representatives of students, "communication forms", copies of identity cards and birth certificates, photos, as well as well as via electronic system including their collection, utilization and storage. In addition, the inspection revealed that the electronic system, through which the initial registration of minors as well as data processing for the purposes of conscription for military service are carried out, is administered by the structural unit of the administration of Tbilisi City Hall – the Secret Mobilization Service. Accordingly, its data processors have access to the data in the said electronic system.

As part of the inspection, it has been stated that the procedures for primary military registration and the role, powers and documentation to be provided by each entity involved in this process (municipality, educational institution, conscript) are determined by Decree No. 247 of the Government of Georgia of 02 June 2015 "On Approval of the Regulation on Military Registration of Citizens". According to the regulation, the process of obtaining documentation/information from the Board of Management is

regulated in such a way that the documentation of the minor and the data in the application form must be submitted directly to the Board of Management by the minor or his/her legal representative. In addition, the questionnaire also contains the personal data of a conscript that the school is not legally entitled or obliged to possess according to the legislation. As a result of the inspection, it was established that, contrary to the rule stipulated by the regulation, the administration obtained the personal data (such as a photograph) via the school, however, it should have been provided directly by the conscript. In this way, the conscript's personal data became available to the unauthorized persons who had neither need, nor legitimate reason or purpose to access the said data, which in turn increased the risks of unlawful data processing.

The inspection also demonstrated that data was collected directly from data subjects, including questionnaires and "communication forms". However, the Administration did not inform the data subjects to indicate the obligatory and voluntary data in the questionnaire in accordance with the rules enshrined in Article 15 of the Law of Georgia on Personal Data Protection. In addition, it was revealed that the electronic system contained the fields to be filled in (fields for psychiatrist, surgeon, therapist, ophthalmologist and others), the need for which could not be justified during inspection. At the same time, the electronic system did not fully capture all the actions taken in relation to the data existing in the electronic form (e.g., logging in/out, searching/viewing a person's personal data, opening/viewing/copying a downloaded document). The mentioned, in turn, increases the risks of illegal acquisition and disclosure of data, as the possibility of identifying the person responsible for illegal data processing is greatly reduced under the conditions of existing the relevant wrongful events (for example: disclosure of documents uploaded to an electronic system). Thus, by the decision of the President of Personal Data Protection Service, the District Administration as well as the City Hall of Tbilisi Municipality were imposed liability for the administrative offence envisaged by Article 46 (1) of the Law of Georgia on Personal Data Protection on the grounds of failure to comply with data protection requirements. At the same time, in order to eradicate the violations identified, the Administration as well as City Hall were given the mandatory instructions to carry out.

- *LEPL — Centre for Professional Training and Retraining of Convicts.* In order to ensure children's right to privacy, it is important to process minors' personal data, especially the one of sensitive

category, in accordance with legal requirements. And if the issue concerns the disclosure of children's data, consideration should be given to how the publicized data is perceived by the third parties. In the process of disclosing juvenile data, it is especially noteworthy that publicizing of misleading information can even result in the stigmatization of a child in society. This is why, the Personal Data Protection Service of Georgia, on the basis of the request from the non-governmental organization, examined the lawfulness of minors' personal data processing by the Centre through the publication of photos on "Facebook" social network. According to the notification submitted to the Service, the information about the congratulations on Children's Day to the beneficiaries of the Monk Andrew's Charity Fund and other children suffering from oncological diseases, which was attached the identifiable photo of minors, was publicized in the form of a Facebook post.

The inspection of lawfulness of personal data processing revealed that the legal representatives of the children depicted in the photos published by the Centre and other persons had declared their consent to processing of their data. At the same time, besides the beneficiaries of the foundation (children with cancer) the photographic material showed the images of other children and family members of beneficiaries, who were at foundation for various reasons on the particular day. The information made public through "Facebook" by the Centre was therefore misleading, as according to the information indicated in the "post", the representatives of the Centre visited the beneficiaries of foundation. However, within the verification process it was stated, that together with the publicized information the photo material, posted on the social networking site by the Centre, contained the images of other persons apart from the beneficiaries as well. By decision of the President of Service, the LEPL - Centre for Professional Training and Retraining of convicts was instructed to change the information in so called "post" in such a way, that its readers could become aware that the photos attached to the published information showed not only the beneficiaries of the fund.

- *LEPL — Public School №198 of Tbilisi.* This is the resource school that provides general educational activities for students with special educational needs. Thus, the school, given the specific nature of its activities, processes not only so called "regular" category, but also the special categories of data of the students. The legitimate processing of the mentioned information is very important, as the unlawful processing of data of the sensitive category of

minors can have the negative impact on the emotional state of a child and his/her further development. Considering the above mentioned, the Service on its own initiative started the inspection of the school, which included examining the legality of minors' data processing by the public school through creating, storing and transferring the Individualized Education Program to the third parties.

As a result of examining the lawfulness of data processing by the school, the Service stated, that prior to the enrolment of each student in school, the special educational needs of a student were assessed by the multidisciplinary team drawing up the relevant conclusion, which was further sent to the school. The conclusion contained the information about the student's personal data including that of special categories. Based on the information and assessments obtained from the observation of the student by the group involved in Individualized Education Plan (IEP), the school prepared the Individualized Education Program for each student each year. It was also revealed that the school, for example, shared such curricula with other schools in the case of student mobility. As part of the inspection, it was established, that students' personal data were stored both in the physical and electronic forms. The data had been transmitted to those who had the right to access via so called "drive" link, which, if obtained, would have allowed anyone, including unauthorized persons, to access the relevant documents stored on it. In addition, there was a case identified where the "Drive" link was accessed from a computer that was not password-protected. It should be noted that in case of the computer, which is not protected by a password, it is possible for anyone to access the data saved on it. In such circumstances, the necessary data security measures required by Law cannot be ensured. According to the decision of the President of Personal Data Protection Service, in order to share the documents existing electronically, the school was instructed to use such links, which would allow only the specific user(s) to access the shared document(s). In addition, the school was additionally instructed to provide the access to the data existing in the electronic form only from password-protected computers.

- *The teacher of one of the public school.* Every decision concerning minors should be made considering the best interests of a child. The persons caring for children, including teachers, perform the special role in the proper exercise of the right to privacy. Having regard to the above mentioned, on the basis of a request, the Personal Data Protection Service of Georgia examined the lawfulness of taking photos of public school students by the teacher of the same school and the disclosure

of the photo(s) by him/her. According to the information obtained by the Service from publicly available sources, it was revealed that the school teacher had taken the photos of minors kneeling/ squatting during the lesson and sent them to their parents.

As a result of the probe into the lawfulness of data processing by the school teacher, the Service stated, that the public school teacher had taken two photographs of students. In particular, one photo depicted those pupils, who had come prepared for the lesson, sitting at their desks, and in another photo there were captured so called "squatting" students, who had not learnt the lesson. According to the explanation provided by the public school teacher, capturing the situation of punishing students in a photo and sending the said photo to the parents was conditioned by the learning objectives. In particular, he wanted to inform the parents about their children's academic performance, so that they also could feel responsibility. He was sure that such a measure would be the source of motivation for students to learn better. The teacher also pointed out that the mentioned measure had paid off and the students started to improve their learning performance. It should be noted that the students in the photo, circulated in the media, made the impression as if they were in a "kneeling" position. Regardless of whether the children were in the "squatting" or "kneeling" position, in both cases their photograph, given the full context of the photo taken and sent to the parents, emphasized their difference from the students who came to the class prepared. In addition, taking into account the factor that the mentioned condition of students was associated with their poor academic performance, both being in "squatting" and "kneeling" positions were perceived as the violation of dignity. The infringement of a minor's dignity was thus singled out as a counterbalance to the educational objectives set by the educator, which, in turn, constituted the threat of being the victim of oppression of children, so called "bullying", their discrimination and ill–treatment. Giving consideration to the above mentioned, the Service established that when processing the data of students, who were not prepared for the lesson, the school teacher did not observe the principle of data processing without violating the dignity of the data subject. Therefore, the school teacher was held liable for the administrative offence pursuant to Paragraph 1 of Article 44 of the Law of Georgia on Personal Data Protection.

• It is worth noting that minors usually have little information about the harmful effects of illegal data processing and are less aware of the importance of protecting their personal data. In addition, the illegal disclosure or any other kind of data processing about juvenile disciplinary offences can cause the violation of the dignity of a child, his/her stigmatization i.e. "Bullying", discrimination and/or can otherwise negatively affect the emotional state and further development of the juvenile. Thus, due to the fact that schools process a large amount of data on minors through disciplinary collegial bodies and the said process contains the risk of illegal processing of children's personal data, the Personal Data Protection Service of Georgia on its own initiative examined the lawfulness of data processing on disciplinary offences in public and private schools.

The study of the lawfulness of data processing related to the disciplinary wrongdoings by the Service revealed the case, where during processing the data on disciplinary offences the school obtained the amount of data incompatible with the legitimate purpose and no storage period was specified. The inspection of one of the public schools demonstrated that in the process of disciplinary proceedings the reflection of information about the student's social status in the field of violations of the electronic logbook did not serve any purpose. However, the school did not take any appropriate measures to remove information from the specified area and the data processing was only stopped after receiving the relevant information from the Service. At the same time, the school was unable to specify the storage period for the materials of disciplinary proceedings.

As a result of inspection of one of the schools it was also established that data security measures had not been taken when using electronic data processing system in case of disciplinary wrongdoings. In particular, the persons entitled to access the data did not use the individual user name and password. In addition, not all the data operations were registered in the mentioned electronic system. Having regard to the above mentioned, in order to prevent unlawful data processing of minors, the data controller was instructed to determine the amount of data processed in case of disciplinary offence as well as the time limit of their storage and to take the appropriate organizational and technical measures for ensuring the data security.

• *A person's right* to freely use hygienic facilities without others' observation is one of the important guarantees of his/her privacy. Accordingly, monitoring of the data subject in these spaces for any purpose is not justified. At the same time, when it comes to minors' data processing the special attention should be focused on their interests, as even the accidental disclosure of such information could inflict the considerable harm to them. Thus, taking into account the large volume of children in schools and especially the risks associated with processing of private information, the Personal Data Protection Service of Georgia, has, on its own initiative, examined the possible video surveillance in the areas designated for hygiene of various public and private schools (16 schools in total).

As part of the inspections carried out by the Service it was established, that video surveillance was being used in schools to protect the safety of minors. In addition, the inspections of public schools have revealed, that the body responsible for the security at schools is also represented by LEPL – Office of the Educational Institutions Mandatory, which together with the school is engaged in the process of implementing video surveillance. Several cases were identified where the area designated for hygiene (a washbasin) was in the view of surveillance cameras (CCTV cameras) located in schools. In a number of cases, it was found that in case of the toilet entrance door being left open, the washbasin of the toilet room got in the viewing area of the CCTV cameras located in the corridor. It is true that hygiene areas usually have doors that close, but as minors are less aware of the risks to their privacy, they may leave the front door open when using the mentioned space and their actions in the hygiene area may be caught by the surveillance cameras. The inspections revealed the infringement of law as well and, in a number of cases, considering the best interests of a child and in order to prevent the violations against these minors, schools were given mandatory instructions to carry out.

• *One of the private hospitals.* The health-related data include particularly sensitive information about a person's private life, mental and physical condition. The unlawful acquisition, disclosure or other data processing of a similar nature about an individual may not only be a violation of privacy but also the cause of indignity, stigmatization or discrimination. Thus, the confidentiality of health-related data necessitates special protection. This is why international and Georgian Law sets high

standards and safeguards for the protection of health–related data. On the basis of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of the information disclosed by the director of the hospital in a telephone comment to a television company, which concerned the health condition of the applicant's deceased son (including the congenital disease, treatment procedures performed, etc.). According to the applicant, his deceased minor son had overcome the health problems listed and disclosed by the hospital director and had been fully rehabilitated a year and a half before the telephone comment. Thus, the surgeries and other congenital health problems listed by the doctor had no relation with the health condition and death of the applicant's son.

According to the information provided by the hospital in the process of examining the lawfulness of data processing, the provision of information in telephone commentary served to protect the interests of the hospital, because the child's parents and family members had disseminated the inaccurate information via the media. The patient had many comorbidities from birth which, all together, further resulted in the minor's death. Thus, the purpose of the disclosure of the information referred to in the Medical Director's telephone commentary on behalf of the hospital was to protect the reputation of the hospital and to provide the public with accurate information on the matter. Within considering the application, the Service stated, that the hospital had no need to disclose that extent of the data, as it was done in the telephone comment by the Medical Director of the hospital. As part of the inspection, the hospital was able neither to justify the need for disclosure of detailed information, nor the reason why only the general reference to the child's health status would not suffice to achieve the objective of the hospital. Occasioned by this, the data publicized by the hospital director was not considered as adequate and proportionate. By the decision of the President of the Personal Data Protection Service of Georgia, the hospital was held administratively liable for the administrative offence under Article 44, paragraph 1 of the Law of Georgia "On Personal Data Protection" (Violation of principles of data processing).

- *One of the individual entrepreneurs.* The right to privacy of minors requires special protection, as the violation of this right can cause irreversible harm to a child's future development. And in order to ensure the protection of this right, the importance is attached to the issue of data security. Through the social networking site Facebook, the Service learned that the video footage

of CCTV (Surveillance camera) located in the nursery school owned by an individual entrepreneur, which showed the physical confrontation between the nursery–school children, had been publicized by the parent of one of the children on the social site Facebook. The Personal Data Protection Service of Georgia, on its initiative, started examination of the lawfulness of personal data processing through the CCTV cameras located in the mentioned nursery school.

As a result of the inspection into the lawfulness of data processing by the nursery school, the Service stated that CCTV cameras had been placed inside the nursery school for the safety and protection of minors from harmful effects. The parents/legal representatives of the nursery–school children had access to the data processed through the video surveillance system installed in the nursery school, about which they were informed in writing. In addition, the persons entitled to access the data (including legal representatives of the nursery–school children) did not use the individual login and password. The legal representatives of nursery school children were only able to watch the video in real–time (they could not scroll, download, etc.). However, if they managed to record the video by other means and use it for other purposes, the nursery school had no leverage to control technically the process.

Thus, as a result of the examination of the lawfulness of data processing by the nursery school, the Service found that the nursery school had not taken sufficient organizational and technical measures to ensure the protection of records existing in the video surveillance system from accidental and/or unlawful disclosure. By the decision of the President of the Personal Data Protection Service of Georgia, the data controller was imposed liability for the administrative offence pursuant to Article 46(1) of the Law of Georgia "On Personal Data Protection" (the failure to comply with data security requirements). At the same time, the individual entrepreneur was instructed to take measures for ensuring data security, among them to identify the persons entitled to have access to the data obtained through video surveillance as well as to reflect the powers and duties of parents/legal representatives in the contract concluded between them and nursery–school.

MAIN TRENDS AND RECOMMENDATIONS

In order to raise public awareness of the processing of minors' personal data the Service has implemented a number of activities in accordance with the requirements established by the Law of Georgia "On Personal Data Protection". The cases examined by the Service and the measures implemented clearly show that certain irregularities/deficiencies are identified in the minors' personal data processing by various public and private entities and to prevent such issues in the future it is important to consider the following recommendations:

✓ During the processing of minors' personal data, it was established, that the data controllers had not taken appropriate organizational and technical measures to prevent unauthorized access to minors' personal data, which could create risks of unlawful disclosure of their personal data. In order to ensure data security, data controllers must take the appropriate organizational and technical measures that minimize the possibility for unauthorized persons to gain access to the data;

✓ There have been identified cases where the electronic systems, through which the personal data of minors are processed, do not record all the actions taken on the data. In order to protect data security, it is important to fully record all the actions taken on the data existing in the electronic form with the responsible person indicated;

✓ As a result of examining the processing of minors' personal data, it was ascertained that some data controllers process more data than necessary to achieve the set goal. In addition, in some cases, the controllers have not determined a specific period for data storage. In order to ensure the principle of minimization, it is important for data controllers to define a specific period for the storage of data and the amount of data needed to achieve the legitimate purpose, which, in turn, will reduce the threat of illegal data processing;

✓ There has been detected a tendency, when data controllers share the special categories of minors' data with third parties to an extent they cannot justify the purpose for. In the process of disclosing minors' data, including special categories, it is necessary for the data controller to have

legitimate grounds for such disclosure and throughout this process the principles of data processing, including minimization, must be followed. Depending on the nature of treatment administered to the minors, if information regarding various procedures carried out on them, including surgeries or medical procedures, is disclosed to third parties and publicized in form that is accessible to all, the best interests of minors must be protected;

✔ Every data controller is obliged to respect and protect the privacy and dignity of the child. When processing a minor's data, it is particularly important for data controllers to process the data fairly and lawfully, without violating the dignity of the minor. At the same time, when disclosing information about a child to a third person(s), including the child's legal representatives, the best interests of a minor need to be assessed, as only then can a decision be made on the disclosure of data.

In order to improve the standard of minors' personal data processing, institutions processing children's data and individuals involved in the same process must pay attention to the recommendations outlined in this report as well as prioritize the best interests of a child[18]. For this purpose, it is recommended that institutions develop a policy document on the minors' personal data processing that defines its purpose and necessity as well as the data security issues and standards for the transfer and/or disclosure of data to third parties, among them, sharing the records of a video surveillance system with law enforcement bodies. The information about a person's health status is the basic element of privacy, accordingly, the obligation to maintain its confidentiality is crucial to build the patient's trust in the medical profession and health care services, in general; the above mentioned should also be taken into account in the case of minors[19]. The international standards set out the responsibility of schools for minors' data processing[20]. Additionally, institutions processing the personal data of

[18] Case of N.Š. v. Croatia, [2020] ECHR App. No. 36908/13, § 99; Case of Paradiso and Campanelli v. Italy GC, [2017] ECHR App. No. 25358/12, § 208; Case of Jeunesse v. the Netherlands GC, [2014] App. No. 12738/10, § 109; Case of Strand Lobben and Others v. Norway GC, [2019] ECHR App. No. 37283/13, § 207.
[19] Case of L.L. v. France, [2006] ECHR App. No. 7508/02, §44; Case of L.H. v. Latvia, [2014] ECHR App. No. 52019/07, § 56; Case of Konovalova v. Russia, [2014] ECHR App. No. 37873/04, §§ 27, 41.
[20] CoE Committee of Convention 108, Children's Data Protection in an Education setting, 2021, §§ 7.1.2, 7.3.1.

minors should provide their staff involved in this process with regular training sessions on the issues relating to personal data protection and care for raising their awareness.

3.3. PROTECTION OF PERSONAL DATA IN EMPLOYMENT RELATIONSHIPS

Employment relationships, which include pre-contractual, contractual and post-contractual relationships, are associated with the processing of a large amount of personal data. At any stage of the employment relationship, the employer processes the personal data of job-seekers, current and former employees for various purposes (the recruitment of qualified personnel, signing employment contracts, ensuring the security of the establishment, professional development, fulfilment of statutory obligations, etc.). Among other things the employers have access to the special categories of data, such as a person's health status, criminal record, etc.[21]

Occasioned by the subordination, which is characteristic of the employment relationship, the employee is economically dependent on the employer and represents the so called "weaker party". This relationship between the parties is reflected in personal data processing by employers. In particular, in some cases the employee agrees against his/her will to provide the employer with information about himself/herself that may not be relevant to the employment relationship between parties at all. And the mentioned is in direct proportion to the shortcoming of the employer's legitimate purpose in the course of data processing and implies the abuse of his position. Protecting the confidentiality and security of personal data gained about an employee and processing the data only for lawful purposes in full compliance with the principle of proportionality and legal requirements represent the basic prerequisite for the bona fide employment relationship. Thus, all the employers at any stage of the employment relationship must strike a fair balance between the employee's right to privacy and the legitimate interests of the employer when processing data.[22]

Given the consideration to the volume of personal data processed by the employer, there are usually several people involved in the data processing. They use the information obtained by the employer for the purposes of employment relationship within the scope of their duties. In addition,

[21] Hendrickx F., ILO Working Paper 62 - Protection of Workers' Personal Data: General Principles, 2022.
[22] Case of Barbulescu v. Romania GC, [2017] ECHR App. No. 61496/08, §§ 116-123.

employers often process personal data through various electronic systems. It should be noted that more than one person may have the access to electronic systems.[23] Consequently, in case the adequate organizational and technical measures are not taken to protect the confidentiality of data, there may be posed the increased risk of inadvertent or improper personal data processing.

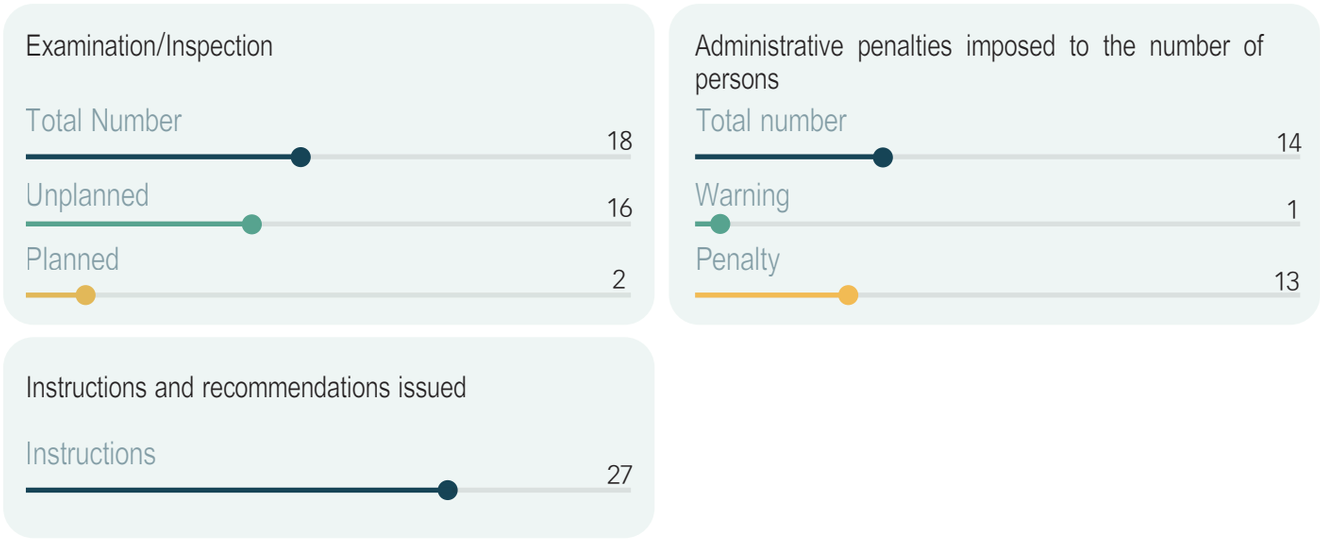
Considering the above mentioned, the protection of personal data within the employment relationship is the particular priority for the Personal Data Protection Service of Georgia. This is why, the Service implemented a number of activities that contributed to the provision of employees with information about the legal requirements for processing of employees' personal data and raising the public awareness.

PROCESSES STUDIED

In 2022, the Personal Data Protection Service of Georgia examined 18 (eighteen) cases of personal data processing within the framework of employment relationships, out of which 2 (two) were initiated by the Service and 16 (sixteen) were implemented on the basis of applications/ notifications of citizens. During the reporting period, based on the analysis of applications and notifications received from citizens, several main issues of personal data processing were singled out in the employment relationship: the disclosure of employees' personal data by the employer to unauthorized persons without a legitimate purpose and with violating the principle of proportionality; the employed person's personal data processing by the employer without the grounds stipulated in the Law of Georgia "On Personal Data Protection"; employees' personal data processing through audio monitoring; processing of employees' biometric data; video surveillance of the employees' workspace and/or hygiene area.

[23] Article 29 Data Protection Working Party, WP 249 Opinion 2/2017 on Data Processing at Work, 2017.

Based on the cases examined by the Personal Data Protection Service of Georgia, 14 (fourteen) persons were imposed the administrative liability for committing 21 (twenty-one) offences. The warning was applied to 1 (one) person as a sanction and 13 (thirteen) persons were fined. In parallel to administrative fines, in order to improve the data processing in public and private entities and ensure their compliance with the Law of Georgia "On Personal Data Protection", the Service issued 27 (twenty-seven) mandatory instructions.



In the reporting period the Personal Data Protection Service of Georgia examined/inspected:

- *One of the companies.* On the basis of a citizen's application, the Personal Data Protection Service of Georgia discussed the lawfulness of disclosing the special categories of applicant's data – sick leave to the third party(s) by the company.

Within the review of application, it was stated that during the paid leave the applicant asked one of the medical institutions for a sick leave due to the deterioration of health condition. The applicant, as an employee of the company, submitted to the company a sick leave letter issued by the medical institution. In the sick leave letter, in the column for "Place of work and position of the sick person" there was not indicated the company as the applicant's workplace but another establishment. Given consideration to the mentioned, the company proceeded on the assumption that the applicant worked at the designated place in parallel and consequently, the original of the maternity leave letter had been submitted to the designated establishment. In order to confirm the authenticity of the document and to clarify the issue of compensation for the applicant's leave period, the company addressed the establishment in writing attaching a copy of the sick leave letter.

The company identified the purpose of providing the applicant's data to the establishment as its legitimate interest – to verify the authenticity of the sick leave submitted by the applicant as well as to obtain information from the establishment as to whether the applicant was simultaneously employed by it and whether he was entitled to the sick leave during a certain period, so as to protect its legitimate interests and request the hospital for the refund of the money paid for the period of sick leave, in addition, to file a lawsuit in court within the statutory time limit.

As a result of inspecting the lawfulness of the disclosure of special categories of applicant's data to the establishment, the Personal Data Protection Service of Georgia stated, that the set goal could be achieved by providing the establishment with less information about the applicant. In particular, in order to achieve its legitimate interest, the provision of the establishment with the information, that the employer had submitted the document, in which the establishment was referred to as the employer, sufficed. On the basis of this information, the company may have specified and requested the information necessary for its purposes. The applicant's sick leave was related to the person's medical condition, which contained the data about the period of incapacity for work and the treatment regime. And the above mentioned represented the special categories of data and its disclosure could not be regarded as the proportionate means of achieving the legal aim.

Thus, the Personal Data Protection Service of Georgia held the company liable for the administrative offence under Article 44(1) of the Law of Georgia "On Personal Data Protection (the violation of data processing principles).

- *One of the companies.* On the grounds of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of the access of the company to the applicant's personal data (personal email).

Within the scope of the review of application, it was verified that the company processed the applicant's personal data by storing it through the computer hard drive (the "Winchester"). In addition, the applicant's personal email address was stored on the memory in a "browser". Accordingly, in case of installing the hard drive disc in the computer, there was possibility for the access to the applicant's personal correspondence at any time. The company cited the protection of legitimate interests as the grounds for processing the applicant's personal data. In particular, according to the explanation of the company, after turning on the computer belonging to an individual, the reasonable suspicion arose that he/she had passed on the confidential information of the company to the rival institution. This assumption was based on the fact, that regular customers had stopped cooperating with the company. Accordingly, the company filed a claim for damages against the applicant, and intended to file a motion with the court for the appointment of forensic examination of the applicant's personal email address. At the same time, the company explained that it had no information about the content of the correspondence existing in the applicant's personal email.

The legitimate interest cited by the company was not shared by the Personal Data Protection Service of Georgia. Considering the fact, that the company, according to its own explanation, had no information about the content of correspondence in the applicant's personal emails, it would be unknown to him whether processing the applicant's personal emails through their storage would be necessary. Having regard to the above mentioned, the company could not have the legitimate interest in processing the applicant's data. Furthermore, it should be noted, that the communication with others is the guaranteed human right, which enables the individual to determine the time, content and addressee of the communication himself and to expect it to be protected against the interference from outsiders.

According to the decision of the President of Personal Data Protection Service of Georgia, the company was imposed the liability for the administrative offence envisaged by Paragraph 1 of Article 43 of the Law of Georgia "On Personal Data Protection" (data processing without the grounds). The company was instructed to delete the applicant's emails from "Hard disc".

- *One of the companies.* On the grounds of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of processing the personal data of employees by a company in order to record the entry to and exit from the building.

Within the scopes of inspection, it was stated that the company recorded the employees' clock- in and clock -out using the card system, in order to monitor their attendance at work. It should be noted that prior to the introduction of the card system, the company processed employees' fingerprints for the purpose of monitoring their entering and leaving the building. According to the representative of the company, it was no longer necessary to collect the fingerprints for that purpose and was converted to the card system.

A legislator is imperative to define the list of data that can be processed for the purpose of entry to and exit from the building. It is worth noting, that the legislative list does not specify the possibility to process biometric data. However, it should be considered that during the inspection, the company itself indicated the need to collect fingerprints. Occasioned by the mentioned, the Personal Data Protection Service of Georgia evaluated the purpose of processing the biometric data, namely fingerprints, by the company as inconsistent with the Law of Georgia "On Personal Data Protection".

Having regard to the above mentioned, by the decision of the President of Personal Data Protection Service of Georgia the company was held liable for the administrative offence under Article 44, paragraph 1 of the Law of Georgia on "Personal Data Protection" (data processing without a legitimate purpose).

- *Town Hall of Khashuri Municipality.* On the grounds of a citizen's application, the Personal Data Protection Service of Georgia inspected the lawfulness of disclosure of the applicant's personal data by Town Hall of Khashuri Municipality.

According to the explanation of Mayer's office, the applicant participated in the civil dispute at the court hearing as a lawyer during working hours without informing the employee. The Mayor's Office was provided by the said information by the person involved in the lawsuit and the appropriate response was required by him/her. Town Hall provided the author of notification with the information about the outcomes of disciplinary proceedings initiated against the applicant and the position occupied by him/her. Within the examination, the Mayor's Office reasoned that the person involved in the litigation was an interested party and the actions of the public official may have had the negative impact on the citizen's trust in the public entity. Accordingly, in order to avoid the reputational damage, the Mayor's Office disclosed the disciplinary proceedings as requested.

In the course of inspecting the lawfulness of the disclosure of the applicant's personal data by Town Hall, the Service regarded the provision of information on the specific disciplinary responsibility and the exact position to the third party as the disclosure of the excessive amount of data. According to the Service, equating the third party with the disciplinary sanctioned person in terms of the access to the detailed personal information unreasonably limited the privacy of the data subject. The legitimate goal, set by the Mayor's Office, could have been achieved by easier means and did not require the provision of specific information about the exact position and disciplinary responsibility of the civil servant. In addition, in order to protect the reputation of administrative authority, it would be sufficient to provide the information on the adequate amount of the disciplinary responsibility/penalty without specifying it and to clarify that the applicant was an employee of the Mayor's Office.

By the decision of the President of Personal Data Protection Service of Georgia, the Mayor's Office has been held administratively liable for the administrative offence enshrined in Paragraph 1 of Article 44 of the Law of Georgia "On Personal Data Protection" (violation of principles of data processing).

- *LEPL – National Agency of Public Registry.* In the employment relationships it is common, when employers, including government agencies, transfer the telephone numbers registered in the employer's name for the use to their employees or offer them to give their consent for registering the telephone numbers they hold in the employer's name, so as to connect the corporate network. Employers, as telephone number holders, retain the right to request the detailed statements about

the telephone numbers they hold from the mobile network operators. This allows them to process a number of employees' personal data directly, using the relevant phone numbers. Considering the above mentioned, the Personal Data Protection Service of Georgia, on its own initiative, requested the information from the mobile network operators about all those institutions which, from 1 February, 2022 onwards, requested the detailed statements of telephone numbers connected to their corporate network from mobile network operators. On the basis of the information obtained, the inspection of the National Agency of Public Registry was initiated, which included examining the legitimacy of the personal data processing by the Agency, through requesting the detailed statements about telephone numbers connected to the corporate network.

Within the inspection, it was established that the Agency requested and received the detailed statement from the mobile network operator on the phone number used by the person working for the Agency, which was recorded on its balance and contained the detailed information of the actions taken with/on the phone number (date of the call, exact time, duration, date of going online, date of receiving/sending short text messages, etc.). As it was explained by the Agency, the need to request the detailed phone number statement was prompted by the assumption that the employee using the number in question might have been involved in the corrupt transaction. Considering the above mentioned, it was important to verify the possible existence of communication between the employee of Agency and two (2) phone numbers.

The Personal Data Protection Service of Georgia regarded the request of Agency and processing of the detailed statement of the employee's mobile phone number as excessive data processing. In particular, the request of Agency for the detailed statement served to verify the fact of communication with two (2) phone numbers of its employee. In addition, the Agency failed to explain the necessity of the request for the detailed statement of the phone number from the mobile network operator and the voluminous information specified in it, in order to achieve the objective set. The stated purpose could have been achieved by processing a smaller amount of data on the employee, in particular, by requesting the information on the communications with two (2) telephone numbers directly within the legitimate interest of Agency.

Thus, by the decision of the President of Personal Data Protection Service of Georgia on the grounds of the request for the detailed statement of the mobile phone number from the mobile operator an administrative offence was imposed on the Agency under Paragraph 1 of Article 44 of the Law of Georgia "On Personal Data Protection" (violation of principles of data processing). In addition to the above mentioned, the inspection revealed that after registering the phone number on the balance sheet of the Agency the persons working for the Agency were not informed, as to whether the employee was allowed to use the number for personal purposes. The employee was not informed that once placed on the balance sheet of the Agency, the activities carried out using the mobile phone would be subject to monitoring. Thus, the Agency was instructed to develop the rules for the use of phone number in the name of the Agency.

In addition to the above mentioned, during the reporting period the breach of legislation was detected by the Personal Data Protection Service of Georgia in several cases examined in terms of the issues about personal data processing within the framework of employment relations:

• Data processing through storing the special categories of data. The Service has conducted an examination regarding the legality of processing special categories of data pertaining to current and former employees, including the documents reflecting Covid-19 and criminal records, by a certain bank. The Service has determined that the bank has retained the special categories of data of both current and former employees for a duration exceeding the necessary period (twenty-five (25) years required to achieve the prescribed legal objectives. Considering the aforementioned findings, the bank was held liable for the administrative penalty for the breach of the principle of data processing pursuant to the first paragraph of Article 44 of the Law of Georgia "On Personal Data Protection".

• Data processing by means of audio monitoring. In one of the cases, the Personal Data Protection Service of Georgia stated that the company was conducting audio monitoring using the portable audio recording devices belonging to employees. Not only the customers of the company, but the employees were subjected to audio-monitoring throughout the working day as well. It is worth noting, that in the course of work there exists such an aspect of the relationship between persons, which is considered as a part of personal life. The employees' data processing in the given form implies the particularly high

degree of interference with their privacy, violates the fair balance between the legitimate purpose of data processing, the interests of the data controller and the rights of the data subject. Thus, the Personal Data Protection Service of Georgia considered the audio monitoring of the employees by means of a portable audio recording device during the whole working day to be the violation of the principle of proportionality of data processing and held the company liable for committing the administrative offence under the Article 44, paragraph 1 of the Law of Georgia "On Personal Data Protection".

• Personal data processing through video surveillance system (CCTV). In the course of the Service's examination, evidence was uncovered indicating that employers had implemented video surveillance systems in locker rooms and hygiene areas. As a result of this finding, the data controllers were subjected to administrative liability and issued instructions. It is essential to recognize that individuals possess an inviolable right to freely utilize these aforementioned spaces without being subjected to external surveillance. This right is safeguarded by the principle of privacy and is protected under the law.

• Personal data processing through electronic systems. Within a specific subset of cases examined during the reporting period, it was observed that employers had neglected to implement adequate organizational and technical measures during the processing of data. Specifically, in numerous instances, the electronic systems employed for data processing lacked the necessary technical capabilities to record all actions executed on personal data. Furthermore, in certain cases, the level of access to the electronic system was either undefined or granted to employees without clearly defined roles and justifiable needs.

MAIN TRENDS AND RECOMMENDATIONS

During the course of personal data processing within the scope of employment relationships, the violations of the requirements of the Law of Georgia "On Personal Data Protection" were identified in both public and private sectors. Considering the variety of ways and forms of data processing, the processing of employees' personal data by employers remains one of the salient challenges. In most instances the data processing is related to the conflict between the legitimate interests of employers and employees, hence, it is important to strike a fair balance between the right to privacy of employees and the legitimate interests of employers. The cases examined by the Service clarify that there have been certain irregularities and shortcomings in data processing in the area of employment relations and in order to eradicate them, it is expedient to consider the following recommendations:

✓ There were identified the cases, when the employers obtained and disclosed more data, including the special categories of data, than necessary to fulfil legitimate purposes. Data controllers must act on the principle of minimizing the amount of data processed and maintain the fair balance between the legitimate purpose of data processing, the privacy of the data subject and the right to protection of personal data in the course of personal data processing. The mentioned implies that the form of data processing chosen by the data controller must be adequate, necessary and effective to achieve the legitimate purpose of data processing. At the same time, the data must only be processed to the minimum adequate extent that will enable the data controller to achieve the relevant legitimate purpose;

✓ The cases were revealed when an employer processed the employee's personal email without a proper legal basis. Communicating with others is the guaranteed human right that allows the individual to determine the time, content and addressee of the communication and to expect that this communication is protected against the interference from outsiders. Data processing during the private communication is the gross intrusion into the privacy of the data subject. Thus, in each case, in order to process data in accordance with the requirements of the law, the data controller must

clearly define the legal basis provided by the Law of Georgia "On Personal Data Protection" and follow the principles enshrined in the same law with absolute precision. Exactly the same ensures the fair balance between the employee's right to privacy and the legitimate interests of the employer;

✓ Within the employment relationship during the personal data processing there were revealed the facts of processing biometric data (fingerprints) of employees without any legitimate purpose. It is crucial to acknowledge that the law imposes high standards for the processing biometric data, allowing such processing only when it is necessary to achieve the purpose(s) specified by the law. This necessity must arise when other means or methods are inadequate, or when a disproportionate effort would be required to achieve the same objective.

✓ An employer was identified to have processed the special categories of data of the current or former employees for a longer period of time than it was necessary to achieve the purpose of data processing. When processing data, institutions are obligated to clearly establish the legal purpose and the specific timeframe required to achieve the designated legal objective. Once the specified timeframe has elapsed and the objective has been attained, the data must be deleted in accordance with the legal requirements.

✓ In specific instances, there were revealed the facts of implementing the video surveillance in locker rooms and hygiene areas and thus processing the personal data of employees by the institutions. It should be deemed that the locker rooms and hygiene areas, depending on the functional load, are particularly private space. Thus, monitoring the data subject in the aforementioned space is unreasonable for any purpose. In addition, when introducing the video surveillance in workplaces, it is essential for institutions to implement the surveillance only in the exceptional cases, after informing all the employees in writing;

✓ In the course of personal data processing within the framework of employment relations, there were identified the facts about the failure of data controllers to take the appropriate organizational and technical measures for the prevention of unauthorized access to personal data. This failure exposes the risk of unlawful disclosure of personal data pertaining to job applicants, current employees,

and former employees. In order to ensure the data security, the data controllers must importantly take the appropriate organizational and technical measures that will maximally limit the possibility of the access to data;

✔ Within the framework of inspections and examined processes implemented by the Personal Data Protection Service of Georgia, it was singled out that in a number of cases the electronic systems, through which the personal data of job applicants, current and former employees are processed, do not record all the actions taken on the data.

Even in the context of employment, an employee retains the right to privacy[24], which places an obligation on the employer to undertake all requisite measures for safeguarding the employee's private life. In addition, in order to raise the standard of data processing in the employment relationship, it is important for the employer to effectively manage each instance of employee's data processing, protect the confidentiality and security of the information obtained, as well as ensure the fair balance between its legitimate interest and the employee's right to privacy[25].

[24] Case of Antovic and Mirkovic v. Montenegro, [2017] ECHR App. No. 70838/13, §§ 40-43
[25] Case of Lopez Ribalda and others v. Spain GC, [2019] ECHR App. Nos. 1874/13, 8567/13, § 116.

3.4. VIDEO SURVEILLANCE

PERSONAL DATA PROCESSING THROUGH VIDEO MONITORING

The presence of video cameras in streets, roads, buildings, public transport, and the ongoing video surveillance has become an integral part of contemporary reality. In line with the advances in technology, the video surveillance systems are used not only by public entities and private organizations, but by natural persons as well. This trend is conditioned by the availability of society members to the technical means, including video surveillance devices, to provide security and protect the property of members of the society. The intensive use of CCTV cameras has the significant impact on the monitoring of individuals' behaviour[26]. It is therefore important that the personal data processing through CCTV cameras is carried out in accordance with the rules laid down in the legislation.

Articles 11 (The video surveillance of streets and public transport), 12 (The video surveillance of public and private buildings) and 13 (video surveillance of residential buildings) of the Law of Georgia "On Personal Data Protection" regulate the data processing through the video surveillance systems. The law exhaustively specifies the purposes for which the video surveillance may be utilized, although the rules vary depending on the specifics of the buildings and premises.

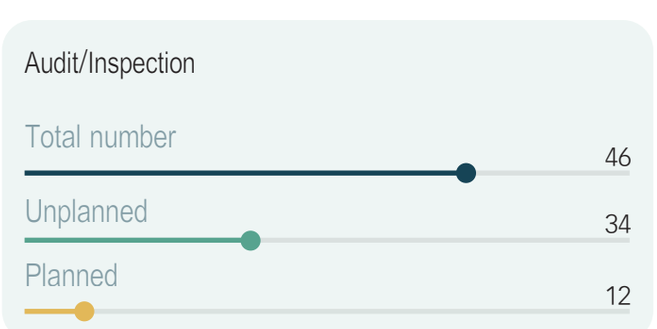
During the reporting period, the Personal Data Protection Service of Georgia implemented the various activities related to the processing of personal data via the video surveillance system. These activities aimed to ensure compliance with the legislation on personal data processing and to raise public awareness.

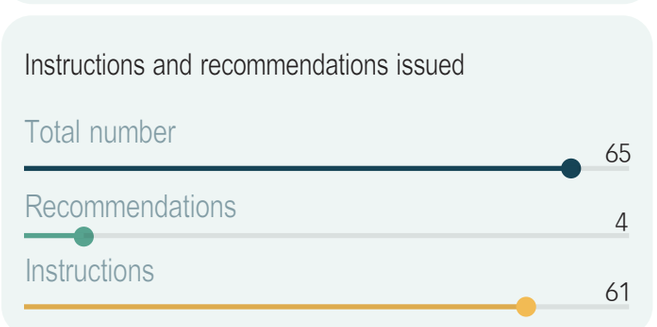
[26] EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices Version 2.0, 2020, § 1.

THE PROCESSES EXAMINED

During the reporting period, the Service examined 46 (forty-six) cases of video surveillance in public institutions and private establishments, which included schools, nursery schools, shopping centres, sports and recreation centres as well as residential buildings. Out of these cases, 12 (twelve) were initiated by the Personal Data Protection Service of Georgia, while 34 (thirty-four) were based on citizens' application or requests regarding breaches of rules on workplace video surveillance, video monitoring of residential premises, apartment/common entrance surveillance by neighbours and the video surveillance of locker rooms installed in shopping centres, etc.

Based on the cases investigated by the Personal Data Protection Service of Georgia, 26 (twenty-six) individuals were found administratively liable for a total of 32 (thirty-two) offences. Out of these, 14 (fourteen) persons were sanctioned with the warning, while 14 (fourteen) persons were levied a fine. In parallel to administrative offences, the Service issued 4 (four) recommendations and 61 (sixty-one) mandatory instructions to improve data processing in public and private entities and ensure compliance with the Law of Georgia "On Personal Data Protection".





In 2022, the Personal Data Protection Service of Georgia, both on its own initiative and on the basis of citizens' requests, conducted the examination of the lawfulness of personal data processing by public and private organizations and individuals through the video surveillance system. The inspection was carried out in Tbilisi and various regions.

During the reporting period, the Service paid particular attention to the examination of the security measures implemented for processing personal data through video surveillance systems as well as the lawfulness of disclosing the video recordings to the third parties. Among them, the Service examined/inspected:

- *One of the institutions.* The inspection, initiated on the basis of a citizen's application, comprised the investigation of the lawfulness of personal data processing through audio-monitoring of the video surveillance system by the institution in the building belonging to it.

As a result of the inspection, the Service determined that CCTV cameras had been installed in the room where several staff members of the institution were on a hunger strike, as well as in the corridors and in the courtyard of the building. The inspection ascertained that the data controller had not placed the appropriate warning sign about video surveillance, so the data subjects were not informed about the rule on video surveillance envisaged by the law.

The inspection also revealed cases of failure to implement other types of organizational and technical measures. Particularly, it was discovered that a single user account was created for the video surveillance system, which was shared among multiple individuals. The device was not password-protected and was accessible to anyone who came into contact with the device. In addition, the physical security of video surveillance system was not ensured, as the video storage device was not installed in the secure room.

The Service assessed the aforementioned facts as the administrative offence envisaged by Articles 46 (the breach of requirements of data security) and 48 (the violation of rules on video surveillance) of the Law of Georgia "On Personal Data Protection", the data controller was imposed the administrative liability and the mandatory instructions to be fulfilled were issued by the Service. In particular, the

institution was instructed to protect the video surveillance system with password as well as to define the individual user and password for the person(s) entitled to access it. The institution was also instructed to place the warning sign of video surveillance in the prominent area.

• *One of the nursery- schools.* The Data Protection Service of Georgia was made aware of the video footage circulating on social media, which depicted the physical confrontation between the nursery-school children. The mentioned video recordings were made public by the parent of one of the minors, who was able to remotely access the video surveillance camera located in the nursery-school. The Personal Data Protection Service of Georgia, on its own initiative, started to examine the lawfulness of personal data processing through the video surveillance cameras located in the mentioned building of the nursery-school.

In consequence of the examination the Service stated, that CCTV cameras had been installed inside the nursery-school for safety and protection of minors from harmful effects. The inspection stated that the parents/legal representatives of the nursery-school children had access to the data processed through the video surveillance system installed in the nursery-school, which they were notified of in writing. At the same time, the persons entitled to access the data, including parents/legal representatives of nursery-school children, did not use the individual user name and passwords. The nursery school teachers were only able to watch videos in real time (they could not scroll, download, etc.). However, if they could record the video by other means and used it for other purposes, the nursery-school technically had no leverage to control the process. Thus, the Service stated that the nursery- school had not taken the sufficient organizational and technical measures to ensure that the CCTV recordings were protected from accidental and/or unlawful disclosure.

According to the decision of the Personal Data Protection Service of Georgia, the data controller was held liable for the administrative offence envisaged by Article 46(1) of the Law of Georgia "On Personal Data Protection" (the non-compliance with data security requirements). At the same time, the nursery school was instructed to take such organizational and technical measures, which would allow to avoid illegal/ inadvertent disclosure, misuse, dissemination and other risks of the data reflected in the recordings. In addition, it was instructed to identify the persons having the right of access to the data obtained by video

surveillance and to reflect the powers and responsibilities of parents/legal representatives in the contract concluded between them and the nursery school.

The problem lies in the legitimacy of video surveillance conducted by private companies in the workplace. In a number of cases, companies could not justify the need for video surveillance of the workplace and the failure to achieve the same goals by other means. There have also been detected the violations of the rule of informing employees about video surveillance in writing and explaining their rights to them.

Based on the applications/notification of citizens, the Personal Data Protection Service of Georgia investigated several cases relating to the video surveillance in the workplace:

- *The private company.* In response to a request from an NGO, the Service initiated the examination of the lawfulness of video and audio monitoring by a private company. According to the information presented to the Service, the video and audio monitoring was carried out over the territory of the company, including locker rooms.

As a result of the investigation into the legality of the data processing, it was determined that the activities of the company represented the manufacture of heavy industrial metalwork of high–risk jobs. In order to protect the property and security, CCTV cameras were placed both on the exterior and interior perimeters of the building. In particular, the working areas, the meeting room and the kitchen located in the production and office area of the company were in the view of video monitoring. It should be noted, that no video surveillance was implemented in the hygiene areas and locker rooms.

It was ascertained that although the employees of the company had been informed in writing about video surveillance in the workplace and their rights, the company failed to justify the need for video surveillance in the office area, meeting room and kitchen. The purpose and risk factors for implementing video surveillance at the above mentioned premises set by the company, such as the possible conflict between employees, the disclosure of information /documentation, negligence, the prevention of theft, were not considered to be exceptional cases prescribed by the law. The above risk factors, as a rule,

accompany the work process. And the use of video surveillance for the purpose of controlling the quality of work performance and the adherence to internal organizational rules and regulations by employees does not comply with the legal requirements and cannot be regarded as the legitimate purpose of video surveillance.

By the decision of the President of Personal Data Protection Service of Georgia, the company was held liable for the administrative offence pursuant to Article 48(1) of the Law of Georgia "On Personal Data Protection", in particular, on the grounds of violating the rules of video surveillance. In addition, the company was instructed to stop video surveillance in certain areas of the building owned by it and to remove the recordings collected by the video surveillance equipment placed in the mentioned areas.

• *Companies organizing gambling games.* During the reporting period, the Personal Data Protection Service of Georgia carried out 2 (two) inspections based on citizens' requests, within which it examined the possible fact of video surveillance implemented in the locker room(s) by casinos in the building belonging to them.

Within the examination of the lawfulness of personal data processing by one of the casinos, it was stated that CCTV cameras had been installed in the employees' locker room of the company. However, the inspection of the video recording server demonstrated, that in fact, no video surveillance was implemented there. The casino was instructed to dismantle the CCTV cameras installed in the locker rooms to simulate video surveillance.

The inspection of the other casino revealed that CCTV cameras had been installed in women's locker room of the company, and according to the company, along with the protection of property and security the purpose of monitoring of the said space was the control over employees. By the decision of the President of Personal Data Protection Service of Georgia, the company was found to be in breach of Article 48 of the Law of Georgia "On Personal Data Protection" for the administrative offence and was instructed to stop the utilization of video surveillance cameras in the mentioned building for controlling the employees.

VIDEO SURVEILLANCE IN A RESIDENTIAL BUILDING

Individuals are increasingly using video surveillance systems in residential buildings to protect their property and personal safety. The Law of Georgia "On Personal Data Protection" does not apply to data processing by a natural person for explicitly personal purposes, when the processing is not related to his/her business or professional activities. However, if video surveillance by a natural person extends beyond his/her personal space and partially covers the public space, it is not considered as the case of data processing for personal purposes and falls within the scope of the legislative regulation. Accordingly, upon installing the video surveillance systems in a residential building by a natural person, it is mandatory to comply with the rules established by the Law of Georgia "On Personal Data Protection". One significant aspect of privacy is a person's right to freely utilize their own living quarters without being observed by others. This means that their movement around the dwelling, the time of entry and exit, and the identification of persons entering and exiting from the residential building should not be recorded. As video surveillance of residential buildings increases the risk of unwarranted intrusion into the privacy of others, natural persons should take into account the interests of their neighbours and the persons living close to them and obtain their written consent to implement the video surveillance of the entrance hall, entryway and common areas of the residential building.

During the reporting period, among the cases examined by the Service in terms of the lawfulness of video surveillance, sixteen (16) out of forty-five (45) were related to video monitoring of residential buildings by individuals. Several cases investigated by the Service in the reporting period were based on data subjects' applications, which revealed the following violations:

- *In several cases examined by the Service, it was established that video monitoring of individuals was carried out in violation of the requirements of Article 13 of the Law of Georgia "On Personal Data Protection" due to the circumstances, that they had not obtained the written consent of the other co-owner(s) of the apartment building, which was qualified by the Service as the administrative offence envisaged by Article 48 (the violation of video surveillance rules) of the law, and the data controllers were instructed to stop video surveillance and/or to implement video*

surveillance in compliance with Article 13 of the Law of Georgia "On Personal Data Protection".

- *Within the review of one of the applications by the Service, the similar case represented the placement of CCTV cameras in a residential building by an individual. It is worth noting that some of the signatories were no longer the owners of the residential building at the time of reviewing the application. Accordingly, due to the fact that the data controller did not have the written consent of more than half of the owners envisaged by the law, the administrative offence was constituted.*

MAIN TRENDS AND RECOMMENDATIONS

The cases examined by the Personal Data Protection Service of Georgia and the measures taken demonstrate the existence of certain irregularities and shortcomings in the process of audio-video surveillance by various public and private entities and the owners of residential premises. As the video surveillance is a fairly intensive form of interference with the right to privacy, it is important that both private and public entities as well as natural persons strictly comply with the law, namely:

✓ During the process of conducting personal data processing through video surveillance the data security is not often protected. Accordingly, at the time of implementing video surveillance by public and private entities for the purpose of protecting the data security, the data controllers must ensure: the physical security of video surveillance system; the provision of the access to recordings to a certain circle of persons; the use of personal login and individual password to gain access to the video surveillance system by persons entitled to recordings; recording all the actions performed on the data existing in CCTV systems, so that the person responsible for any operation performed on the data can be identified; developing the document of internal policy detailing the video surveillance rules and security measures adopted by the organization; the issues about the operation of system, the access to the system as well as the details of those responsible for the system security and others. In the process of implementing the video surveillance by public and private entities, it is necessary for the data controller to ensure the physical security of the video surveillance system. In addition, recordings must only be accessed through using the individual user name and password. It is mandatory to record all the actions taken on the videos footages (who and when viewed them,

scrolled through, downloaded, deleted, etc.).

✔ It has been revealed that the video surveillance in the workplace is often carried out in violation of the legal requirements. In case of video monitoring of workplace, the data controller must comply with the relevant rules laid down by the legislation, in particular, video surveillance of the workplace must only be performed for the purposes of personal and property safety and the protection of confidential information as well as in order to conduct or administer examinations/testing. Video surveillance in the workplace is not permitted for the purpose of monitoring the communication between employees, their attendance at work as well as the compliance with the internal organizational norms of employees. In addition, the employee(s) must be informed in writing of the video surveillance process and their rights.

✔ Frequently, the video surveillance in public and private entities is conducted without the presence of a warning sign. Public and private entities are required to place the warning sign about the video surveillance in a prominent place. The location of the warning sign and the inscription with the appropriate image on it must be recognizable to any person entering the building.

✔ In residential buildings data controllers often have CCTV cameras placed in such a way that not only the entrance of his/her flat but also the common area and the entrance of other owners' houses are captured by CCTV cameras. In the case of video monitoring of a residential building, prior to starting the video surveillance, the data controller must ensure that only the room belonging to the person performing the video surveillance is in the view of cameras. And, in case of surveillance of the common space, the written consent of more than half of the owners is required, also, in case of video surveillance of the room belonging to another person, including an entryway, window, balcony, their written consent is required. In addition, the neighbours must be informed about implementing the video surveillance.

✔ In many occurrences, the natural persons as well as public and private entities install CCTV cameras fictitiously without actually activating them, which misleads citizens and creates the misconception about processing their data. In order to avoid misleading of data subjects, it is

expedient not to install such CCTV cameras.

✔ In each case of disclosure of recordings, the institutions implementing the surveillance should take into account the interests of the third parties reflected in the recording and minimize the possibility of identifying the third parties in the recording (e.g. obscuring the image).

Maintaining the ability to move without being observed and safeguarding the confidentiality of one's behavior and characteristics are crucial aspects of privacy. Accordingly, the video surveillance systems and the organizational and technical measures adopted during their operation, the stipulated storage period for video recordings and the forms of their use as well as other issues relating to processing the data of the persons captured on video footages are mandatory to be in full compliance with the legislation in force.

3.5. PERSONAL DATA PROCESSING IN THE SPHERE OF HEALTH CARE

In compliance with the national and international legislation, information regarding the health condition of a natural person is subject to a high standard of protection due to its sensitive nature. Medical records contain very intimate information about a person's lifestyle, habits, mental and physical state. Their unlawful disclosure may inflict the significant damage to a person's personal and family life, as well as to their employment and integration into society. During a number of trials, the European Court of Human Rights noted the importance of data relating to health status and interpreted that this is the most salient part of the right to privacy guaranteed by Article 8 of the European Convention on Human Rights[27].

In order to preserve or improve a person's health and quality of life, citizens' personal data is processed daily within the range of services provided by the health care sector. The mentioned information is used by outpatient and hospital medical institutions, the representatives of independent medical and nursing practices, laboratories, insurance companies, pharmaceutical companies, dental clinics, as well as the legal persons of public law responsible for the management and administration of the health sector and others. When visiting the health care facility, it is important for the individual to have the sense and expectation for protecting the confidentiality of his/her personal data regardless of the specifics of the service provided. This affects the individual's willingness to receive health care services, as well as the quality of the services received, the health of the individual and the functioning and efficiency of the health care system. Accordingly, the respect and protection of the information about the crucial aspect of an individual's personal life, health information, is important for the individual as well as for the reputation and effectiveness of health care institutions.

Given consideration to the diversity of the health care sector and the importance of protecting a patient's confidentiality, the processing of health information is regulated by various legal acts,

[27] Case of Y.Y. v. Russia, [2016] ECHR App. No. 40378/06, § 38; Case of Frâncu v. Romania, [2020] ECHR App. No. 69356/13, § 52.

including the "Constitution of Georgia", the Laws of Georgia "On Personal Data Protection", "On Health Care", "On Patient Rights", "On Medical Practice" and by other by-laws, such as: Decrees of Georgian Government and normative acts of the Ministry of Labour, Health and Social Affairs of Georgia as well as the international treaties of Georgia and international declarative and recommendatory documents. The protection of data about the health status is of utmost importance in EU legislation and practice on the protection of personal data. The General Data Protection Regulation (GDPR) states that the processing of health-related information is prohibited with certain exceptions. Exceptional cases are the consent of an individual himself /herself, the public interest relating to public health, the need for medical care or social protection and others. Furthermore, even under the conditions of such cases, the General Data Protection Regulation obliges Member States to define the appropriate rules and safeguards for this category of data security at the legislative level.

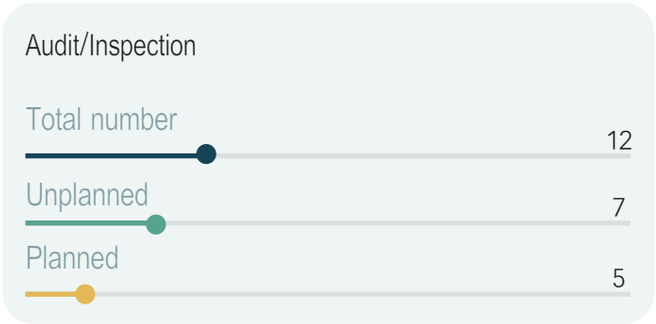
The coronavirus pandemic and the challenges associated with protecting personal data in the process of dealing with the virus as well as the globalization and technological advancements highlighted the need to strike a fair balance between the efficiency of the health care system and the protection of patients' rights. This is why, in 2022 one of the priorities of the Personal Data Protection Service of Georgia was to examine data processing in the health care sector and to protect the patients' personal data along with the proper functioning of the sector.

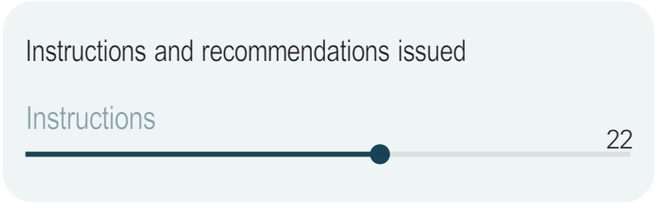
One of the urgent challenges of 2022 represented the protection of special categories of data, including medical information. Resulting from this, in the "Plan of Planned Examinations (Inspections) of the Lawfulness of Personal Data Processing for the Year 2022", approved by Order No. 01/23 of the President of the Personal Data Protection Service of Georgia dated April 7, 2022, processing of medical information was defined as one of the main topics of planned inspections. The same order implied the inspection of various medical institutions and public authorities of health care system (including those involved in the management and administration of social programs). During the reporting period the Service investigated various cases of data processing in the health care sector, both private and public entities, and participated in the events (trainings, meetings) aimed at raising the awareness of the persons responsible for sensitive data processing and, in general, the society.

PROCESSES STUDIED

In 2022, the Personal Data Protection Service of Georgia examined 12 (twelve) cases of data processing in the health care sector, out of which 5 (five) were initiated by the Personal Data Protection Service of Georgia and 7 (seven) of them were implemented following the applications/notifications of citizens. It should be noted that citizens most often cited the disclosure/publicizing of their and/or their family members' data by health care institutions, as well as the facts of disproportionately voluminous data processing by health care facilities.

Based on the cases examined by the Personal Data Protection Service of Georgia, 9 (nine) persons were imposed the administrative liability for 12 (twelve) offences. 2 (two) persons were given the warning and 7 (seven) persons were levied the fine. In parallel with the administrative fines, in order to improve the data processing in public and private entities and ensure their compliance with the Law of Georgia "On Personal Data Protection", the Service issued 22 (twenty-two) mandatory instructions to be implemented.





In 2022, the Personal Data Protection Service of Georgia, on its own initiative as well as on the basis of citizens' requests, examined the cases related to data processing by public and private entities as well as by natural persons in the health care sector, including:

• *LEPL — National Health Agency.* The inspection was initiated by the Service, due to the fact that the Agency represented one of the key institutions involved in functioning of health care system throughout the country and implementing health programs. The scope of the inspection implied the examination of lawfulness of pregnant women's data processing by the Agency through the electronic program (module) of monitoring pregnant women and neonates, within which it was stated that a large volume of data was processed through the module, for example, between January and November 2021 alone, the total of 54407 (fifty-four thousand four hundred and seven) pregnant women were provided with the services through antenatal care.

The investigation stated that the module contained the information needed to implement various health programs that are processed by various subjects within the framework of the functions assigned by the legislation (LEPL — National Health Agency, LEPL — L. Sakvarelidze National Centre for Disease Control and Public Health, Obstetric and Antenatal Care Facilities). In addition, LEPL — Information Technology Agency participated in the activities related to data processing as a data processor in terms of technical administrations of the module. The component of antenatal care of one of the state programs, namely, the state maternal and child health program is implemented by the Agency. The mentioned implies the recognition of pregnant women as the beneficiary of the state program and the reimbursement of cost of rendered services to the health care facility within this program. Antenatal care services are provided only by the health care facilities that are registered as providers of these services in accordance with the law. The total of 229 (two hundred and twenty-nine) medical organizations were registered in the module during the period of inspection, out of which 184 (one hundred and eighty-four) were antenatal care providers.

The study determined that through the module, the Agency staff had the access to all the information that was recorded by health care providers about a particular pregnant woman, including the identity and

nationality of the pregnant woman and her guardian, the father of the new-born, the information about the pregnant woman's visits and their medical research recorded in the module (which encompasses the following information: whether the obstetrician-gynaecologist has been consulted; whether the pregnant woman has been administered the general blood test, rapid/simple screening for syphilis, hepatitis B and C and HIV antibodies, pelvic ultrasound, screening for gestational diabetes and relevant results), in addition, the data on the substances taken by the pregnant woman, the development of gestation process, the health status of the new-born, etc.

The studied circumstances revealed that the Agency had the access to a considerable amount of detailed and mainly special categories of personal data registered in the module, the processing of such information by the Agency was unnecessary for the proper exercise of its own authority. (to implement the various components of the State Maternal and Child Health Program). For example: the nationality of the pregnant woman's guardian and the father of the new-born; the information on those pregnant women who had not applied to be recognized as beneficiaries within the antenatal care component; the data on pregnant women registered by the medical institutions who were not incorporated as antenatal care providers, etc. Within the inspection, the attention was also focused on the need to process the aforementioned data in order to fulfil other functions entrusted to the Agency by the legislation. However, the mentioned was not identified, which was also confirmed by the Agency. Thus, the Agency was found to have processed more information through the module than it was necessary to achieve the legitimate aims defined by law. This, in turn, led to the disproportionate invasion of the privacy of pregnant women and persons associated with them.

The investigation also revealed that a number of organizational and technical measures had been taken by the Agency to ensure the data security in the module during data processing, but there were also singled out the episodes of incomplete recording of actions taken on the data in the module (so-called "logging") and therefore, the certain episodes of the breach of data security as well. Given the volume and category of data, the mentioned above posed the challenge to identifying/preventing the risks of inflicting the significant harm on the privacy of pregnant women. In addition, it was established that the module did not register the person performing the actions on the data (if any) and the fact of viewing the data as well as the certain categories of users were able to directly access the database server of

the module, although the fact of access was not recorded. It should be noted, that improper recording of actions taken against data makes it impossible to trace the instances of access to data protected in the module and identify the untargeted accesses. It was also stated, that there were three (3) users registered in the module with the status as agency employees, who were not employed by the agency at the time of the inspection and did not have access to the data, so there was no need for the user to exist on their behalf. By the decision of the President of Personal Data Protection Service of Georgia on the grounds of the disproportionate data processing as well as for the non-compliance with the data security requirements, the Agency was fined for administrative contravention pursuant to Paragraph 1 of Article 44 and Paragraph 2 of Article 46 of the Law of Georgia "On Personal Data protection". In order to eliminate the violations identified during the inspection, the Agency was given mandatory instructions to implement.

• *LEPL – National Health Agency.* In the application filed with the Service, the citizen pointed out that within the dispute, the respondent submitted the health certificate (Form No. 100) issued by a private clinic in 2018 on the deceased father (deceased person) to the court for the purposes of litigation. According to the explanation of the private clinic issuing the certificate, the mentioned patient's health certificate for the period of 2022 was handed over only to the representative of the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia on the basis of the phone call from the latter. As in the application submitted there was indicated the possible disclosure of data reflecting the services rendered within the provision of health service, the mentioned issue was examined by the Service as part of the unplanned inspection.

Under the circumstances examined, it was established that in February 2022, on the basis of the verbal request, the private clinic sent the health certificate for a deceased person to the Head of one of the unit of the Agency to his/her personal (unofficial) email address, which was saved on the same person's email account for the duration of inspection. Although the Agency was unable to state the specific legal purpose for requesting, receiving and storing the health certificate for the person who died in February 2022, the legal circumstances examined as part of the inspection established that the Agency was the executor of public health care programs and, together with other government agencies, represented the

subject responsible for administering the health care programs. Accordingly, within the scope of its statutory duties and in order to ensure its assigned functions, the Agency needed, in certain cases, to additionally request, receive and store the medical records for a period of five (5) years after the end of reimbursed/unreimbursed cases. In addition, the Agency denied disclosing the health certificate to the third party, and during the enquiry the person having submitted the certificate to the court indicated, that the certificate had been handed over by the author himself in the past. Accordingly, the fact of disclosing the health certificate by the Agency was not supported by evidences obtained during the examination, however, another type of violation was detected.

In particular, the Agency was found to have used the telephone communication for the promptly request of documentation from the medical institutions. At the same time, on a number of occasions the staff of the Agency used the personal emails to exchange medical documentations. The Agency had not established the internal organizational rule/instruction to regulate the means of communication (e.g. office email, personal email, etc.), which the staff of Agency were allowed to use for the exchange of information related to the exercise of their official authority. Consequently, due to the absence of proper instructions, the daily receipt of unregistered medical records containing data via telephone and personal e-mail by the Agency, in the form of grouping, sorting of requested/received data and/or other forms, increased the risk of access to data for illegal purposes and made the possibility to identify data processors much more difficult.

By the decision of the President of Personal Data Protection Service of Georgia, on the grounds of non-compliance with the requirements of the data security the Agency was levied the fine for the administrative offence stipulated in the first paragraph of Article 46 of the Law of Georgia "On Personal Data Protection." In addition, in order to eliminate the irregularities identified during the inspection, the Agency was assigned the mandatory instructions for implementation.

• *LEPL — Emergency Situations Coordination and Urgent Assistance Centre.* On the basis of a citizen's application, the Service investigated the fact of disclosing the personal data of the author of the message on the Centre hotline. According to the appeal, after calling the emergency phone number and notifying the information about the death of a family member, on the same day and

through the same telephone number, the applicant was contacted by the person who offered funeral services prior to the arrival of ambulance crew.

Within the framework of the investigation, it was established that the doctor of ambulance crew of the Centre, who should have responded to the author's call, gave the author's phone number to his/her friend, who implemented funeral Services, before the arrival of ambulance to the address. Having regard to the specific case of data disclosure, it was important to determine the purpose and circumstances of data processing, accordingly, the subject responsible for data processing. For this purpose, the internal organizational documents of the Centre and the course of data processing were examined as well as the explanations of the staff were obtained.

As a result of the inspection, it was demonstrated that the Centre had taken certain measures to protect the confidentiality of the caller's telephone number. In particular, doctors of the Centre were not provided with the information about a caller's telephone number through the software, and if it is necessary to connect the doctor with the person initiating the call by telephone, the dispatchers have the software ability to redirect the doctor to the person, who initiated the call. Also, the Centre presented the labour regulation approved by order of the director of the institution, which defines the obligation to protect confidential information and the receipt confirming that the doctor of the Centre familiarized him/herself with it. According to the above mentioned circumstances and explanations of the Centre, the existence of the instruction/authorization issued by the Centre for disclosing the data by the doctor was not confirmed. On the contrary, it was revealed that the doctor of the Centre, in disclosing the data to his acquaintance, had acted independently from the Centre without providing the legal basis for data processing and informing the owner of the phone number. In addition, when publicizing the data, the doctor had no information whether it was actually necessary to provide the ritual services to the deceased. Accordingly, as a result of a number of verification activities, the doctor of ambulance crew of the Centre was identified as responsible for the data disclosure.

The decision of the President of Personal Data Protection Service of Georgia was focused on the fact, that despite the ability of the dispatcher of the Centre – to ensure the prevention of disclosing the phone number during the communication between the doctor and the initiator of the call through using

a special program, the inspection established that in practice there were detected the occurrences where the phone number of the call initiator was communicated verbally (over the phone) by the dispatcher to the doctor. According to the explanation of Centre, the dispatchers were verbally warned not to share the data of the initiator of a phone call even with the doctors of the ambulance crew. Within the investigation, the physician's responsibility for the disclosure of data was confirmed. By the decision of the President of the Service, the doctor of ambulance team was sanctioned for the administrative offence envisaged by Article 43 paragraph 1 of the Law of Georgia "On Personal Data Protection" for disclosing the information obtained during the professional activity without legal grounds. In addition, taking into account the circumstances revealed during the inspection, the Centre was instructed to resolve the issues relating to data processing in the process of medical emergency-calls in writing.

• *One of the private clinics.* The Personal Data Protection Service of Georgia investigated the alleged disclosure of data by the obstetrician at the private clinic on the basis of a citizen's application. According to the application, a month and a half after consulting the obstetrician at the polyclinic and obtaining the relevant treatment regimen, the applicant was contacted through the phone by the stranger who wanted to know the name of the medicine prescribed by the doctor for the purpose of inquiry and verification. In addition, the applicant indicated the date of purchase of the medication prescribed by the doctor and the name of the relevant pharmacy chain.

Within the inspection, the information was requested from the mobile phone operators (with the aim to identify the caller) as well as from the Clinic, the doctor, the pharmacy chain and the organization that had made the call. According to the evidences collected, the review of application failed to establish when, by whom and to whom the applicant's personal data was disclosed. At the same time, the investigation highlighted the fact of having taken the insufficient measures by the Clinic, in order to protect data security. In particular, in order to fully investigate the circumstances relating to data processing, there were also examined the course of data processing in the electronic form by the Centre. As it was stated, the Clinic additionally made the medical records in the electronic information system of the Clinic (electronic system), where all the information related to the provision of patients with the medical services was reflected, including the services rendered to the applicant and the corresponding treatment regimen. In order to determine the supposed source of disclosure of information containing the applicant's

personal data, the Service requested the information from the Clinic about the logbook (so called "logging") of actions carried out on the applicant's personal data in the electronic system. As a result, it was stated that the electronic system saved the fact of access to the records only if any changes were made to it. In the case of only viewing the recordings, the program did not save any information. Consequently, the persons authorized to have access to electronic system of the Clinic were able to view a particular patient's data without identifying him/her and use the information obtained, including for non-duty purposes.

Conditioned by the above mentioned, under the conditions of absence of necessary measures for data protection, it was impossible to determine whether anyone had obtained his/her data through the electronic system of Clinic after the applicant's visit to the gynaecologist. Due to this, despite the numerous activities carried out within the investigation and a large number of persons interviewed, the alleged unlawful processing of the applicant's personal data was not established.

By the decision of the President of the Service, the Clinic was held administratively liable for the failure to comply with the data security requirements stipulated by the first paragraph of Article 46 of the Law of Georgia "On Personal Data Protection", and in order to eliminate the infringements identified during the inspection, the mandatory instruction was issued to be implemented.

• *One of the private hospitals.* On the basis of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of the information disclosed by the director of one of the hospitals in a telephone commentary to the television company, which concerned the health condition of the applicant's deceased son. According to the applicant's explanation, his/her deceased minor son had overcome the health problems listed and disclosed by the hospital director a year and a half prior to the telephone comment, and he was fully rehabilitated. Thus, the operations and other congenital health problems listed by the doctor had nothing in common with the health status and death of the applicant's son.

In the process of examining the lawfulness of data processing conducted by the hospital, it was stated that the information disclosed to the media encompassed the deceased minor's congenital morbidities,

the medical procedures administered long ago, medical indications and others. According to the information provided by the hospital, the telephone commentary served to protect the interests of hospital because the child's parents and family members had disseminated the inaccurate information via the media, however, the patient had many co-morbidities since birth, which altogether caused the minor's death. Thus, the purpose of the disclosure referred to in telephone comment of the medical director on behalf of the hospital was to protect the reputation of hospital and to provide the public with the accurate information on the matter.

The review of the application established that the information disclosed by the hospital to the media, and accordingly, publicized, was voluminous and contained many sensitive details that may not have been known even to the family members of the deceased minor. Considering the volume and sensitivity of the disclosed data, the hospital could not justify the need of disclosing the detailed information and the reason why only the general references to the child's health status would not suffice to achieve the objective set by the hospital. Parallel to the salient role of care for human health, medical institutions are obliged to treat the information about their patients with the utmost responsibility and to process only a minimum amount of information, even in case of existing their own legitimate interests.

Occasioned by the mentioned, the data publicized by the director of hospital with the aim set by the hospital was not considered as adequate and proportionate, due to which by the decision of the President of Personal Data Protection Service of Georgia, the hospital was held administratively liable for the administrative offence under the Article 44, paragraph 1 of the Law of Georgia "On Personal Data Protection" (the violation of personal data protection principles).

MAIN TRENDS AND RECOMMENDATIONS

The occurrences of data processing examined in the sphere of health care by the Service and the measures implemented demonstrate that data processing in the health sector is related to a number of specific issues, the part of which are directly linked to the role and purpose of the government in the health care sector. Having regard to the mentioned, the data controllers in the relevant sector must importantly consider and solve the following problems:

✓ Many public institutions, each with its own functional load, are often involved in the process of achieving the goals and objective of health care. In order to protect the personal sphere along with a person's health, it is essential for each data controller to have the access only to the needed and necessary data. At the same time, the public institutions engaged in the health sector were found to often use the services of data processors (public or private organizations) to process the data. It is important, that each of them is aware of their responsibilities as of a controller and the issues to be considered in relation to data processors;

✓ When processing data in the healthcare sector, data controllers often fail to take the adequate data security measures, resulting in the accidental and unlawful disclosure of personal information. At the initial stage of data processing, the organizational and technical measures must be importantly taken to protect data from accidental or unlawful destruction, alteration, disclosure, extraction and any other form of unlawful use and accidental or unlawful loss. At the stage of launching data processing, the improper adoption or complete failure to implement the data security measures create the risks of unlawful data processing and at the same time, given the specific nature of these processes, make it impossible to correct them and/or significantly increase the amount of costs required to protect data security;

✓ One of the necessary and effective ways to protect data security is to restrict/separate the access to electronic systems and record all the actions taken on the data. At the same time, it is impossible to determine the specific, universal list of measures to be taken in order to ensure data security. However, given the particularities of the field, such measures should create the effective

safeguard for the protection of an individual's privacy;

✓ In some cases, the health facilities as well as the persons responsible for the management and administration of health sector process more information about patients than it is necessary to achieve the relevant legitimate objectives. Considering the sensitivity of data processed in the health care sector, it is essential to process the patients' data in accordance with the principle of data minimization, only to the extent and for the duration that is consistent with the achievement of the legitimate aim. The mentioned reduces the acuteness and risks of violation of a patient's private life;

✓ It is expedient that health care organizations develop the internal organizational rules for processing the personal data of patients, which ensure that, in accordance with the functions of employees, the processes and forms related to data processing, the purpose of data processing, the need for data security and the cases of data transfer and/or disclosure to the third parties are described in details. It is also important to inform/educate those working in the health care organization about personal data protection at reasonable intervals, so that patients' privacy is not compromised in the course of their work, even inadvertently.

It is essential that the persons, employed in the field of health care, process personal data fairly and lawfully, without violating the dignity of the individual; in addition, not to disclose information to the third parties without gaining consent as well as for the purpose of personal benefit and/or the provision of patient with various services[28]. In order to introduce the appropriate and consistent standards of data processing in the healthcare industry, the organizations need to continually care for the employed personnel to further their qualification in terms of personal data protection, identify the internal organizational problems and in response to develop the appropriate rules and guidelines, which should be periodically communicated to healthcare workers.

[28] Case of Mockute v. Lithuania, [2018] ECHR App. No. 66490/09, §§ 93-95.

3.6. PERSONAL DATA PROCESSING IN THE FINANCIAL SECTOR

In the country, from the qualitative standpoint the majority of data controllers belong to the private sector. The financial sector, which encompasses commercial banks, microfinance institutions, credit institutions, distressed asset management companies, etc. represents the largest data controller[29]. They process a large amounts of data, including information on data subjects' addresses, workplaces, financial obligations, financial transactions, a person's marital status, family relationships, relatives, etc.

In contrast to other data controllers existing in the private sector, in the financial sector the awareness of personal data protection has been raised, as well as the standards for principles of data processing, for definition of the basics and those of security protection adopted in the course of data processing have been improved. At the same time, the number of occurrences of creating electronic databases and their utilization for diverse purposes through various modern technologies is increasing. This in itself increases the risk of errors and irregularities in data processing.

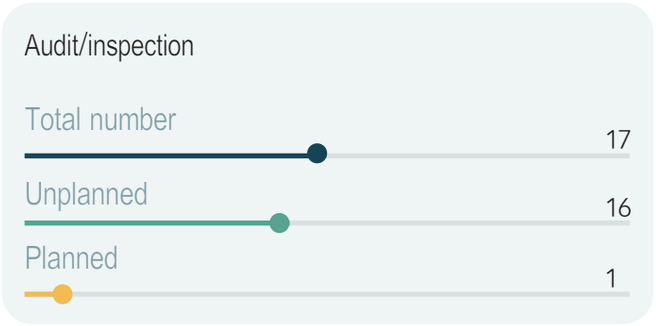
Protecting personal data in the financial sector became the major challenge for the Personal Data Protection Service of Georgia in 2022. Exactly for this purpose, the Service examined a number of data processing occurrences in the said sector and, depending on the relevance of the issue, implemented different types of activities to provide information on the legal requirements for personal data processing in the financial sector and to raise public awareness.

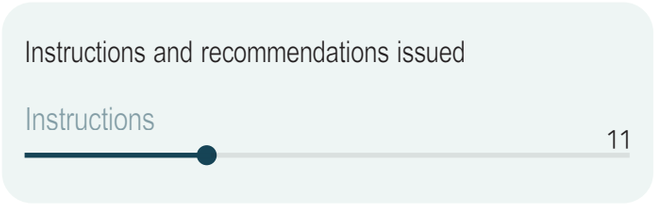
[29] Case of M.N. and others v. San Marino, [2015] ECHR App. No. 28005/12, §§ 51-53.

PROCESSES STUDIED

In 2022, the Personal Data Protection Service of Georgia examined 17 (seventeen) cases of personal data processing in the financial sector, out of which 1 (one) was initiated by the Service and 16 (sixteen) were implemented on the basis of citizens' applications/notifications. During the reporting period, based on the analysis of applications and communications submitted by citizens, several major issues of personal data processing were singled out in the financial sector: banks and microfinance institutions as well as various distressed asset management companies often contact the third parties, including family members, friends and neighbours of the debtor, so as to track the debtor and make him/her repay the debt; the companies illegally obtain and process their data and sometimes the contact with the third party continues, even after the financial institution becomes aware, that the person concerned is unable or unwilling to help the company to put it in contact with the debtor. Consequently, the data is processed without a legitimate purpose or need.

On the grounds of the cases examined by the Personal Data Protection Service of Georgia, nine (9) persons were held administratively liable for nine (9) breaches. Two (2) persons were given the warning and 7 (seven) persons were fined. In addition to the administrative fines, in order to improve the data processing in private institutions and ensure their compliance with the Law of Georgia "On Personal Data Protection", the Service issued 11 (eleven) mandatory instructions to be fulfilled.





During the reporting period, the Personal Data Protection Service of Georgia examined/inspected:

• *One of the banks.* On the basis of a citizen's application, the Personal Data Protection Service of Georgia discussed the lawfulness of the applicant's data processing and established that the bank employee had informed the debtor on the telephone conversation that he/she lived with his mother and brother. At the same time, the employee pointed out that he had the information about his/her place of residence and school. The applicant explained that he had not provided the company with the information about his school and persons living with him/her either at the time of concluding the contract or at a later stage. The applicant requested to verify the lawfulness of processing of his personal data by the bank.

The bank explained that the purpose of processing the applicant's data was its legitimate interest, namely, to fulfil the obligations envisaged by the loan agreement and ensure the repayment of the loan, among them, to offer the opportunity for the applicant to receive assistance from his family members. Having regard to the fact, that such information about the debtor could not be linked to the fulfilment of his/her loan obligation, the Personal Data Protection Service of Georgia did not share the argument provided by the bank. At the same time, the aforementioned data processed by the bank was more extensive than it was necessary to achieve the relevant legitimate purpose. In the specific case, it was up to the debtor to determine the means of securing his obligation. And, the additional processing of the aforementioned data by the bank constituted the unwarranted interference with the applicant's private life.

By the decision of the President of Personal Data Protection Service of Georgia, the bank was imposed the liability for the administrative offence envisaged by Article 44(2) of the Law of Georgia "On Personal Data Protection" (the violation of the principles of data processing).

• *One of the banks. Within the scope of reviewing the application, the Personal Data Protection Service of Georgia stated that the private company, as a data processor, implemented the processing of information about the data subject on the basis of the service contract concluded with the bank. The data subject requested the information from the data processor about processing the physical and electronic signature on the document upon delivering the message, but he/she has not been submitted*

the requested information within the set deadline and in the requested, written form.

By the decision of the President of Personal Data Protection Service of Georgia, the bank was held liable for the administrative offence pursuant to the first paragraph of Article 50 of the Law of Georgia "On Personal Data Protection". It was instructed to implement such measures which in the future, would ensure the provision of data subject with the information within the time limit prescribed by Law of Georgia "On Personal Data Protection" even in case of the data subject(s) making request for the information from the data processor.

- *The inspection of one of the banks.* The inspection was initiated by the Service and included the examination of lawfulness of data processing during the audio monitoring of the communication between the bank and customer through the hotline.

As a result of inspection it was revealed that the audio monitoring of telephone conversations had been conducted since 2009, about which both the bank employees and customers were informed via the appropriate answering machine. In addition, telephone conversations were recorded and stored by the bank through its own official technical devices (where electronic systems and communication channels are loaded). It should be noted that audio recordings of telephone conversations were stored during 25 (twenty-five) years after the call was made.

It is significant that the bank could not substantiate the necessity of storing the data (audio recordings) processed by audio monitoring of telephone conversations between the bank employees (including former employees) and clients for 25 (twenty-five) years. He did not provide the specific reasons, due to which it was necessary to keep the audio recordings of telephone conversations for the said period.

The inspection also established that the audio recordings of telephone conversations were stored on the server, which could be accessed directly from the server as well as from the telephone intercom station. At the same time, the actions performed on the data were not fully registered at the telephone intercom station. In particular, only the user's login and logout were recorded. The implementation of the access directly from the server was ensured by the staff of IT department, although they did not use the individual

user and password. In addition, in the case of the access directly from the server, the actions performed on the data were not recorded.

By the decision of the President of Personal Data Protection Service of Georgia, the bank was held liable for committing administrative offences under the first Paragraph of Articles 44 and 46 of the Law of Georgia "On Personal Data Protection". In addition, the bank was instructed to take the appropriate organizational and technical measures so as to ensure data security.

- *One of the companies.* On the basis of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of processing of the applicant's personal data.

According to the applicant's explanation, the company called him/her four times at regular intervals on the telephone number belonging to him/her, when he was addressed by name and asked to provide the information to an unknown person. The applicant explained that he/she had repeatedly informed the representatives of the company that he/she could not assist in providing information to the person in question. At the same time, they disregarded the request to stop processing his/her data.

Based on the information provided by the company within the review of application, the communication with the debtor was impossible. Due to the mentioned, it was necessary to visit the debtor at his/her address, during which the employees of the company obtained the contact number through which they could communicate with the debtor. According to the explanation of the company, during the telephone communication the applicant had expressed his/her willingness to assist the company in finding the debtor and provide the information (the applicant denied this fact during the review of application), but during the communication carried out by e-mail the applicant demanded not to be contacted again.

The position of the company was contradicted by the evidence obtained by the Service. In particular, it was established that the applicant had indicated in the e-mail sent to the company that during each telephone call he told employees of the company not to call him/her again. However, in the letter sent by the company to the applicant, the company did not explicitly declare, that during the telephone conversation the applicant did not request to stop processing of his/her data. Accordingly, the company

had made a call to the telephone number belonging to the applicant without a lawful purpose, which contravened the requirements set out in Sub-paragraph "b" of Article 4 of the Law and constituted the administrative offence under Article 44 of the Law.

By the decision of the President of Personal Data Protection Service of Georgia, the company was held liable for the administrative offence under Article 44(2) of the Law of Georgia "On Personal Data Protection".

- *One of the banks.* The Personal Data Protection Service of Georgia was applied by a person who indicated in the application that he was a customer of a particular bank, had a personal banker and was authorized for his/her email address. However, after the change of personal banker, he/she received the e-mail from the bank, in which the sender of the e-mail informed him/her that he/she was his new personal banker. The recipient field of the same email (the so-called "to whom") contained the email addresses of dozens of other persons in addition to the email address of the applicant. Accordingly, these persons were able to find out the information about the applicant's email.

As part of the review of the application, the Personal Data Protection Service of Georgia established that upon sending the email to the applicant by the bank, besides the applicant, the recipient of the email was 161 (one hundred and sixty-one) other persons, because instead of the field "blind carbon copy" (so called "bcc") of the email the personal banker accidentally indicated the recipients of the email in the field "carbon copy" (so called "cc"). Accordingly, the applicant's e-mail address became known to every recipient of the message. Within the review of the application, it was stated that the purpose of the bank was not to disclose the applicant's email address to others. At the same time, the bank had taken certain organizational and technical measures, but they did not suffice to prevent the disclosure of the applicant's e-mail address to other persons in the case at hand.

The Personal Data Protection Service of Georgia considered that the bank had violated the first paragraph of Article 17 of the Law of Georgia "On Personal Data Protection", which represented the offence envisaged by the first paragraph of Article 46 of the same law and the grounds for

imposing administrative liability. By the decision of the President of Service the bank was held liable for the administrative offences under Article 46(1) of the Law of Georgia "On Personal Data Protection".

- *One of the companies.* On the basis of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of the applicant's personal data processing. The applicant pointed out, that he/she had applied for a loan on the company website, indicating his/her first name, surname, personal ID number, and mobile phone number. On the same day, he/she was contacted by the company through the mobile phone number referred to in the loan application and asked where he had worked in 2013. To the question why the company evinced its interest in the said issue, it was explained that the mentioned was the subject of interest of the department reviewing the applications, whereupon the applicant provided the company with the requested information. On the same day, the applicant contacted the company again and inquired about the purpose of the company to process the information about his/her workplace in 2013. He/she was explained that the company wanted to determine whether the applicant had the continuous service record.

Within the review of the application, it was stated that prior to establishing the business relationship with clients, the company carries out the check of clients in various types of databases at its disposal, which includes the lists of politically active and sanctioned persons. According to the company, due to the fact that the applicant's first and last name coincided with the person in the database, it was necessary to obtain additional identifying information, namely, where the applicant worked in 2013.

The objective of the company to determine the suspiciousness of the transaction and to take the appropriate preventive measures, including asking the client clarifying questions, is legitimate. However, in the case at hand, the above argument of the company could not be shared by the Service. In particular, the database could not be considered as a reliable source because, apart from the first and last names, it did not contain any other identifying data (such as the personal identity number) by which a person could be reliably identified. Accordingly, in order to achieve the legitimate aim of the company, the information about the applicant's place of work as of 2013 could

not be regarded as the adequate means of achieving that aim, since on the basis of the applicant's response the company could not determine whether the applicant was the person referred to in the database.

By the decision of the President of Personal Data Protection Service of Georgia, the company was held liable for administrative offences according to Article 44(1) of the Law of Georgia "On Personal Data Protection".

MAIN TRENDS AND RECOMMENDATIONS

The issue of voluminous data processing in the financial sector represents one of the most salient challenges. The process of data processing in most cases involves the conflict between the legitimate interests of the data controllers and their clients/debtors, in which case it is important to strike a fair balance between the right to privacy of the data subjects and the legitimate interests of the controllers. Based on the analysis of the cases examined by the Service, in order to protect personal data and prevent its inappropriate processing in the financial sector, the financial institutions should importantly take the following measures. They must:

✓ Assess and strike the balance between the legitimate interests of the company and the rights of the debtor and others persons during processing the debtor's data;

✓ Ensure that the data subject signs the written agreement with the data processor and/or gives such instructions that provide the data subjects with proper information in accordance with the law on processing the data by a data processor at the request of the data subject;

✓ To take such organizational and technical measures that will allow to electronically record all the actions taken on the data in the case of data processing through electronic systems;

✓ To request for only such information from clients that would be adequate to achieve the

legitimate purpose at the time of implementing the preventive measures in the process of establishing the business relationship with clients;

✔ In the financial sector, to stop processing his/her data at the data subject's request and/or to provide him/her with information about the refusal of the request in the course of processing the data of the third party in order to search for the debtor.

In order to raise the standard of data processing in the financial sector, it is salient for the financial institutions to effectively manage the individual case of data processing of each debtor and/or the third party. It is imperative to protect the confidentiality and security of information obtained from debtors and to ensure the fair balance between the privacy of debtors and the third parties. Giving consideration to the large number of individuals engaged in the financial sector, it is important to ensure that they are continually trained and adequately informed about the legal regulations.

3.7. DATA SECURITY

In line with the advancements of modern technology and its widespread utilization the compliance with the rules on data security is increasingly growing in salience.[30] The protection of information existing in the electronic systems and databases, to a large extent, determines public confidence in data processing institutions. The violations of rules on data security, including the improper assessment of the risks associated with data processing or taking insufficient organizational and technical measures to protect data, may pose the threat of unlawful data processing.[31] The mentioned can damage the reputation of the data controller and the interests of the individual citizen and, in some cases, lead to the breach of confidentiality protected by professional secrecy. Moreover, data security becomes particularly important in the context of processing the personal data of minors.

Occasioned by the volume of data stored in the electronic systems and databases and the possibility of their straightforward search, the systematic monitoring of the access to the data stored in such systems is particularly important for the security of data stored within the institution. At the same time, in order to prevent the data processing for personal purposes by employees, it is important to duly inform employees about the rules of data processing and the concomitant consequences.

In order to protect the interests of every citizen, data processing institutions are obliged to take the appropriate organizational and technical measures to minimize the risk of illegal data processing. The measures to be taken for data security should be adequate to the risks associated with data processing. In addition, it is also essential to ensure the protection of software mechanisms against unauthorized access to databases and to record all the actions taken on the data existing electronically. Furthermore, any co-employee of the data controller and the data processor participating in data processing must not exceed the remit of his /her authority.

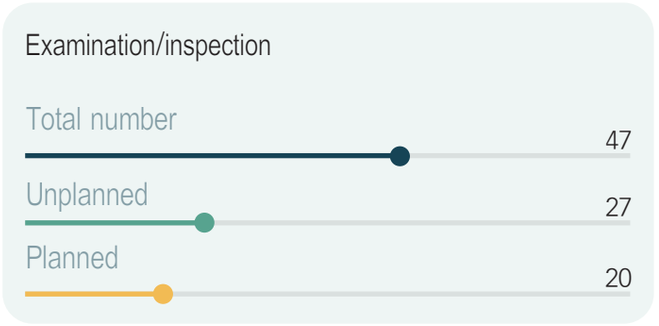
[30] CoE Committee of Convention 108, Opinion on the Data Protection Implications of the Processing of Passenger Name Records, 2016, p. 9.
[31] CoE, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, §49. CoE, Explanatory Report of Modernised Convention 108, 2018, §§ 62-64.

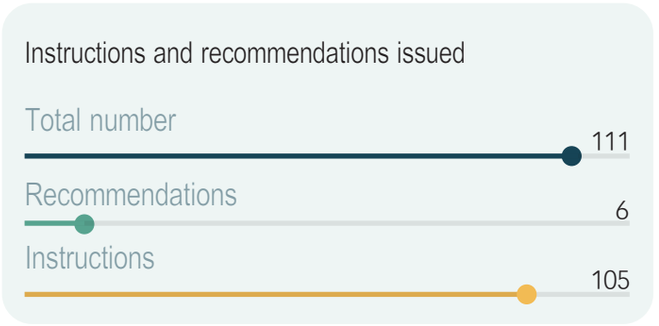
In 2022, the Personal Data Protection Service of Georgia examined a number of cases related to the compliance with the rules on data security within the planned inspections as well as on the initiative of citizens' requests. In addition, various events (including training sessions, public lectures, etc.) were held intending to raise public awareness and that of responsible persons for data protection about the rules on data security.

PROCESSES STUDIED

In 2022, the Personal Data Protection Service of Georgia investigated the total of 47 (forty-seven) cases related to data security. 20 (twenty) of them were implemented at the initiative of the Personal Data Protection Service of Georgia and 27 (twenty-seven) were based on citizens' applications/reports. In the applications submitted to the Service, the citizens mainly referred to the cases of illegal disclosure of their personal data, as well as the facts of implementing the inadequate video and audio surveillance.

In the cases examined by the Personal Data Protection Service of Georgia, the total of thirty-nine (39) persons were held administratively liable for fifty-five (55) offences. Fifteen (15) persons were issued the warning as a sanction, twenty-four (24) persons were levied fines. In parallel to the administrative fines, in order to improve data processing in public and private entities and ensure their compliance with the Law of Georgia "On Personal Data Protection", the Service issued six (6) recommendations and one hundred and five (105) instructions mandatory to be fulfilled.





In 2022, the Personal Data Protection Service of Georgia on its own initiative as well as on the basis of citizens' requests, examined the various case related to the protection of data security within the professional activities of public and private entities as well as natural persons. During the reporting period, in order to examine the issues related to the compliance with data security regulations, the Personal Data Protection Service of Georgia carried out the inspections in Tbilisi and in the regions. The Personal Data Protection Service of Georgia examined/inspected:

• *LEPL – National Agency of Public Registry.* The data processing was investigated on the basis of the general application of 5 (five) citizens, which concerned the lawfulness of reflection of the names and personal identification numbers, together with the court decision, of 2 (two) legal entities in the extracts (in the clause of sequestration/prohibition) from the Register of Enterprises issued by the agency. According to the position taken by the applicants, they had no connection with the above–mentioned legal entities, at the same time, in case of viewing the extracts, the information about the ongoing criminal case against them became known to anyone.

Within the inspection it was stated that the National Agency of Public Registry utilized the separate software with the aim to produce the Registry of public–law restrictions and the Registry of entrepreneurs. The data exchange process was carried out in such a way, that the data registered in the Registry of public–law restrictions was reflected without any changes in the extract from the Registry of entrepreneurs prepared about the data subject concerned through the program (automatic control equipment). In addition, the agency developed the "Rules for Electronic Distribution of Cases Received by LEPL – National Registry of Public Agency", which indicated that the Agency is obliged, in case of existing more than one public–law restrictions, to receive the individual application for each one (e.g. application, the address in writing, etc.) submitted to the Agency. In this case, based on the Court Ruling the Agency made the decision about the registration of the origin of distraint related to the goodwill in intangible assets of the individuals and entities (including the applicants) referred to in the same Order. On the basis of the said decision, the details of all the natural and legal persons mentioned in the resolution, including the names and personal identification numbers of the applicants, are cumulatively recorded in the registry of public–law restrictions.

As a result of the inspection, it was also established that the data registered about 2 (two) legal entities specified in the resolution section of the ruling had been amended by the decisions of the Agency, as a result of which on the grounds of the court decision the information (including the identification data of the applicant) analogues to the data logged in the register of public–law restrictions against the applicants was also reflected in the extract from the Entrepreneurial registry, in particular, in the sequestration/prohibition clause. Following the review of the issue conducted by the Service, the technical errors in the registered data of above mentioned 2 (two) legal entities

were corrected by the decisions of the National Agency of Public Registry and the personal data of the applicants were withdrawn from the sequestration/prohibition clause in the updated extracts.

As a result of the examination, it was established that according to the Acts regulating the activity of registering body, the extract from the registry of entrepreneurs must reflect the data logged about a single subject only, as well as the information about the public–law restriction registered in relation to the same subject and/or his/her partner's share at the time of drawing up the extract. It was also stated, that the applicants did not represent such legal entities, with respect to which the obligation to reflect the data (in particular, the information on public–law restrictions) in sequestration/prohibition clause of the extract about 2 (two) legal entities was envisaged by the legislation regulating the activities of Agency. Consequently, the applicants' data was processed without the legitimate purpose and the mentioned action created the risk of processing inaccurate data about the applicants (such as putting the applicants in contact with the relevant legal entities).

The inclusion of information about the applicants' public–law restrictions in the extracts of legal entities and accordingly, their unlawful processing was, in turn, accounted for by the absence of adequate organizational and technical measures, such as the joint registration of information about public–law restrictions of several entities in the Registry of Public–law Restrictions (which contradicts the obligation to receive individual applications established by the "Rules for Electronic Distribution of Cases Received by" LEPL – National Registry of Public Agency"), and then the automatic import of data from the said Registry into the Entrepreneurial Registry (the technical possibility — to mechanically (manually) correct the data imported from the Registry of Restrictions was not utilized by an employee of the Entrepreneurial Registry).

According to the decision of Service, the National Agency of Public Registry was imposed liability for the administrative offence provided by the first paragraph of Article 46 of the Law of Georgia "On Personal Data Protection" on the grounds of non–compliance with the data security requirements. In addition, as a result of the risk assessment relating to processing of data stored in the Registry of Restrictions, the Agency was recommended to take the adequate organizational and technical measures for the protection of data security.

- *The City Hall of Rustavi Municipality.* Within the health programs/subprograms, the municipalities process large volumes and specific categories of data on vulnerable groups, including minors, through using the automated tools as well. With respect to the data mentioned, the compliance with data security rules requires the adequate risk assessment. The inspection was initiated by the Service and included the review of the lawfulness of processing the beneficiaries' personal data in the course of implementing the rehabilitation sub-program for children with autism spectrum disorders.

As part of the inspection, it was stated that for the purpose of inclusion of the children with autism spectrum disorders in the rehabilitation sub-program, together with the application the considerable amount of information about the beneficiary (including the information about the health status) was submitted to the administration of Rustavi City Hall. The application was submitted to the Mayor's Office both physically and via the e-mail of the Rustavi City Hall or the citizens' electronic portal. The electronic copy of the application and the attached documentation was initially uploaded onto the electronic case management software, where a number of data about the beneficiary and his/her legal representative (name, surname, personal identification number, date of birth, photo, etc.) were automatically entered from the database of LEPL – Public Service Development Agency. In order to implement the sub-program, electronic documents in "MS Excel" format were also created, updated and utilized, where a number of personal data of the beneficiary was also provided. The technical support for functioning of the electronic case management software and citizens' portal was provided by NNLE – Municipal Services Agency.

Within the inspection, it was ascertained that any type of correspondence logged in the case management program of the Municipality could be accessed, in case of using some of the search functionality existing in the electronic case management software of Mayer's Office of Rustavi Municipality. In addition, a number of staff members having the service account in the electronic case management software had activated the mentioned functions and therefore, could access a large amount of data processed within the rehabilitation sub-program for children with autism spectrum disorders. However, the inspection demonstrated that the part of the mentioned employees did not need to have the access to beneficiaries' data for the performance of their duties and functions

(for example, at the time of inspection, the total of 39,277 (thirty–nine thousand two hundred and seventy–seven) correspondence, including the correspondence relating to beneficiaries with the autism spectrum disorders logged in the case management program was available to the designated staff).

The outcomes of inspection also revealed that there was no electronic logbook of the actions taken on the data included in the shared folder, through which the City Hall staff had the access to the electronic documents in MS Excel format containing the personal data of the beneficiaries. The aforementioned created the risk of failure to identify the relevant facts and the data processor in case of unlawful processing of data, including the disclosure by employees with the right to access the data.

In addition, within the inspection it was revealed that for the purposes of operating the electronic case management software and the citizen's portal, the data was obtained from the database of LEPL – Public Service Development Agency. However, the contract signed between the Agency and the Rustavi City Hall with respect to the above mentioned did not envisage the issues relating to the submission of individuals' photographs to Rustavi City Hall and the provision of real–time data to the civil portal of Rustavi City Hall.

According to the decision of the Service, Rustavi City Hall was held liable for the administrative contravention stipulated by Article 46, Paragraph one of the Law of Georgia "On Personal Data Protection" on the grounds of failure to comply with the data protection requirements. In addition, the Mayor's office was instructed to record all the actions taken with regard to the beneficiary's data (including the data existing in the shared folder) as well as to introduce the measures to prevent the cases of transfer in breach of legal requirements of the data processed in the electronic case management software to the third parties, and to allow the access to this data only for those persons who need the access to the said data for the performance of functions–duties assigned to them. The Rustavi City Hall and LEPL – Civil Service Development Agency were also instructed to contractually regulate the issue of obtaining personal data from the mentioned agency in real time and in the amount proportionate to the purpose of processing as well as in the process of operating

the electronic case management software and the civil portal.

- *Tserovani Public school №3 of Mtskheta Municipality.* The inspection was initiated by the Service due to the fact that schools process a significant amount of personal data on disciplinary offences of minors, among them via automatic means. The failure to take the appropriate organizational and technical measures with regard to the said data can lead to the unlawful disclosure or other forms of processing, which, in turn, can inflict the harm to the dignity of children, their stigmatization, i.e., can be a conditioning factor of "bullying" and discrimination.

The inspection revealed that the school was processing students' data within the disciplinary offences, among them through the automated means (electronic journal). In particular, the acting school principal and his/her deputy received the data on a student's disciplinary offence in the infringement registration section of the electronic journal from the electronic information database of the Office of Educational Institution's Mandatory (including the information on the place, time, and event conducted by the Mandatory) by software. In addition, the student's name, surname, personal ID number, date of birth, gender, grade and social status were displayed in the infringement section of the electronic journal from the general Education Management Information System ("e-School"). During the disciplinary proceedings, the school received the written explanation from the student about the alleged violation and the extent of the student's responsibility was determined by the individual administrative act of the school principal. The software for the e-journal, the electronic information base of the Office of Educational Institution's Mandatory and the e-school was run through the LEPL – Educational Management Information System.

As part of the inspection, it was stated that out of the actions implemented, the search/view actions were not recorded in the electronic journal. The actions performed on the data were not recorded in case of direct access to the database used to store the data in the electronic journal, either. In the case of direct access to the database, the administrators of database of the LEPL – Education Management Information System utilized the same users. It should be noted, that even in the case of recording the actions taken on data, the access to data by the common user makes it difficult to identify the person performing the specific action that does not meet the data protection requirements.

According to the decision of the Service, the LEPL – Educational Management Information System was found to be in breach of Article 46 of the Law of Georgia "On Personal Data Protection" for committing the administrative offence (non-compliance with data security requirements). In addition, the system was instructed to record all the actions taken on the data existing in the electronic journal as well as in the database (in case of direct access to the database). At the same time, taking such organizational and technical measures that allow the data processors to directly access the database of electronic journal only through the individual user accounts protected by the appropriate password.

- *Data processing through the general courts' case management.* The Service was applied by the citizen who pointed out, that the information about the case of administrative offence filed against the applicant in Batumi City Court, namely, the Articles of the Code of Administrative Offences, on the grounds of which the proceedings were taken in Batumi City Court, appeared in the data, alongside his name and surname, of one of the civil cases initiated in Tbilisi City Court, where the applicant was the representative of plaintiff's side.

The inspection stated that for the purposes of legal proceedings management the general courts (the total of 28 (twenty-eight) courts) have been using the internal case management program since 2011, which records all the cases initiated in general courts and is accessible for employees of the courts of general jurisdiction. Although the courts of general jurisdiction use the case management program on a daily basis, they do not have the capacity to take the necessary technical steps for managing and administering the program. From 2019 onwards, on the basis of the Organic Law of Georgia "On General Courts", the Council of Management Department assesses the expediency of amendments and then, in case of a positive decision of the High Council of Justice of Georgia, prepares and introduces the case management program, due to which the Council is considered to be a data controller.

Upon registering each of the cases in the case management software, the identifiable data of the persons participating in the case (parties and their representatives) is recorded by the data controller of the court. The functionality of the program allows to search for, edit and save already existing

data about this person in the program in the process of registering the participant of the case. In such cases, the edited data then replaces the data about this person existing in other courts as well. The investigation demonstrated that when registering the case of administrative offence against the applicant, the data processor of Batumi City Court indicated the Articles of the Administrative Code as well as the number of the case against him along his/her name and surname and then saved the edited details of the data. As a result of the above-mentioned, the information recorded, together with the applicant's first and last names, became available in the ongoing case with his involvement at Tbilisi City Court.

The persons participating in the proceedings (parties and their representatives) have access to the case and personal data of the parties/their representatives through the special portal – the "Personal Cabinet", where the information/documentation logged in the proceedings is automatically reflected. Accordingly, the plaintiff, the defendant and his/her representative in the pending case before the Tbilisi City Court was granted the access to the grounds of the initiation of administrative offence case (the relevant Articles of the Code) and the case number in relation to the applicant. Having regard to the fact, that the improper use of the functionality of the program resulted in the disclosure of information of utmost importance for the applicant and the program allowed one court to edit the data registered by another court, the entity authorized to conduct and administer the case management system – the Council failed to justify the purpose of this functionality in the program, its necessity and compliance with the personal data security requirements within the inspection. It was also demonstrated, that the Council had not developed the written policy/instruction or any other type of document that would explain to the users of case management software the rules and consequences of running the software, including the use of various functionalities when registering participants.

In addition to the above-mentioned, the examination of the case management software revealed that the actions taken on data (so-called "logging"), including the changes and/or viewing of registered data were not implemented at any stage of the course of the particular case. This increased the risks for unlawful processing of data and made it impossible to monitor the actions taken in relation to the data as well as to identify the data processor in the case of infringement of legislation during data processing.

The Council was held liable for the administrative contravention stipulated by Article 46, Paragraph one of the Law of Georgia "On Personal Data Protection" on the grounds of failure to comply with the data protection requirements. In addition, the Council was instructed to bring the functionality of the program in line with the legislation, so as to eradicate the irregularities identified during the inspection.

- *One of the companies.* The inspection was conducted on the basis of the anonymous notification submitted to the Service. According to the notification, audio monitoring was implemented by the company in one of the casinos, during which the personal data of employees and customers of the company was processed. At the same time, based on the explanation of the author of the notification, employees of the company were not informed about the implementation of audio monitoring.

Consequently, to the inspection, it was established that the audio monitoring in the gaming parlour belonging to the company was carried out through two different types of electronic systems, namely, eleven (11) portable audio recording devices (carried by employees in their pockets during working hours) and one (1) video surveillance camera placed in the cash desk area.

The inspection revealed that the audio surveillance was carried out with the aim to protect the security and property of the company, as well as to exercise its statutory powers. In addition, the portable voice recorder did not have the electronic log book of the actions performed on the data (so-called "logging"), and the company recorded the actions performed on the data existing in the portable voice recorder in "Excel" file. It is worth noting that in the case of logging the actions performed on the data, which is input in Excel file manually using the human resource, the risk(s) of accidental or illegal data processing cannot be ensured due to the fact, in case of filling in Excel manually, the probability of making errors is high. Thus, in the case of unlawful data processing, it is possible that the data processor who is responsible for the unlawful data processing, may not be identified. As part of the inspection, it was singled out that audio surveillance was conducted in order to protect the property and security of the company and to exercise the powers vested in it by law.

According to the decision of the President of Personal Data Protection Service of Georgia, on the

grounds of violation of rules on data security the company was found to be in breach of Article 46 of the Law of Georgia "On Personal Data Protection" for committing the administrative offence. The company was also instructed to develop such a written document that would define the purpose and scope of audio monitoring, its duration, the rules and conditions for accessing, storing and destroying recordings, and the mechanisms to protect the rights of data subjects.

- *Parcel Transportation Company.* In line with the advances in technology and the simplification of purchasing things on the foreign market, the number of people actively buying things from different countries in their daily lives has increased. The companies implementing parcel transportation offer the opportunity for their customers to order parcels from different countries via the websites with the aim to simplify their service. Giving consideration to the large volume of personal data processed, the Service took the initiative to inspect the lawfulness of receiving and storing the consumers' data via the website of one of the companies implementing the organization of the international transportation of parcels.

Within the inspection, it was stated that the company provides the consumers' freight transportation to Georgia from different countries of the world. Any individual can utilize the mentioned service of the company (a total of 79 639 (seventy-nine thousand six hundred thirty-nine) consumers use the service of the company).

The inspection demonstrated that all the actions taken on the data were not recorded in the course of data processing through the administrative panel on the website of company. The passwords of users of the panel administrator as well as employees of the company were stored in the database in the unencrypted form. In case of changing the company user's password, the website no longer asked to change the new password sent to the user's email. Accordingly, this allowed to use the automatically generated new password even in case of keeping on working on the website, which, in turn, created the risk of unlawful use of the password.

By the decision of the President of Personal Data Protection Service of Georgia, on the grounds of violating the rules on data security, the company was found in breach of Article 46 of the Law of

Georgia "On Personal Data Protection" for the administrative offence and was instructed to log all the activities carried out on the data during data processing through the administrative panel as well as to store the data (including the user's data and login and password for the administrative panel) in the encrypted form; It was also prescribed to take such organizational and technical measures, as a result of which, in case of changing the user's password, the new one sent to the e-mail of the company user would become a one-time password and the system would mandatorily require the automatically generated password to be changed.

- *The natural person conducting the legal activities.* In the course of professional activities of data processing organizations as well as natural persons, it is essential to protect data security, especially with regard to processing special categories of data. The examination was conducted by Prosecutor's Office of Georgia on the basis of the notification submitted to the Service. According to the application, the information was submitted to the Prosecutor's Office by a natural person notifying that his son had found a package of 73 (seventy-three) computer disks in one of the squares (yard) located in Tbilisi. The Prosecutor's Office established, that the CDs in question contained the materials of several criminal cases, which the lawyer acting for the defense in the criminal proceedings had received from the prosecution.

During the inspection, it was highlighted that the materials of the criminal case recorded on the aforementioned discs contained the personal data of various persons, including the name, surname, personal ID number, the information on the initiation of investigation, etc. The CDs in question belonged to the lawyer representing the defence within the criminal proceedings.

The inspection established that the lawyer had not taken any organizational and technical measures to prevent the accidental or unlawful processing of the data contained in the computer disks. In addition, it is noteworthy, that there were other lawyers working at the law firm who processed a large volume of data, including that of special categories, independently or on behalf of the company. In the office of the company, the information on criminal cases was packed in boxes and was available to the persons employed there as well as to outsiders as well.

According to the decision of the President of Personal Data Protection Service of Georgia, the lawyer was held liable for the administrative offence envisaged by Article 46 of the Law of Georgia "On Personal Data Protection" on the grounds of non–compliance with data protection requirements. The lawyer and the law firm were instructed to develop such organizational and technical measures which would ensure the protection of personal data security (e.g. keeping the files containing the data in the place protected by an appropriate lock, etc.).

- *One of the oil and gas companies.* The inspection was initiated by the Service, as the company processed the personal data on a large number of users when issuing the corporate (discount) card. It should be noted that the inadequate implementation of security measures during the processing large volumes of data may create the particular risks of illegal data processing. The inspection included the examination of the lawfulness of obtaining and storing personal data of clients in the process of issuing a corporate (discount) card by the company.

Within the inspection, it was established that the company issued corporate (discount) cards at the request of consumers physically – on their visits to the service centres of the company or electronically after completing the registration form on its website. Upon receiving the corporate (discount) card, the fuel purchase agreement was concluded which contained the text of the consent to data processing.

It was also revealed that during data processing the company did not encrypt the data through the website. The transfer of data via the Internet was made openly, which created the risks of accidental or unlawful data processing by the third parties. Moreover, the website did not log all the actions performed on the data. The program recorded adding, editing and deleting of data, but viewing and deleting of data was not recorded. Besides, in case of the direct access to the database of program, the actions performed on the data were not recorded in the database. Consequently, data security rules were also breached by the company.

According to the decision of the President of Personal Data Protection Service of Georgia, the company was held liable for committing the administrative offence envisaged by Article 46 of

the Law of Georgia "On Personal Data Protection" on the grounds of violating the rules on data security. The company was instructed to encrypt the consumers' personal data during transferring it via the Internet and record all the actions taken on the data existing electronically.

MAIN TRENDS AND RECOMMENDATIONS

The practice of the Service evidences that a number of irregularities and shortcomings are detected in the course of data processing by the public as well as private institutions using modern technology, and therefore, it is expedient to consider the following recommendations. In particular:

✓ On some occasions, data controllers do not or incompletely record the actions (e.g. viewing, downloading, deleting and editing data) performed on the data existing electronically. In frequent cases, the actions performed on the data through direct access to the database are not logged by institutions. It should be noted that without their full recording as well as in the event of improper data processing, including its disclosure by a data processor having access to the data, the establishment of the relevant fact and identification of the responsible person may not be possible. Thus, recording and periodic monitoring are effective means of preventing illicit data processing. It is worth noting that it is important to automatically record the actions performed on electronic data, as there is a high probability of indicating incomplete/inaccurate information in case of logging the actions mechanically using human resources (e.g. by entering MS Excel format into a document);

✓ In some cases, the staff from different agencies share common users to access data through automated means. The mentioned also complicates the identification of the person implementing the data processing and does not represent the organizational and technical measures consistent with the objectives of preventing unlawful data processing. It is important that all the users only access the data via the appropriate password-protected user account personalized to him/her;

✓ In some cases, access to large amounts of personal data (including special categories of data) stored in the institutional databases is granted to those employees who do not need such access in the performance of their duties. There were also instances singled out, where the accounts

for accessing information were created even for the employees who had never been employed by the data processing agency or had worked in those institutions in the past. In order to prevent illegal data processing (e.g. unlawful disclosure), it is important for the institutions to provide access to data only to those persons who need it to perform the functions and duties assigned to them;

✓ There were identified cases where the systemic errors in the case management or other programs caused by the failure to take appropriate organizational and technical measures, including the established practice of exchanging information between two different systems, create the risks(e.g. providing the access to information for the unauthorized employer of the organizations implementing the data processing or the disclosure of data to the third parties) of unlawful processing of data of a large volume. It is important for data controllers to periodically assess the risks posed by data processing and to take appropriate measures to prevent them in the process of planning the administration of systems as well as during operation;

✓ The data-processing agencies pay less attention to the accuracy of data in electronic databases and to the issue of their updating. It should be noted that unlike written documents the verbal regulation of the issue and the practice based on it may have a less binding effect on the persons involved in data processing. Thus, in order to prevent illegal data processing, it is important for institutions to develop the policy document that will regulate the purpose and manner of data processing in the electronic database, the timing of its updating, the storage period and the method of destruction, as well as the effective mechanism for periodic monitoring of data processing by employees and ensuring the compliance with the outcomes concomitant with the illegal data processing;

✓ The private as well as public entities are increasingly utilizing the biometric data for the purpose of remote identification of individuals. From this perspective, it is important for data controllers to consider that the processing of biometric data by public entities is permitted only for the purposes of personal security, the protection of property and the prevention of disclosure of confidential information (if these objectives cannot be achieved by other means or are linked to the disproportionately large amount of effort) as well as for the purpose of issuing the identity document

or identifying the person crossing the state border in accordance with the rule established by law and in other cases stipulated by Georgian legislation. As regards the private entities, processing the biometric data by them is permitted for the purposes of conducting business, ensuring security and protecting the property, as well as for preventing the disclosure of confidential information, if these purposes cannot be achieved by other means or require unreasonable effort. When processing biometric data there should be ensured the adequate organizational and technical security measures as well;

✔ There were singled out the cases where physical security of the data was not properly ensured leading to posing the significant risks of unlawful processing of the mentioned data. It should be noted that there is no universal list of measures to be implemented with the aim of data security, and the development/implementation of these measures should be done on the grounds of joint analysis of the circumstances/risks associated with data processing on a case-by-case basis. In order to set the high standard of data protection, data processing organizations should take into account the necessity of data confidentiality as early as at the stage of designing the work space so as to minimize access to data by unauthorized employees and outsiders (For example: the data should be kept out of the reach of unauthorized persons, protected by a suitable lock, the access to the data should only be granted to those with the relevant need, etc.).

3.8. PERSONAL DATA PROCESSING BY LAW ENFORCEMENT BODIES

One of the directions of activities of the Personal Data Protection Service of Georgia is to study the lawfulness of personal data processing by law enforcement bodies, conducted covert investigative actions and monitor the activities performed in the central databank for electronic communications identification data. The inspection of the lawfulness of personal data processing during legal proceedings is the issue of top priority, as law enforcement activities are linked to data processing during criminal or administrative proceedings, investigation of crimes, criminal prosecution, and execution of sentences. Additionally, law enforcement bodies have access to electronic databases, CCTV footage, and data obtained from open and covert sources in the process of implementing measures for the prevention or suppression of crimes, policing, including the operative–investigative activities, and protection of public order. This in itself includes the risks of processing personal data in breach of legal requirements, as well as in an untargeted and more excessive volume than necessary.

In the course of processing a large volume of data, technological advances allow for conducting the effective analytics as well collecting and analysing data through electronic communications. However, they also present the opportunities and challenges for law enforcement bodies. This is accompanied by the risk of interference with the right to privacy[32], which should be assessed considering the principle of proportionality[33].

On the other hand, the illegal data processing by law enforcement bodies may lead to violations of the rights, honour and dignity of data subjects, as well as discrimination, among other consequences. The primary purpose of the Personal Data Protection Service of Georgia is to protect universally recognized human rights and freedoms, including privacy.

[32] Case of Roman Zakharov v. Russia GC, [2015] ECHR App. No. 47143/06, §§ 227-228, 232.
[33] Case of Z v. Finland, [1997] ECHR App. No. 22009/93, § 94; Case of Khelili v. Switzerland, [2011] ECHR App. No. 16188/07, § 62. Case of Hämäläinen v. Finland GC, [2014] ECHR App. No. 37359/09, § 65; Case of Roche v. the United Kingdom GC, [2005] ECHR App. No. 32555/96, § 157; Case of Gaskin v. the United Kingdom, [1989] ECHR App. No. 10454/83, § 42. Case of Vincent Del Campo v. Spain, [2018] ECHR App. No. 25527/13, §§ 36, 40.

The law enforcement authority, as a body processing a large volume of data, is responsible for all the operations carried out during data processing. The collection of personal data for the purposes of legal proceedings should be limited to the amount that is necessary and proportionate for the prevention of real threat or for investigation and prosecution of the specific crime [34].

During the reporting period, based on the analysis of infringements revealed in the practice of personal data processing by law enforcement bodies, the Service examined 11 (eleven) facts of processing covering almost all the specific areas of activities of law enforcement bodies based on the planned examinations/inspections initiated by the Service at the beginning of the reporting year. A number of sensitive topics were examined, including the issue of notifying data subjects about the covert investigative actions, the condition of compliance with the statutory rules, principles, grounds and security measures for personal data protection during ongoing proceedings in the cases involving the sexual offences committed against women and minors, etc.

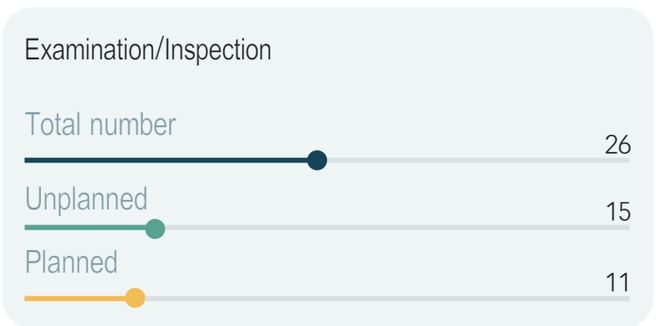
The practice demonstrated that during the reporting period there is a tendency to violate the principle of proportionality in the personal data processing by the law enforcement bodies during the case handling. In particular, during processing the special categories of personal data, such as the untargeted utilization of criminal records (convictions), including those declared annulled, in certain investigative actions, for example, drawing up the photographic identification protocol; also, processing the personal data of the individuals whose photos are necessary as analogues for law enforcement authority; the facts of disclosure to family members without considering the will of an adult during administrative offence proceedings; the cases of aimless photographing of individuals during administrative or criminal proceedings by the representatives of Ministry of Internal Affairs, etc.

When conducting the covert investigative actions and controlling the activities performed at the central databank for electronic communications identification data, as one of its main functions,

[34] EDPB, Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, 2020, §§ 30, 32-34. Case of Kennedy v. The United Kingdom, [2010] ECHR App. No. 26839/05, §§ 120-121, 151-154.

the Service is guided by Article 40[16] of the Law of Georgia "On Personal Data Protection". Such activities and electronic communication companies are monitored by the Service through examining and inspecting the lawfulness of data processing in the electronic monitoring and the special electronic monitoring systems.

During the reporting period, based on applications, 14 (fourteen) violations were identified as a result of 15 (fifteen) unplanned and 11 (eleven) planned inspections, fines were levied in 9 (nine) cases, warnings were issued in 4 (four) cases, and in 2 (two) cases, the liability could not be imposed due to the expiry of limitation period. During the reporting period, 206 (two hundred and six) consultations and 15 (fifteen) instructions were issued.



PLANNED INSPECTIONS

In order to perform the duties imposed by the legislation, the "Topics of the Plan for the Examinations/ Inspections of Lawfulness of Personal Data Processing for 2022" and "2022 Plan for Examinations/ Inspections of Lawfulness of Personal Data Processing" were approved by Order No. 01/23 of the President of Personal Data Protection Service of Georgia on 7 April 2022. The inspections to be implemented in law enforcement bodies were determined considering the salient issues such as the impact on specific target groups or areas, within which the lawfulness of personal data processing

is of crucial importance. Accordingly, the planned inspections to be implemented in law enforcement authorities should be focused on examining the lawfulness of processing the personal data of minors, women, and target groups of migrants, including processing of special categories of data. The said inspections also encompassed areas such as modern technologies, covert investigative actions, and electronic communications.

The planned inspections were conducted at the Ministry of Internal Affairs of Georgia, the state subordinate agency within the system of the Ministry of Justice of Georgia – Special Penitentiary Service (hereinafter referred to as the "Special Penitentiary Service"), the Prosecutor's Office of Georgia, the Electronic Communications Company and LEPL – Operative-Technical Agency of Georgia. In addition, the planned inspections related to the lawfulness of processing the data of employed persons were launched in the Ministry of Defence of Georgia and the Special State Protection Service of Georgia in 2022. The inspections focused on protecting the rights of migrants are implemented in the Ministries of Internal Affairs and Foreign Affairs of Georgia.

Although the Law of Georgia "On Personal Data Protection" does not impose other different conditions regarding the processing the personal data of minors, the Juvenile Justice Code should be noted in relation to law enforcement agencies. It regulates the administrative and criminal liability of juveniles, the peculiarities of proceedings in cases of administrative offences and criminal processes involving minors, as well as the special rules for the enforcement of punishments and other measures. It is worth noting that, in order to ensure the welfare of the child and promote the effective implementation of the Constitution of Georgia, the UN Convention on the Rights of the Child, its additional protocols and other international legal instruments recognized by the state, the "Code on the Rights of the Child" has been in force since 2019.

Women's rights comprise the rights and freedoms of women and girls of all ages. International acts such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and other international instruments protect the legal status of women. The fundamental principle relating to the conclusions on women's rights is the prohibition of discrimination against women. It should be noted that the

National Strategy for the "Protection of Human Rights in Georgia" 2022–2030, submitted by the Government of Georgia to the Parliament of Georgia, also deals with the protection of the rights of women and minors.

The processes studied demonstrate that law enforcement bodies process the personal data of women and minors according to their needs and specificities, as stated by the relevant inspections carried out by the Service, in particular:

- *Special Penitentiary Service.* The provision of primary and basic education is compulsory for juvenile defendants/convicts. It is also worth noting that the penitentiary institutions organize the educational–rehabilitation process in order to provide general education and the formation/development of general educational skills for the juvenile defendants/convicts, as well as vocational education for the juvenile convicts. Furthermore, according to the "Code of Imprisonment", the penitentiary institution is obliged to provide the conditions for defendants/convicts to acquire general and vocational education. According to the agreement signed with the Ministry of Education and Science of Georgia within the framework of the "Access to General Education", the juveniles imprisoned in penitentiary institutions are enrolled in public schools, which ensure conducting the courses as envisaged by the national curriculum. The convicts are not the students of one specific school, they are enrolled in the public schools they attended before entering the penitentiary system.

The Special Penitentiary Service provides the Ministry of Education and Science of Georgia with information on juvenile accused/convicted persons, as well as the collects the necessary documents to be submitted for the enrolment of a student in the general education institution and ensures their timely delivery to school upon request. Furthermore, the penitentiary institution facilitates the participation of accused/convicted persons in external, certification and national examinations.

Penitentiary institutions process the personal data of juveniles and participate in the process of providing general education to them, only in case the convict does not have a parent/legal representative. Otherwise, the processes are sharply demarcated, and the penitentiary institutions do not share the personal data of minors to public schools. On the other hand, the legal representatives

of the minors express their consent in writing to processing of the minors' personal data. However, during the inspection it was revealed that the aforementioned consent form, which was a pre-designed model document, did not reflect all the data to be transmitted to the Ministry of Education and Science. In addition, the consent form encompassed the data that was not disclosed by the Penitentiary Service.

Accordingly, with the aim of protecting the best interests of the minors placed in the penitentiary institution, as well aligning the consent declared by their legal representative with their actual desire, and simultaneously avoiding the risks of improper processing of children's personal data, the special penitentiary service has been instructed to modify the forms of written consent to ensure that the forms precisely reflect only the information shared with the Ministry of Education and Science of Georgia.

- *The Ministry of Internal Affairs of Georgia.* The inspections carried out encompassed the lawfulness of personal data processing, including special categories of personal data, through the monitoring systems and the registry of persons convicted and deprived of rights for crimes committed against sexual freedom and inviolability, that was established in accordance with the Law of Georgia "On Combating Crimes against Sexual Freedom and Inviolability". It is noteworthy, that the mentioned systems are new and their inspection has been conducted for the first time.

As a result of the examinations carried out, it was established that the Ministry of Internal Affairs of Georgia produces the aforementioned electronic monitoring program and registry to facilitate the identification of the offender in case of the crime prevention and repeated offences to be committed by individuals. Additionally, the registration of personal information pertaining to the aforementioned persons and the processing of their data are regulated by the Law of Georgia "On Combating Crimes against Sexual Freedom and Inviolability" and other normative acts. The registry and electronic program contain personal data pertaining to both ordinary and special categories of convicted individuals and those deprived of their rights, including information about place of work, qualifications, border crossing, vehicle and weapon data. The aforementioned program also uploads the documents received and prepared during personal proceedings.

In order to assess risks, determine preventive and precautionary measures, as well as document the reasons for taking the specific measures through the electronic monitoring program, there is necessity to process data to a specified extent. Based on the risk assessment, the case manager should pursue the strategy for the form of monitoring, as the law offers the opportunity to utilize various measures. As regards the registry itself, it should be noted that there is not reflected any information on crime victims, and the registry itself does not contain such graphs. At the same time, it should be highlighted that the inspection implemented by the Service identified the circumstance that the personal data of women and children were not processed through the registry at all, and similar data was processed in the monitoring program to an extent proportionate to the relevant legitimate purpose. The examination also revealed that, taking into account the rules stipulated by various legal acts and mechanisms in force, as well as the measures taken by the Ministry of Internal Affairs of Georgia, including those related to data access and security issues, were, in fact, in compliance with the requirements of the Law of Georgia "On Personal Data Protection".

- *Prosecutor's Office of Georgia.* The Service also examined the lawfulness of processing personal data of juveniles and women to be questioned as witnesses through the program for electronic criminal proceedings.

It is worth noting that all the investigative bodies also conduct investigations in the electronic form, where the witnesses to be interrogated are registered and their mandatory and non-mandatory data are indicated. The obligatory data to be processed is determined by the Criminal Procedure Code of Georgia, while the necessity for optional data is conditioned by the purposes of law enforcement agencies, which may serve the needs of disabled witnesses, crime prevention, analytical activities, or statistics. The inspection revealed that only the mandatory information from the registration data was recorded into the witness's interrogation protocol. However, based on the technical parameters of the software, it was impossible to complete the interrogation process without indicating the status of "ethnic origin" and "disability". Hence, the specified data was technically mandatory to be indicated.

The inspection established that the need to fill in the data on a disabled person stemmed from the

obligation enshrined in the UN Convention on Persons with Disabilities and served a legitimate purpose. A witness with a disability is further additionally informed about his/her rights and all his/her needs are provided during the interrogation process. As regards the information on ethnic origin, the Prosecutor's Office of Georgia has pointed out that the said information is processed for statistical and analytical purposes, and the only source of its acquisition is the data subject who voluntarily provides the data. However, the Law of Georgia "On Personal Data Protection" does not apply to the processing of such special categories of data during the interrogation of a witness.

In order for the consent given by the data subject to be considered legitimate, a number of requirements must be met. In particular, it is important to provide data subjects with the information prior to obtaining their consent. They must be informed during the decision-making process and be aware of the specific data to which they are giving their consent to be processed.

The inspection revealed that the processing of information about ethnic origin is not envisaged by the Criminal Procedure Code of Georgia or other legal acts. Accordingly, the Law of Georgia "On Personal Data Protection" is applicable to the specified form of processing data on ethnic origin. The processing of information on ethnic affiliation in the mentioned form was assessed as an infringement of law. The Prosecutor's Office of Georgia was held liable for processing the special categories of data without a legal basis and was instructed to take such organizational and technical measures that would ensure the completion of the process of interrogating witnesses without the obligatory indication of persons' ethnical affiliation.

At the same time, one more circumstance identified by the inspection is worth noting. In the program for electronic criminal proceedings, the witnesses were not differentiated according to sex and age. The identical fields to be filled in for minors and women, as well as adults and/or men were different only in the case of minors where the identity of their representative was additionally indicated, that is occasioned by the legislation, in particular, pursuant to Article 23 of the Juvenile Justice Code aiming prevention of the secondary and repeated victimization.

As the aforementioned cases clarify, the planned inspections are necessary to effectively control the

lawfulness of data processing. The plan of inspections was developed considering the trends, current realities, needs and challenges revealed in the activities of the Service, which ultimately facilitate the identification of the areas or issues where there exist the high risks of illicit data processing. The planned inspections carried out by the Service focus on identifying all potential problems and implementing the appropriate measures for their eradication in accordance with the objectives of the Service, that will contribute to setting the standards that comply with data protection legislation.

MAIN TRENDS AND RECOMMENDATIONS

Based on the reviewed cases, it is important for law enforcement bodies to focus on the trends identified as a result of planned inspections carried out by the Service as well as to analyze the ongoing data processing and facilitate the implementation of the recommendations listed below:

✓ When introducing electronic programs/databases and processing of personal data through them, data controllers must take into account the salience of the issue and implement such organizational and technical measures that, having regard to the existence of relevant legal basis, will ensure processing only the data required to achieve the specific legitimate purpose;

✓ When processing special categories of data, where the consent serves as legal basis, the data subjects shall be informed in a transparent and explicit manner to be clear for them which and what proportion of data they are giving their consent to be processed;

✓ In the course of data processing, the juveniles' best interests and needs must be taken into consideration.

THE RIGHT OF DATA SUBJECTS TO BE INFORMED

During the reporting period, there were a number of applications relating to the improper informing of data subjects by law enforcement bodies. The cases examined clarified that the problem lies in the failure to inform data subjects in accordance with the Law of Georgia "On Personal Data Protection". The issue is even more significant when law enforcement bodies process personal data on a daily basis in various ways, including collecting, photographing, storing, using, disclosing, as well as accessing large volumes of data.

At the request of the data subject, the law enforcement body is obliged to provide not only the information, but the copies of documentation existing in the agency about this person as well. It is noteworthy that informing the data subject is linked to the exercise of other rights, enshrined in the law, by that person, including the right to erasure, correction or appeal against the incorrect data. Consequently, the failure to obtain the information/documentation within a reasonable period of time may be detrimental to the interests of the data subject.

During the reporting period, in consequence of the specific case studies, the following shortcomings of law enforcement bodies were demonstrated in terms of informing data subjects:

- *State Security Service.* In the review of a citizen's application, the Service clarified that the law enforcement body had not processed the applicant's personal data and the data subject was informed about it during the examination process conducted by the Service, in particular, 1 month and 17 days following the submission of the request by the applicant.

Since the State Security Service did not process the applicant's personal data, the agenda was set for assessing whether it was obliged to inform the applicant under Article 21 of the Law of Georgia "On Personal Data Protection". It is important for the data subject to confirm or reject the fact of processing itself. The mentioned standard is approved by the international acts as well. The Regulation of the European Parliament and of the Council of 27 April 2016 (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data (General Data Protection Regulation), and 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 strengthen the right of the data subject to receive confirmation from the data controller as to whether their personal data is being processed.

In the case at hand, it was established that the law enforcement body had the obligation to inform the data subject under Article 21 of the Law of Georgia "On Personal Data Protection", irrespective of whether or not the data is processed. The notification was provided well beyond the statutory 10-day deadline. Considering the circumstances, the case in question established the fact of administrative offence.

- *Investigative Service of the Ministry of Finance.* The data subjects applied the investigative authority and requested information/documentation about them specifying the form of their receipt and instructions for sending the data to the email address indicated in the application as well.

The data controller explained that in the case in question, there were grounds for restricting the right, of which the applicants had been informed through the telephone communication. While examining the application, the data controller was unable to provide evidence proving that the applicants had been provided with the relevant information about the basis for restricting the data subject's right during the telephone communications.

However, the actions of the investigative service of the Ministry of Finance were not deemed to be effective, as the applicants could not receive the comprehensive and proper information about the restriction of their rights. In addition, their repeated statutory request for getting clarification in writing, particularly by email (which the data subject has the right to choose) was ignored by the data controller. Considering the above-mentioned, the fact of an administrative offence was established on the grounds of failure to inform the data subjects in the due manner.

- *Special Investigative Service.* The data controller did not have the specific documents requested by the data subject about him/her, of which he/she was made aware shortly after the submission of the application. However, the applicant was informed of it one (1) month later when he submitted a repeated application with the same request.

Giving consideration to the circumstances examined, the data controller was in a position to inform the applicant in a shorter period of time. Furthermore, it is an established fact that there are no such factors or limiting circumstances that would make it impossible to fulfil the said obligation on time. Within the framework of the investigation the data controller was explained that, regardless of whether or not they processed the material requested by the applicant, they should not have allowed the said process to be unreasonably delayed, especially as the investigative service could not point to any circumstance that could be considered as an objective reason for the period used to inform the data subject.

Taking into account all of the above, the Service established the fact of the administrative offence. In case of the data subject's request for the documentation containing his/her personal data, the data controller has been instructed to promptly and within reasonable timeframe inform the data subject, as well as in case of the absence of sufficient grounds to restrict the data subject's right. This applies regardless of whether or not the personal data of the mentioned individual is being processed. Taking the aforementioned into account, the Service established the administrative offence.

The cases studied have clarified that informing the data subjects within the statutory deadline is a problematic issue. The challenge again lies in the delivering copies of documentation reflecting information about data subjects within the reasonable time limit and informing the data subjects properly, which also includes their provision with complete information or documentation related to data processing. Even if there are grounds for restricting the right, it is crucial to inform data subjects in a way that properly conveys the purpose of the restriction. Additionally, despite the existence of the grounds for restriction, there is no guarantee that the data subject will receive the information in the requested format.

MAIN TRENDS AND RECOMMENDATIONS

✓ Data controllers must ensure that data subjects are properly informed according to the rules and terms establitshed by the law, even in circumstances when the grounds to restrict the right are present or applicants' data are not processed;

✓ Apart from the information, data controllers must provide data subjects with copies of existing documentation upon request;

✓ Despite the circumstance that Article 21(5) of the Law of Georgia "On Personal Data Protection" does not set the deadline for the transfer of documentation to data subjects, the data subject's request must be satisfied within a reasonable time limit and at the very first opportunity. Additionally, it is important that data controllers do not unreasonably delay the period necessary for the transfer of documentation;

✓ In case of data subjects' reasonable expectations, when processing their personal data by law enforcement bodies, it is essential for data controllers to properly inform them, even if they do not process the data of a particular data subject.

THE STORAGE, DISCLOSURE AND PUBLICIZING OF THE DATA BY LAW ENFORCEMENT AUTHORITIES

A certain part of the inspections carried out by the Service in 2022 were related to data processing, including storage, disclosure to the third parties and/or publicizing by the law enforcement bodies. Since law enforcement authorities hold and store a large amount of data as part of their functions, it is expedient to define the specific storage time limitation, because the indefinite possession of subject's data by such agencies creates the risks of processing personal data in violation of legal requirements. Law enforcement bodies must take special care prior to providing the access to data for the third parties. Additionally, the disclosure of information on the Internet and in the media

poses the increased risk to the data subject, since the data becomes available to a wide range of society. The disclosure of special categories of data, such as the criminal records, as well as the imposition of preventive measures against an individual, can be particularly damaging. In such cases, it is crucial to take operative-investigative measures, since in this process they have access to such data, if disclosed, could cause significant harm to data subjects.

It is also noteworthy that, in terms of data processing in the mentioned manner, there occurred repeated instances of unlawful data processing performed by the same law enforcement body during 2022. As evidenced by the cases examined during the reporting period, law enforcement bodies often cite the performance of their assigned functions and duties as the reason for storing/disclosing personal data, although this does not justify the disregard of the principles of consistency of proportionality in relation to the purpose of data processing:

- *Prosecutor's Office of Georgia.* Since 2013, the Prosecutor's Office of Georgia has been publishing on its official website the personal data of citizens, including the information that falls under special categories of data, such as data related to their detention and the imposition of preventive measures. As regards the grounds for data processing in the specified form, the data controller, being a public agency, was accountable to the public in compliance with the public interest and periodically provided the society with information about its activities and actions implemented.

Obviously, the considerable public interest may serve as the basis for personal data processing, however, the existence of legal grounds for processing the special categories of data must be assessed on a case-by-case basis.

It is worth noting that after the commencement of inspection by the Service, the data controller assessed the need to publicize the indicated information and deleted the data. In this case, as a result of the inspection, the Service stated that the data controller may have had a legitimate basis and purpose for providing the public with information about the measures taken in connection with possible unlawful actions committed by the organized group and posting the relevant information on the official website. However, the achievement of this purpose did not necessitate the disclosure of

identifying information (name and surname) of data subjects. Moreover, the data controller had no grounds to process special categories of data (imposing the preventive measure).

Taking into account all the above-mentioned, the Prosecutor's Office of Georgia was held administratively liable under Article 44, Paragraph one (violation of data processing principles) and Article 45, Paragraph one (processing the special categories of data without the grounds envisaged by the Law) of the Law of Georgia "On Personal Data Protection" on the grounds of committing the administrative offence. At the same time, it was instructed to bring the information, similar to the one published on the website, into full compliance with the Law of Georgia "On Personal Data Protection" by either placing personal data in an exclusive form or deleting them.

- *The Ministry of Internal Affairs of Georgia.* Within the review of the application, the Personal Data Protection Service of Georgia examined the lawfulness of the storing the data subject's criminal records in the electronic database of the Ministry of Internal Affairs of Georgia.

During the inspection, it was established that the database contained the information about convictions that had been expunged 20 years ago. The Ministry of Internal Affairs cited the Laws of Georgia "On Weapons" and "On Combating Crimes against Sexual Freedom and Inviolability" as the grounds of processing, the provisions of the laws restrict certain rights even after the expunging and/or sealing of criminal records. Additionally, according to Georgian criminal law, in order to decide on the issues relating to deferring the execution of the court's order, releasing the convict from further serving the sentence, reconsidering /commuting the imposed life imprisonment to less sever sentence and applying the suspended sentence, the court may take into account the convict's past crime.

It should be noted that the period and purpose of active form of storage and archiving of criminal records are not normatively determined. Additionally, there is no differentiated period of storage for such criminal record information, which is not related to the restrictions stipulated by the laws of Georgia "On Weapons" and "On Combating Crimes Against Sexual Freedom and Inviolability". In the cases under review, the necessity to store the applicant's past convictions was not caused by

any of the above-mentioned laws, and in general, the data controller indicated that there existed no specific purpose for its storage.

Based on the above-mentioned, the information on the applicant's sealed criminal records was available to all the persons who had access to the relevant data, and such an arrangement could not ensure limited access to the data. Indeed, the data controller was entitled to process data on criminal convictions (including those sealed or expunged) for a certain period of time. However, depending on the Law of Georgia "On Personal Data Protection", international and national legislation and judgements/rulings of the European Court of Human Rights and Constitutional Courts of Georgia, the Service considered that the storage of the said information indefinitely did not comply with legal requirements.

Thus, the data controller was held administratively liable pursuant to Paragraph 2 of Article 44 of the Law of Georgia "On Personal Data Protection" (the infringement of data processing principles by the person who has been the subject to the one-year administrative fine for the violation under paragraph one of this Article) stipulating administrative offenses. At the same time, the data controller was instructed to determine in writing the storage period, which is proportionate to the purpose of processing the data of individuals' criminal records, and which will be differentiated according to the respective needs, excluding the possibility of storing data permanently. However, once the purpose(s) of processing have been achieved, the data on criminal records must be deleted or stored in the unidentifiable form. Also, the data controller was instructed to delete the criminal record data of the applicant from the relevant database or store it in the non-identifiable form.

- *Ministry of Internal Affairs of Georgia.* On the basis of a data subject's application, the Service examined the lawfulness of disclosure of the applicant's personal data to third parties by the data controller.

As a result of reviewing the application, it was established that the law enforcement employee had confiscated the applicant's belongings and attempted to contact the applicant multiple times on his/her registered telephone number with the aim of their recovery, but these attempts were unsuccessful. Subsequently, the information database was searched for an alternative telephone

number belonging to the applicant's mother, which the law enforcement employee discovered after calling the number in question. However, the law-enforcement employee provided the applicant's mother with such personal information about her son that she was previously unaware of. Specifically, he informed her that he was contacting the applicant about the fact that the knives had allegedly been seized from her son and she was summoned to the police administrative building to return the items. It is noteworthy that the purpose of contacting the applicant was solely to summon him to the police administrative building to retrieve his belongings, but the law enforcement employee exceeded this legitimate purpose by disclosing more information to the unauthorized person than it was necessary.

The data controller was held administratively liable under Paragraph 2 of Article 44 of the Law of Georgia "On Personal Data Protection" for violation of data processing principles by a person who had been subject to the administrative fine within a year for the violation envisaged by Paragraph one of this Article. The grounds for holding the data controller liable were based on the commission the administrative offence.

MAIN TRENDS AND RECOMMENDATIONS

✓ Upon disclosing information on the official websites of law enforcement bodies, the compliance with the rules on data processing is particularly important, as it makes the data easily accessible to the unlimited range of people and greatly increases the risk of harm to the data subject. Accordingly, data controllers should limit the publicizing of personal data at maximum and confine themselves to disclosing the information to the extent required to achieve the legitimate purpose, if necessary;

✓ It is important for law enforcement bodies to periodically monitor the information posted on their websites and social media sites and ensure the removal of the data that does not have grounds to be processed in the similar form;

✓ The examined processes clarify that with the aim to raise awareness and qualification it is

expedient to conduct the periodical retraining of the persons employed in law enforcement bodies on the issues related to personal data processing;

✓ It is essential to determine the differentiated terms for storing the information about the criminal records that are consistent with the purpose of data processing and exclude lifelong data retention. At the same time, the conditions for archiving, disclosing and accessing to such data must be defined;

✓ The principles of data processing must be strictly adhered to, and once the relevant purpose(s) have been achieved, the data must be deleted/destroyed or stored in a personally non-identifiable form.

DATA PROCESSING IN THE COURSE OF INVESTIGATION

Despite the functions of law enforcement agencies, legislation does not establish the possibility for them to collect data indefinitely. Considering that data processing may have a significant impact on the protection of data subjects' rights, this further increases the importance of implementing data processing by data controllers with the sense of responsibility.

During investigations, the investigative bodies often need to obtain the computer-based data. It should be noted that within the investigative actions relating to the computer data, the number of cases of data processing without the grounds stipulated by the law has decreased. The instances of viewing the video recordings in the computer system by law enforcement officials without a judge's ruling or a prosecutor's decree has taken on more topicality.

- *The Ministry of Internal Affairs of Georgia.* One of the cases discussed during the reporting period related to the viewing of video footage by the representatives of the law enforcement body.

During the examining of the case, it was established that, as a part of an ongoing investigation,

occasioned by the interests of the investigation, the employee of the Ministry of Internal Affairs of Georgia watched the video recordings of the camera installed on the outer facade of the residential building. The examination demonstrated that viewing the video footage may indeed be relevant to the proceedings; however, when assessing this issue, attention should have been focused on the rules and procedures for computer data processing within the investigation.

It is worth noting that the Criminal Procedure Code of Georgia establishes the special rules and conditions for conducting the investigative actions related to computer data. The Code clearly states that computer data–related investigative actions may only be carried out by ruling of a judge or, in cases of urgent necessity, by the decree of a prosecutor; In addition, even in case of reviewing the investigative action – if said action concerns private property – there must exist the court ruling or the prosecutor's decree, in case of emergency.

During the process of examination, the Service stated that the standards established by the legislation was not followed and the viewing of the video surveillance footage of the residential building was not implemented within the framework of investigative actions envisaged by the Criminal Procedure Code of Georgia. Furthermore, the case in question did not represent an operational investigative measure and the employee of law enforcement body gained the access to video recordings only based on the letter that did not specify the relevant legal grounds and the need to view the recordings.

Thus, the action of the Ministry of Internal Affairs of Georgia was deemed as data processing implemented without a proper legal basis, and the extent of liability was applied as envisaged by the legislation.

When investigating criminal cases, personal data of various individuals are processed in the course of each investigative action. During the reporting period, the Service examined the case involving the processing the data of analogous individuals in the process of photographic identification of persons.

- *The Ministry of Internal Affairs of Georgia.* One of the cases examined related to the personal data processing during the investigative process, in particular referred to photographic identification.

During the inspection, it was established that as part of an ongoing criminal investigation, for the purpose of investigative action – photographic identification — the information on the analogous individuals was processed and their demographic data was reflected in the protocols of photographic identification. It should be emphasized that since the investigative action was carried out in connection with the identification of specific individuals from the photographs, the said process only required the physical characteristics of persons presented for identification and their demographic data had no relation with the ongoing investigative action.

The data controller cited the avoidance of ambiguity and uncertainty for the defence as the supportive argument for recording the demographic data of the individuals concerned in the report, as the law enforcement body had not used such means to clarify the source of the data, nor has any action been taken to achieve the above objective through processing less amount of data. According to the explanations of persons conducting the investigative actions, the demographics of the analogue persons had absolutely no relevance for the photographic identification and did not serve the purpose of investigative action. It only necessitated the visual resemblance of the persons presented for identification.

It should be noted that the Criminal Procedure Code of Georgia (including Articles 131 and 135) does not oblige the drafter of the identification report to reflect the demographic data of other individuals in the report, and conversely, it explains that the report reflects the individual and/or generic characteristics of the other person presented for identification, as opposed to the data of identifier and the person presented for identification.

Considering the above mentioned circumstances, in the photographic identification protocols the data of analogous persons was processed in the volume of inconsistent and disproportionate to the purpose, thus establishing the fact of administrative offence. The Ministry of Internal Affairs of Georgia was imposed the appropriate administrative fine and instructed to decide the necessity of

indicating the analogous persons in the report according to the specific needs of proceedings and for this purpose to develop the guidelines in case of photo identification.

- *Some of the cases examined during the reporting period* also dealt with the issues relating to the request for information and its inclusion in the criminal case in the course of investigation. The Service is applied by the citizens who contest the processing of documents containing their personal data within the criminal case, in particular, the attachment of such materials to the criminal case, which will be submitted to the court and shared with the parties involved.

In one of the cases, the applicant pointed out that the documents containing his personal data was kept as part of a specific criminal case and had been submitted to the court and shared with the defence party as well. The review of the case confirmed that documents containing specific personal data were included in the criminal case file, which had been submitted to the court and also shared with the parties. Regarding the storage of documents within the criminal case, the Ministry of Internal Affairs stated that the purpose of the investigation is to collect the evidence related to the crime. In the case to be discussed, it was necessary to process the specific information that was subsequently attached to the criminal case.

In the course of the investigation it was established that, based on the motion proposed by the defence party in the pre-trial hearing, the court considered lawfulness of obtaining the evidence and its inclusion into the case and concluded that the contested evidence had been obtained without a material breach. Accordingly, the aforementioned position of the data controller was shared. The issue of criminal case files submitted to the court represents the data processing for the litigation purposes in court that may interfere with the proceedings before the court reaches the final decision, and to which Article 3, Paragraph 3, Sub-paragraph "b" of the Law of Georgia "On Personal Data Protection" is not applicable. Also, in the case in question, there was the necessary legal basis for transferring the data to the defence party as provided by the Criminal Procedure Code of Georgia.

MAIN TRENDS AND RECOMMENDATIONS

✓ It should be noted that data controllers perform the special role in terms of implementing the appropriate measures for data protection during the investigation. It is important to limit access to data at maximum as well as to monitor the cases of access to data and record the facts related to the transfer of data, which will significantly reduce the incidents of unauthorized persons' access to the documentation existing within the criminal case;

✓ Law enforcement bodies should always take into account the peculiarities of individual investigative actions or operative – investigative measures and their purpose, and the appropriate volume of personal data to be processed. In some cases, the mentioned may necessitate processing the demographic data, and in some cases — quite the contrary;

✓ The objective set can be achieved by processing a minimum amount of data. In case of processing a large amount of data, the data controller assumes more responsibility. The data controller has to justify the purpose of data processing and the existence of legitimate basis for all the information.

✓ The Criminal Procedure Code of Georgia, the Law of Georgia "On Operative Investigatory Activities", the Law of Georgia "On Police" and other legal acts and regulations allow the law enforcement bodies to carry out a number of actions. Therefore, when it is necessary to conduct a certain action by the data controller, they must be provided with the full information about it, as well as be informed about the purpose and legal basis of the action to be taken. Accordingly, only the written statement, which does not indicate the mentioned circumstances, cannot suffice to assess the restriction of the right as legitimate.

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

The Personal Data Protection Service of Georgia monitors the covert investigative actions round-the-clock, for which it uses electronic monitoring and special electronic monitoring control systems so as to have a full view of the covert investigative actions initiated (the covert wiretapping and recording of telephone communications) in the current mode. The Service receives the electronic copies of court rulings and the prosecutor's decrees submitted by the LEPL — Operational-Technical Agency of Georgia through the same electronic system.

On the basis of the above-mentioned, the Personal Data Protection Service of Georgia is provided with the documents related to the implementation of covert investigative actions round-the-clock. The Service analyses them by comparing the paper copies of court rulings with the decrees of prosecutor's office and determines the correspondence of documents with electronic systems as well.

In order to take control over the covert investigative actions using the above indicated mechanisms, the Service exercises, within its competence, the following powers:

✓ In case the requisite or data in the requisite and/or resolution sections of the judge's ruling on the issuance of permit for the secret investigative action presented to the Personal Data Protection Service of Georgia in the electronic and material form do not match or contain ambiguities, the Personal Data Protection Service of Georgia notifies the agency about it via the electronic system, which, in turn, immediately informs the prosecutor or the authorized representative of the relevant investigative body;

✓ Upon the receipt of the said information, the prosecutor applies in writing to the court issuing the ruling, which ensures the removal of ambiguity-inaccuracy existing in the judge's ruling within 12 hours following the receipt of the application and is obliged to forward the ruling to the Personal

Data Protection Service of Georgia within 24 hours after the elimination of the ambiguity–inaccuracy.

In addition, the Personal Data Protection Service of Georgia is entitled to terminate covert wiretapping and the recording of the ongoing telephone communication in the process of monitoring if:

✓ Covert investigative action ––covert wiretapping and recording of the telephone communication is launched without LEPL – Operative–Technical Agency of Georgia having submitted the electronic copy of the judge's ruling regarding the permission to initiate the covert investigative action, which contains only the requisites and resolution section;

✓ The hard (document) copy of the court ruling is not submitted to the Service within 48 hours of the ruling being announced by the court;

✓ Within 12 hours of the commencement of covert wiretapping and recording of the telephone communications, the prosecutor's decree issued on the grounds of urgent necessity is not submitted;

✓ The requisites and/or the resolution section of the prosecutor's decree submitted through the electronic system or in the paper form, contain ambiguities and inaccuracies;

✓ The data in the requisites and resolution section of the electronic copy of the prosecutor's decree submitted through the electronic system and the data in the requisites and resolution section of the prosecutor's decree submitted in the material form do not coincide.

The LEPL –– Operative–Technical Agency of Georgia, the court and the prosecutor or the authorized representative of relevant investigative body within their competence are obliged to submit the material and electronic copies of the court ruling or the prosecutor's decrees confirming the elimination of the grounds for suspending the covert investigative action to the Service. The covert investigative action is continued after the Service has programmatically acknowledged the receipt of specified documentation. In addition, if the reason for its suspension is not eliminated within 3 days following the suspension of covert investigative action, the materials obtained as a

result of the covert investigative action are destroyed in accordance with the procedure prescribed by the Criminal Procedure Code of Georgia.

According to the Criminal Procedure Code of Georgia, the state authority with the relevant competence is obliged to draw up the protocol immediately after the completion of the covert investigative action, which will be immediately submitted to the Personal Data Protection Service of Georgia as well. The Code envisages the procedure for destroying the information/material obtained as a result of the covert investigative action and Part 5 of Article 1438 of the Code stipulates the obligation to submit the protocol on the destruction of material obtained as a result of covert investigative actions to the Service.

Apart from the above-mentioned, Chapter XVI1 of the Criminal Procedure Code of Georgia establishes the rules on the recognition of lawfulness of an ongoing/conducted covert investigative action and the extension of the term of its implementation as well as the recognition of the ongoing/conducted covert investigative action as illegal, its termination, the annulment of results and the destruction of materials/information obtained as a result thereof and the rules on informing the objects of covert investigative action.

In addition to the covert investigative actions, for controlling of which the electronic control systems are utilized, the Personal Data Protection Service of Georgia implements the supervision of covert investigative actions through examining/inspecting the lawfulness of data processing by the data processor/controller under Subparagraphs "b", "d", "e" and "f" of Paragraph one of Article 143^1 of the Criminal Procedure Code of Georgia.

With regard to the supervisory mechanisms assigned to the Service, it should also be noted that the oversight of investigative actions envisaged by Articles 136-138 of the Criminal Procedure Code of Georgia are conducted by the personal Data Protection Service of Georgia through comparing the information provided by the law enforcement bodies and the electronic communications service provider as well as the examination (inspection) of lawfulness of data processing made by data processor/controller. In addition, the activities carried out via the central databank for electronic

communications identification data, where the identification data of electronic communications, obtained from various electronic communications companies, are collected, are also supervised by the Service through the electronic control and inspection system. In turn, the electronic control system allows the real-time access to the activities carried out at the aforementioned bank.

Article 20 of the Law of Georgia "On Personal Data Protection" also defines the liability to notify the Personal Data Protection Service of Georgia implying the legal obligation to submit to the Service the court rulings about the permission to authorize the covert investigative action requested by the law enforcement agency, to recognize it as lawful, to reject the permission to conduct it or to recognize it as unlawful. In addition, in case of urgent necessity the Service is submitted the prosecutor's decree for the covert investigative action as well and the electronic copy of the ruling/decree through electronic control system in case of covert wiretapping and recording of telephone communication. The same article stipulates the obligation to inform the Service about the transfer of electronic communication identification data to law enforcement body by electronic communication companies. In addition, as already mentioned, under the Criminal Procedure Code of Georgia, the law enforcement bodies are obliged to submit the protocols on the destruction of materials obtained as a result of covert investigative or operative investigative actions as well as about the completion of covert investigative action.

Within the framework of oversight of the covert investigative actions, the Personal Data Protection Service of Georgia, both at the request of citizens and on its own initiative, carries out the inspection of the investigative authorities as well as of the LEPL – Operative-Technical Agency of Georgia in order to examine the lawfulness of data processing. The Personal Data Protection Service of Georgia also verifies the issue of informing the persons, towards whom the covert investigative actions are conducted by the Prosecutor's Office of Georgia in accordance with the procedure established by Article 143^9 of the Criminal Procedure Code of Georgia.

In case of administrative offence detected as a result of examining the lawfulness of data processing, the Service imposes administrative liability on the offender. Except for the administrative penalties, to eliminate the deficiencies found in the institutions and rectify the revealed deficiencies, the Service

has been issuing mandatory instructions and recommendations. In addition, if the evidence of the offence is detected during the inspection, the Personal Data Protection Service of Georgia is obliged to contact the relevant investigative authority for the response.

It is worth noting that as a result of amendments made to the Criminal Procedure Code of Georgia on September 6, 2022, the different terms for informing the objects of covert investigative action were established, and several crimes were added to the category of crimes listed in Paragraph 2 of Sub-paragraph "a" of article 143^3.

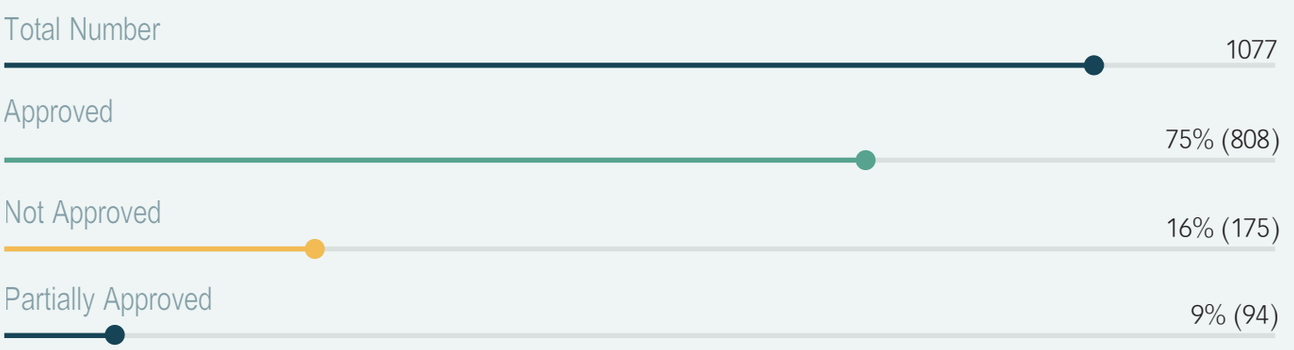
The current version of the Law of Georgia "On Personal Data Protection" envisages the restriction of individual rights of the data subject, including the right to request information by the data subject, if the exercise of this right may jeopardize the interests of state security or protection, public safety interests, crime detection, investigation and prevention, the important financial or economic (including money, budget and tax) interests of the country and rights and freedoms of the data subject and others. Furthermore, the measure in question can only be used to the extent necessary to achieve the purpose of restriction. Therefore, considering the specificities existing in the process of investigating certain crimes, the Personal Data Protection Service of Georgia, based on its mandate, would, naturally, not be in the position to assess the need for this list and the associated extension of the term of covert investigative action.

The need to conduct covert investigative actions in the process of investigation of crimes under certain Articles of the Criminal Code of Georgia and increase their time limits to 3 months at each stage is justified by the investigative purposes and objective necessity.

It is also worth noting, that the procedures for carrying out covert investigative actions, including the legal grounds and the range of persons in respect of whom such actions may be carried out, have remained unchanged. It is important to ensure court oversight is guaranteed at each stage, as well as the control mechanism of the independent oversight authority, the Personal Data Protection Service of Georgia, which remains unchanged. Furthermore, all the procedures for the implementing actions and safeguarding rights that were in force in the previous legislative version, have not altered.

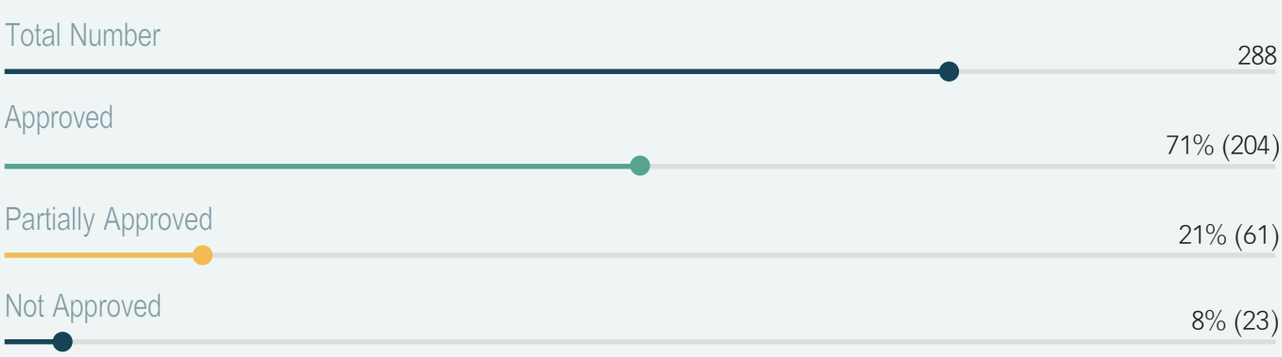
The Personal Data Protection Service of Georgia must actively perform its supervisory function and the activities carried out from this point of view must be based on the circumstances, so that at each stage the necessary legal grounds for processing the data are available, also, the relevant principles must be respected, the data must be processed only insofar as it is necessary to achieve the relevant legitimate purpose and must be adequate and proportionate to the purpose for which it is processed.

The Court Rulings regarding Covert Wiretapping and Recording of the Telephone Communications



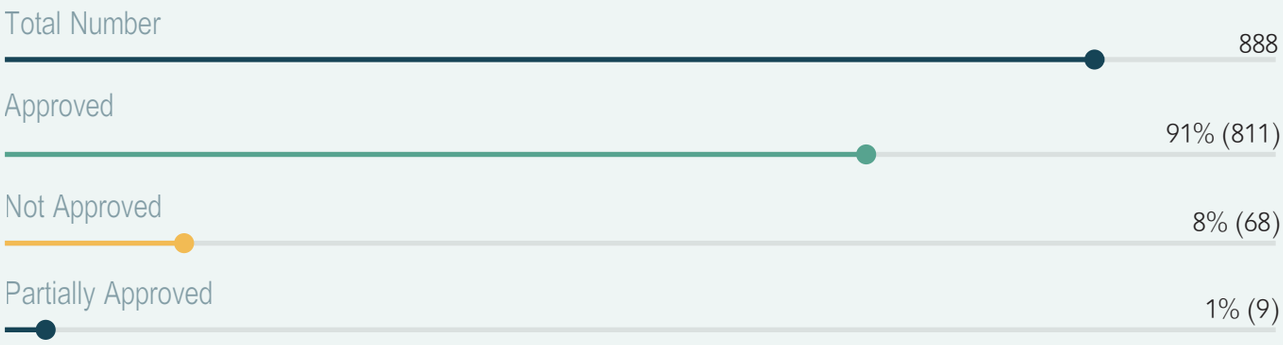
From 1 March 2022 to December 2022, the court considered 1077 motions for covert wiretapping and recording of telephone communication, out of which 75% (808) were approved in full, 16% (175) were not approved and 9% (94) were partially approved.

The Court Rulings regarding the Extension of Term of Covert Wiretapping and Recording of Telephone Communications



The court considered 288 motions for the extension of the term for covert wiretapping and recording of telephone communications, out of which 71% (204) were approved, 21% (61) were partially approved and 8% (23) were not approved.

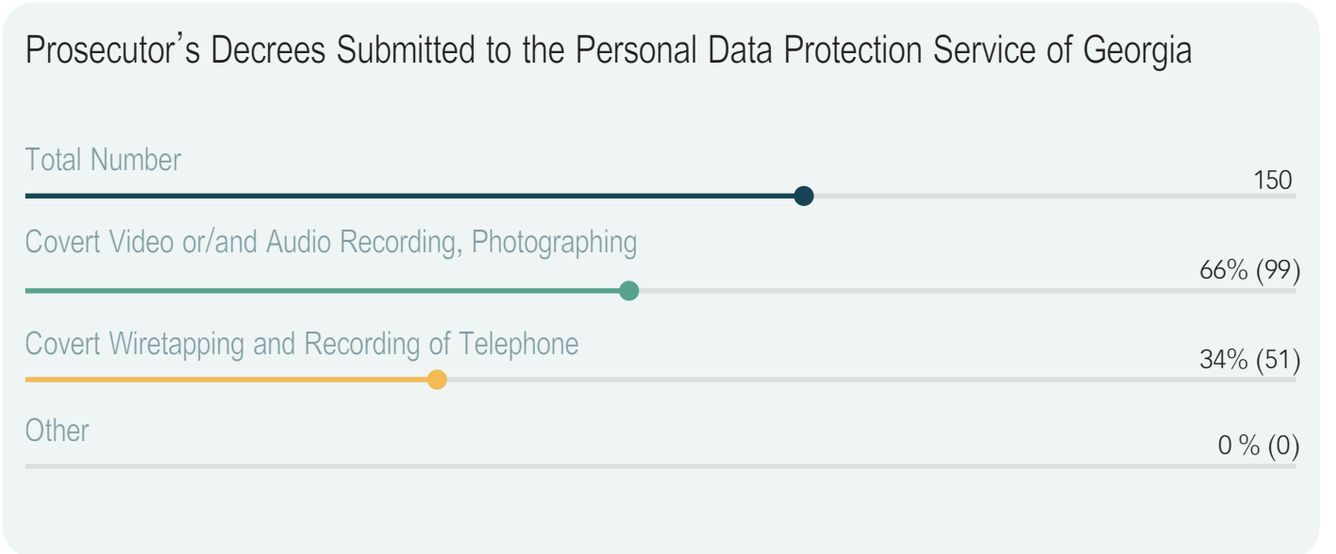
The Court Rulings regarding the Covert Video and/or Audio Recording, Photographing



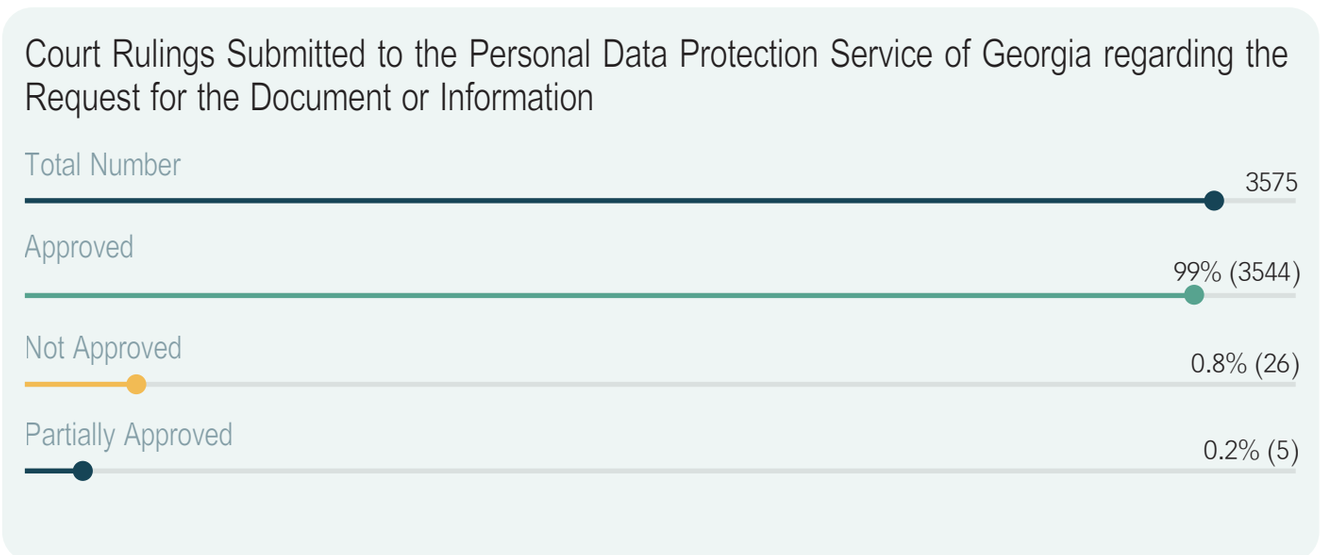
The court considered 888 motions for covert video and/or audio recording and photographing, out of which 91% (811) were approved, 8% (68) were not approved, and 1% (9) were approved partially.

The Court Rulings regarding Extension of Term of Covert Video and/or Audio Recording, Photographing

The court considered 186 motions for the extension of the term for covert video and/or audio recording and photographing, out of which 77% (144) were approved and 23% (42) were not approved.



The prosecutor's decrees for covert investigative actions are submitted to the Personal Data Protection Service of Georgia in case of urgent necessity. Out of the 150 decrees received, 66% (99) of them related to the covert video and/or audio recording, photographing and 34% (51) — covert wiretapping and recording of telephone communications.



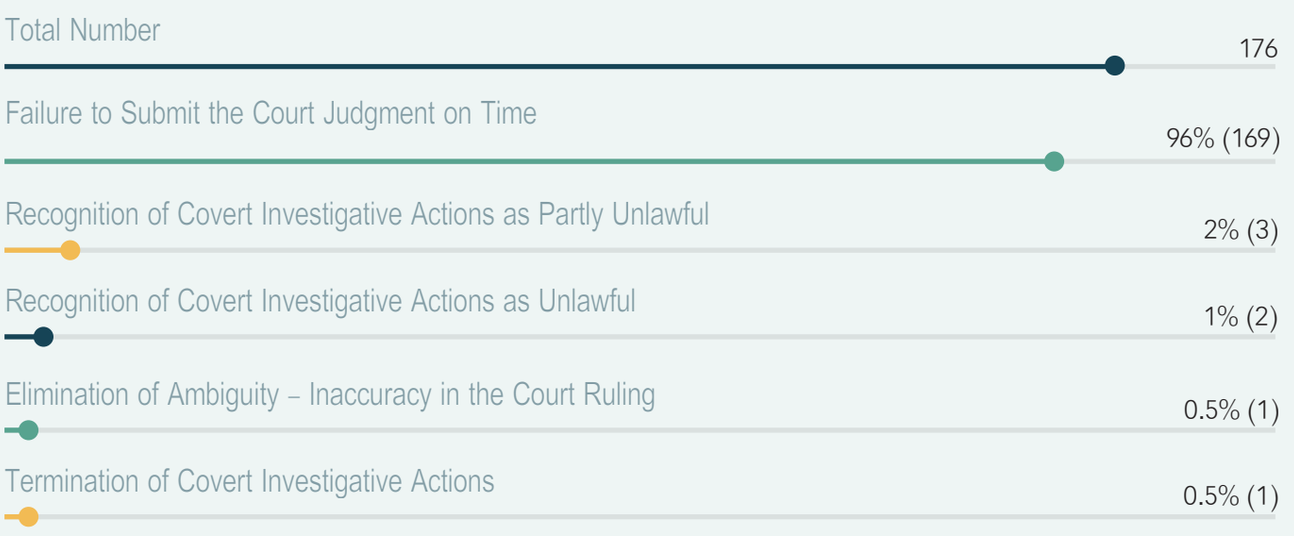
The Personal Data Protection Service of Georgia receives the court rulings and the decrees of the prosecutor occasioned by the urgent necessity to carry out the investigative actions and the request for the document or information pursuant to Article 136 of the Code of Criminal Procedure. Under Article 136 of the Code, the total of 3,575 court rulings were submitted to the Service, out of which 99% of the prosecutors' motions were approved.

PROSECUTOR'S DECREES ON THE SUBMISSION OF INFORMATION OR DOCUMENT OCCASIONED BY THE URGENT NECESSITY

45

Pursuant to Article 136 of the Criminal Procedure Code of Georgia, the Personal Data Protection Service of Georgia received 45 decrees from Prosecutors' Office on the grounds of urgent necessity for the investigative actions — the request of document or information.

Using the Suspension Mechanism



The Personal Data Protection Service of Georgia used the Suspension Mechanism of covert wiretapping and recording of telephone communications (through the electronic surveillance system) in 176 cases, which was caused: by the delayed submission of court's rulings (169 cases), due to recognition of covert investigative actions, initiated on the grounds of the prosecutor's decree based on the urgent necessity, as partially illegal by the court (3 cases), due to the recognition of the covert investigative actions, initiated on the grounds of the prosecutor's decree based on the urgent

necessity, as illegal by the court (2 cases), due to the elimination of ambiguity–inaccuracy in the judge's ruling (1 case) and the termination of covert investigative action by the court (1 case)[35].

USING THE MECHANISM FOR NOTIFYING THE AMBIGUITY-INACCURACY BY THE SERVICE

14

During 2022, various ambiguities and inaccuracies were detected in 11 court rulings and 3 of prosecutor's decrees, which were notified to the LEPL – Operative–Technical Agency of Georgia through the electronic monitoring system. It should be noted that in all the cases the ambiguities and inaccuracy were eliminated within the time limits established by the Criminal Procedure Code of Georgia.

ACTIVITIES IDENTIFIED IN THE CENTRAL DATABANK FOR ELECTRONIC COMMUNICATIONS IDENTIFICATION DATA

79

[35] The decree of the prosecutor on the termination of covert investigative actions was submitted to the Service prior to presenting it to the Operative-Technical Agency of Georgia. Accordingly, the Service terminated the covert wiretapping and recording of the telephone communication before receiving the information by the agency and terminating the investigative action.

Based on the information provided to the Service via the electronic monitoring system of the central databank for electronic communications identification data, the data was issued 79 times by the LEPL – Operative-Technical Agency from the electronic data identification central bank on the basis of the relevant court's ruling.

NOTIFICATIONS SUBMITTED BY ELECTRONIC COMMUNICATIONS COMPANIES

2405

The notifications to the Service were submitted by 15 electronic communication companies, providing the information to the law enforcement bodies 2,405 times during the reporting period on the basis of the court rulings.

CITIZENS' APPLICATIONS REGARDING COVERT INVESTIGATIVE ACTIONS CARRIED OUT TOWARDS THEM

93

The purpose of the Personal Data Protection Service of Georgia is to protect human rights and freedoms, including privacy, accordingly, special attention is paid to monitoring the salient area, such as the covert investigative measures.

In 2022 93 individuals contacted the Personal Data Protection Service of Georgia making a request for the information as to whether they were being subject of covert investigative actions. The Personal Data Protection Service of Georgia responded adequately to all the requests. The Service inspected the applications of data subjects through the mechanisms at its disposal — the documents submitted to the Service and electronic systems, however, there were not detected any circumstances giving rise to the obligation to inform the data subjects established by Article 143[9] of the Code. The Service did not initiate the inspections on the basis of the mentioned applications. At the same time, such applications, according to which the persons made statements on the possible illegal surveillance and wiretapping of their telephone communications, were sent to the Prosecutor's Office of Georgia to receive further response, since in accordance with Article 40[14], paragraph 5 of the Law of Georgia on Personal Data Protection, if the Personal Data Protection Service of Georgia, while carrying out its activities, considers that there are constituted the elements of crime, it is obliged to report on it to the authorized investigative body pursuant to the established law.

PROCESSES STUDIED

In 2022, the data subjects evinced their interest in obtaining the information on covert investigative actions carried out against them. Based on this, the Service conducted the planned inspection of the Prosecutor's Office of Georgia.

In addition, the planned inspections conducted by the Service comprised the electronic communication companies and the inspection of the Operative-Technical Agency of Georgia was launched with the aim to examine the terms of data storage at the central databank for electronic communications identification data and the proportionality of the data issued to the law enforcement bodies[36].

[36] Inspection is on-going.

• *LEPL– Operative–Technical Agency of Georgia.* The Service examined the issue of ensuring the data security during implementing the covert investigative action – the covert wiretapping and recording of telephone communications as enshrined in Subparagraph "a" of Paragraph one of Article 143[1] of the Criminal Procedure Code of Georgia, utilizing the stationary technical possibility to receive the real–time communications by the Agency[37].

No facts of infringement of the legislation were detected within the current inspection, but a number of circumstances that may pose the threat to data security were identified. In consequence of the inspection it was revealed, that the recording of actions performed on the electronic data (so–called "logging") was defective. Accordingly, the Service issued mandatory instructions whose term of implementation has not yet expired.

• *The Prosecutor's Office of Georgia.* Within the inspection, the issue of informing data subjects was examined in relation to the various covert investigative activities. Among them, the inspection encompassed the Territorial Units of Prosecutor's Offices throughout Georgia.

As a result of the inspection, it was stated that in a number of cases the term of appeal was incorrectly indicated in the protocols submitted by the Prosecutor's Office on the notification of data subjects (objects of covert investigative measures) about conducting the covert investigative actions. In particular, when the object of covert investigative actions was informed within the ongoing proceedings, he/she was clarified that the deadline specified for the appeal was one month instead of 48–hour. Also, in some cases, within the completed proceedings the object of the covert investigative action was explained that the term for the appeal made 48 hours. And the mentioned circumstances created the risk that in some cases, the objects of covert investigative actions would violate the statutory term for appeal and would not be able to use the statutory mechanism for it. In the informing process, the incorrect information about the term for appeal could restrict the legally

[37] The content of the inspection constitutes the state secret.

guaranteed right of data subjects to appeal due to the expiry of the statutory deadline.

The Prosecutor's office of Georgia was issued 3 mandatory instructions to carry out on the basis of which the Order of the Prosecutor General on the "Notification about Conducting the Covert Investigative Actions" regulating the rule and conditions of notification was created and issued. In addition, in accordance with the rule on informing the objects of covert investigative actions established by law, the forms of protocols with annexes have been developed, so that all the objects of covert investigative actions can be notified in adherence of the common standards.

- *The Electronic Communication Company.* In order to verify the compliance with the obligation to notify the Service about the electronic data identification, which had been provided for the law enforcement bodies as prescribed by the Law of Georgia on Personal Data Protection, the Service conducted the planned inspection of the company. Within the inspection, the documents received from the court and the electronic communication company were processed and analysed, compared and identified whether the Service had been notified in all the cases.

The inspection revealed that in all the cases the company submitted the notifications regarding the information, having been provided for the law enforcement bodies, to the Service during 24 hours, the vast majority of which contained the information on the subscriber's demographics or the detailed transcripts of incoming and outgoing calls and text messages.

The company failed to inform the Service in only one case, in particular, when the law enforcement body, based on the court decision, made the request for the information from the company about the payments of the subscriber registered to a natural person. Apart from the account number, the information provided by the company on the basis of the said judgment contained the exact amount paid, the date and source of the payment as well as the subscriber's name and personal details, which allowed to identify the individuals. Occasioned by the fact, that the company did not deem the information provided (account number, amount of money paid, date and source of payment) to be personal data, it did not submit the notification to the Service.

Due to the expiry of limiting period for the offence, the company could not be held administratively liable, however, it was instructed to submit notifications within the statutory 24–hour period even in the case of providing the information on the identifiable electronic communication data relating to a natural person, including a customer's payments and services rendered[38].

When conducting covert investigative actions, it is important for law enforcement bodies to strictly abide by the obligations lied down in the Criminal Code of Georgia, as well as to take into account the principle of data minimization and save only those data that correspond to the purpose of the covert investigative actions and the interests of a specific criminal case[39]. In order to ensure the effective oversight of covert investigative actions performed by the Service, it is salient that law enforcement bodies promptly submit the protocols on the completion of covert investigative actions or the destruction of material obtained.

[38] The Service was notified in writing that the instruction had been fulfilled and in similar cases the notifications would be submitted to the Service by the company.
[39] Case of L.L. v. France, [2006] ECHR App. No. 7508/02, § 45; Case of Karabeyoğlu v. Turkey, [2016] ECHR App. No. 30083/10, §§ 112-121.

3.10. IMPORTANT DECISIONS

3.10.1. INITIALS AS IDENTIFICATION DATA OF A DATA SUBJECT

On the basis of the application, the Personal Data Protection Service of Georgia examined the lawfulness of the disclosing the applicant's personal data by one of the law firms on its webpage of the social networking site Facebook.

Within reviewing the application, it was established that the criminal case existing in the proceedings of the Prosecutor's Office concerned the sexual violence against the applicant over many years, for which the court had upheld the acquittal. The defending party (a law firm) posted the details relating to the case on its page of social networking site Facebook. At the same time, it is true that the status did not include the applicant's first and last name, but there were specified his/her initials as well as the case-related details (including the information on the relationship between godfather's and godchild's families participating in the proceedings, the details of the residence of family members, etc.), which, as a whole, allowed to identify the applicant.

Within the framework of the application, the law firm explained that on its side, the data had been made publicly available through the data depersonalization, as far as it was not possible for the general public either to link the information indicated in the status to a specific individual or to identify the applicant. According to its explanation, the personal details of the applicant with the designated status would have been perceivable only to a narrow circle of persons (witnesses and family members of those involved in the case), who were already informed about more significant details of the case than those disclosed through the status. The company additionally pointed out, that the purpose of publicizing of the said information was to restore the acquitted person's damaged dignity and represented the remedy for rehabilitation of the grievous moral damage inflicted to him/her.

The Personal Data Protection Service of Georgia stated, that the Facebook status of the law firm described the circumstances pertaining to the specific criminal case and consequently, to the applicant, thus allowing direct or indirect identification of the data subject without undue effort. The content of the status disseminated by the law firm and the information expressed in the form

of comments on the status effectively excluded the depersonalization of the data. Accordingly, the position of the law firm that it disclosed the applicant's details in an unidentifiable form cannot be shared, since the amount of information disclosed by the law firm and the fact, that the initials disclosed coincided the applicant's first and last name, allowed the applicant to be identified.

Thus, the Personal Data Protection Service of Georgia established that in the process of disclosing the applicant's data through the status on the Facebook social networking page, the principles established by Article 4, Subparagraph "c" of the Law of Georgia on Personal Data Protection were violated and by the decision of the President of Personal Data Protection Service of Georgia, the law firm was found to be in breach of Article 4 on the grounds of committing the offence envisaged by Article 44 of the same law.

3.10.2. CONSENT AS A BASIS FOR DATA PROCESSING AND THE BURDEN OF PROVING EXISTENCE OF CONSENT

On the basis of the application the Personal Data Protection Service of Georgia examined the lawfulness of the applicant's personal data processing through the application — "Mobile Number Database".

According to the information provided by the applicant, processing of personal data, in particular, the mobile phone number, first name and surname, by the application was conducted in breach of the law, as the applicant had never given permission to process his/her data. Relying on the author, the applicant was registered the application in 2019, familiarized him/herself with the relevant agreement during the registration process and consented to the processing of his/her data by the application. In addition, the "e-agreement" was signed by the applicant, on the basis of which the applicant's first name and surname were processed. According to his/her explanation, the general form of the agreement was posted on the application website.

As part of the review of the application, the Personal Data Protection Service of Georgia established that only the "Privacy Policy" was posted on the website, which did not contain any information about processing the data directly of that user (name, surname and mobile phone number), who shared the application with the contacts existing in his mobile phone. In the process of reviewing the application, it emerged that the applicant himself/herself disclosed his/her own phone number to the application. The owner of application could not provide either the information about processing the applicant's name and surname by the application nor the source and legal basis for obtaining it. The Personal Data Protection Service of Georgia explained that according to Article 26, Paragraph 4 of the Law of Georgia on Personal Data Protection, in case of a dispute regarding the presence of the data subject's consent to data processing, the data controller bears the burden of proving the fact of data subject's consent.

Occasioned by the above mentioned, due to processing the information about the applicant's name and surname without the legal basis (bases) established by the Law of Georgia on Personal Data

Protection, the person holding the application was recognized as an offender on the grounds of the offence enshrined in Article 43 of the Law of Georgia on Personal Data Protection and was instructed to delete the applicant's data from the application.

3.10.3. DISCLOSURE OF PERSONAL DATA BY PRIVATE EXECUTOR VIA SENDING LETTER TO A CITIZEN'S EMPLOYER ORGANIZATION

On the grounds of a citizen's application the Personal Data Protection Service of Georgia examined the lawfulness of disclosing the personal data by the private executor via sending the letter to the employer organization of this citizen.

The examination clarified that under the relevant provision of the Law of Georgia "On Enforcement Proceedings" the private executor was obliged to inform the citizen about the initiation of enforcement proceedings against him/her. At the same time, pursuant to the same law, the private executor was obliged to provide the said information to the citizen according to the rule established by the Civil Procedure Code of Georgia on the delivery of court notice. In order to fulfil the above obligation, the private executor prepared the letter containing the information about the initiation of enforcement proceedings, which encompassed the various personal data on the citizen, including the information about the citizen's financial obligation, his participation in the enforcement proceedings with the status as a debtor, the characteristics of the vehicle owned by the citizen, the use of this vehicle as the means of securing the request, etc. The purpose of the private executor was to deliver the letter in question directly to the citizen.

As the mentioned letter could not have been delivered to the citizen at his/her place of residence, the private executor decided to deliver it to the addressee at his place of work in accordance with the provisions lied down in Article 71 of the Civil Procedure Code of Georgia. For this purpose, the private executor sent the citizen's employing organization two letters, which were placed in a single envelope and addressed to the employing organization. In addition, the first letter placed in the envelope was in the name of the employing organization and indicated that the letter intended for the citizen was enclosed as an attachment to be delivered by the employer to the citizen. And the attachment enclosed in the envelope was the letter, addressed to a citizen, which contained the information on the initiation of enforcement proceedings against him/her. It should be noted that the letter addressed directly to the employing organization also contained the personal data of the citizen (e.g. information that the citizen is a debtor in ongoing enforcement proceedings, the identity of the creditor, etc.).

After receiving the communication, the employees of the employing organization not only accepted but they also opened the envelope, as a result of which the letters addressed directly to the employer as well as to the citizen with the personal data indicated in them became available to the employees.

In the decision of the President of the Personal Data Protection Service of Georgia adopted in relation to the mentioned case, it was explained that in order to inform the citizen about the initiation of enforcement proceedings, the private executor has the right to use the means of delivery specified in the Code of Civil Procedure, including the delivery of correspondence containing relevant information to the addressee at his workplace. It should be noted, however, that the Code of Civil Procedure does not contain a priori agreement on the necessity to send the communication directly to the address of administration, if the delivery is made at the workplace. In this case the delivery of the letter can be made by handing in the envelope addressed to the citizen directly to the administration of the workplace or through seeking for the addressee at the place of work, without addressing it to the employer. In the event of failure to complete the above mentioned procedure for one reason or another (including refusal of the relevant employee/person to accept the envelope), the author of the communication has the opportunity to take other measures provided for by the Code of Civil Procedure to ensure the delivery of correspondence. The decision also noted that even if its intended purpose necessitated preparing a separate letter to the employing company (delivery of a letter intended for a citizen), such a letter could have been prepared with the less number of details about the citizen included in it.

The decision also emphasized that by placing the correspondence intended for two different recipients in one envelope and identifying the employer as the sole addressee of the sealed envelope, the private executor failed to ensure the adequate organizational and technical measures to be taken for the prevention of risks associated with data processing.

Occasioned by the aforementioned, due to the processing of citizen's data in violation of the requirements of Articles 4 and 17 of the Law of Georgia on Personal Data Protection, the private executor was recognized as an offender on the grounds of the administrative misconduct envisaged by Articles 44 and 46 of the same Law and was issued the relevant instructions.

3.10.4. LAWFULNESS OF PERSONAL DATA PROCESSING BY PUBLIC ENTITY IN THE DATABASE OF "ADULTS RECOGNIZED AS PERSONS WITH LEGAL INCAPACITY/LIMITED LEGAL CAPACITY"

The inspection established that the electronic database of one of the state agencies contained the data on adults recognized as persons with legal incapacity/limited legal capacity/ beneficiaries of support. In particular, the relevant legal acts are registered on the electronic portal and in this process the relevant data processors (a limited range of persons) are informed about the registration of the person in the database with the following inscription – "The person is considered to be incapable by the court ruling". It should be noted that in order to reflect and update the already reflected information in the electronic database, the mentioned public entity obtains the data from the relevant guardianship and custodial institutions. The inspection also revealed that the portal and its database were located on the server belonging to another state entity that administered it technically and had direct access to the portal database with the right to administer the data.

In regard to the mentioned issue the Service established the inconsistency with the grounds and principle of data processing.

According to the decision of the President of Personal Data Protection Service, the positive obligation of the state is to ensure the participation of persons with limited legal capacity/support beneficiaries in all the areas of social life and create the adequate conditions for the proper exercise of their rights. The aforesaid also implies the provision of full participation of relevant data subjects in administrative proceedings through the development of procedural mechanisms focused on the rights of persons with psycho–social needs and adapted to their requirement, etc. It is noteworthy, that the persons with limited legal capacity/support beneficiaries participate in a number of processes of exercising their rights independently, and in some legal relationships – through a guardian/custodian. It is also important for the lawfulness of a legal act that the person undertaking this action is properly informed of the capacity of the participants in the legal relationship to express their true, informed will and needs existing in this regard. As the inspection revealed, the provision of the above information to the relevant data processors via the electronic database aims at the proper exercise of the rights

and the best, in some cases, vital interests of the participants in legal relationships and serves the prevention of adverse effects on the interests of persons declared as those with limited incapacity/ support beneficiaries.

During the inspection it was stated that the data controller had not defined the specific and clear purposes for processing the data reflected in the "note" column of the electronic database, including the name, surname, personal number, etc. of the guardian/custodian that is a violation of requirements set forth by Article 4 of the Law of Georgia on Personal Data Protection and the grounds for imposing the administrative liability as defined by Paragraph 1 of Article 44 of the same law.

For the proper compliance with the principle of limiting the purpose of data processing the Service deemed it necessary for the data processor to evaluate the specific and legitimate purpose of processing each of the data reflected in the column "note" in the electronic database, to bring the mentioned in consistence with the relevant regulative legal acts and systematically process only the data, given in the columns of relevant designation of the electronic database, which is proportional and adequate to the intended purpose.

The same inspection also addressed the issue of complete updating, reliability and accuracy of the data existing in the electronic database. It is worth noting that the ability of data subjects to properly implement their legal relations pertaining to the relevant legal actions depends on the accuracy of data existing in the electronic database.

The mentioned inspection also highlighted the infringement of rules on data processing by the data processors. It was established that in the course of data processing (including storage) the data controller used the services of the data controller via the electronic database, however, the mentioned circumstance was based neither on the legal act nor the agreement signed under the Law, that constitutes the violation of the requirements envisaged by Article 16 of the Law of Georgia on Personal Data Protection and represents the grounds for imposing the liability prescribed by the first paragraph of Article 51 of the same Law.

Within this inspection the infringement of the rules pertaining to personal data security was also detected. It was established that the individual user and password were utilized to authenticate the portal users. In addition, the portal had the electronic log for recording the actions implemented on the data (so-called "logging"), however, only the information about legal actions registered by the user was logged in the system. The system did not record the following actions: login/logout of the system, the search for a document, opening/viewing/copying of the document. In addition, during the on-site inspection it was detected that the passwords of portal users were stored in the database in an unencrypted, open form.

Finally, on the basis of violations identified during the inspection, the Personal Data Protection Service of Georgia recognized the data controller — a public entity as an offender committing the administrative offence envisaged by the first paragraph of Articles 44, 46 and 51 of the Law of Georgia on Personal Data Protection. At the same time, the offender was given the relevant instructions and determined the terms for their fulfilment.

3.10.5. LAWFULNESS OF A CITIZEN'S PERSONAL DATA PROCESSING BY THE EMPLOYEE OF PUBLIC INSTITUTION

On the basis of a citizen's application, the Personal Data Protection Service of Georgia examined the lawfulness of disclosure of a service recipient's personal data by the employee of one of the public institutions.

According to the information obtained during the examination, a number of data about the citizen, such as name, address and the decision taken by the institution on his/her application, were made available to an employee of the public entity in the course of performing his/her official duties, in particular, in the context of providing one of the specific services. A citizen repeatedly visited the same public entity to lodge the application and appealed against the above decision. Within the indicated grievance, the citizen alleged a personal interest on the part of the employee of the entity. Before the end of the working day, the employee in question contacted the spouse and informed her/him of the identity and address of the citizen receiving the service as well as the content of the grievance aired during the dispute about her/his visit to the entity and the decision taken on the application submitted. Also, the employee got interested if the spouse knew the applicant and had any dispute on the issue relating to the complaint. The employee of the establishment explained, that he/she disclosed the above information to his/her spouse on his own initiative, without receiving any instructions from the employer, because after listening to the citizen's complaint, he/she got agitated and wanted to clarify the matter.

The Personal Data Protection Service of Georgia explained that the disclosure of the applicant's data by the employee of the entity to the spouse went beyond the scopes of data processing for clearly personal purposes and was related to professional activities. When ascertaining this circumstance, the Service focused its attention on the content of the grievance expressed by the service recipient, which was related to official activities of the employee of entity, as well as on the circumstance that the above-mentioned details about the applicant, which fall beyond the professional activities, could not have been known to the employee of the institution. In addition, account was taken of the fact that the disclosure to the third party (spouse) served to clarify the work-related claim.

The Service additionally specified that when disclosing the personal data, the employee of the entity may have evinced the interest in clarification of the claim made against him/her, but this could not be deemed as the benefit worthy of protecting the confidentiality of the applicant's data. It was also pointed out that achieving the desired goal would be possible even without the disclosure of personal data obtained within the professional activities.

The decision of the President of Personal Data Protection Service emphasizes that each employee is obliged to conduct the critical and preliminary evaluation of each fact of data processing and not to use the data obtained as part of professional activities without a specific legal basis.

Occasioned by the above mentioned, due to processing the applicant's data through disclosure without legal basis as provided by Article 5 of the Law of Georgia on Personal Data Protection, the employee of the entity was recognized as the offender on the ground of administrative offence envisaged by Article 43 of the same law.

4. INTERNATIONAL RELATIONS, ANALYTICAL FUNCTION AND ACTIVITIES CONDUCTED IN THE DIRECTION OF STRATEGIC DEVELOPMENT OF VARIOUS SECTORS

One of the main priorities of the Service is to increase the international institutional recognition and to build the high organizational reputation internationally. In order to bring the national legislation closer to international legal instruments and implement the best practices, the Service actively cooperates with foreign counterpart data protection supervisory authorities and international organizations and seeks to deepen relations with them. The Service systematically studies the international field-related trends and existing challenges to ensure the introduction of the best practices and their reflection in daily activities. In addition, the Service is actively engaged in the process of developing and implementing various sectoral policy documents and action plans within area of its competence. In order to implement the short- and long-term priorities for the protection of personal data lied down in the European Union-Georgia Association Agenda 2021-2027, in 2022 the Service carried out a number of activities, among them, at the international level. The Service participated in the process of completing the self-assessment questionnaire of the European Union candidate status and provided the information on the regulatory legislation of the field, as well as on the existing institutional or legislative mechanisms for the effective protection of personal data existing in the country. In 2022 the National Bank of Georgia officially applied for the membership of Georgia in the Single Euro Payments Area – SEPA, in the development of which the Service actively participated in order to exchange information about the regulatory framework of the protection of personal data in Georgia. It should also be noted that within the scopes of the World Bank's GovTech Maturity Index (GTMI) questionnaire, the Service provided the information about the legislative and institutional arrangements for the protection of personal data.

On the path towards European integration, the Service is furthering its institutional development, bringing national legislation closer to European standards, strengthening European values, deepening the cooperation with international partners and incorporating the best practices into its daily activities so as to assure its rightful place among European data protection supervisory authorities.

4.1. INTERNATIONAL RELATIONS

4.1.1. REPRESENTATION OF SERVICE IN INTERNATIONAL FORUMS AND NETWORKS OF THE FIELD

During the reporting period, the Service participated in a number of international fora in the field of personal data protection and privacy. It is worth noting that in 2022 the Service enhanced its international relation, it also was granted the status of membership and the observer in various field-related platforms, which contributes to the increase of its institutional recognition and expansion of existing international partnerships.

During the reporting period, the new delegation composed by the President of Service, the First Deputy President, the Heads of the Department of International Relations, Analytical and Strategic Development and the Legal Department was introduced to the Council of Europe Consultative Committee on "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" ("T-PD"). The President of Service participated in the regular 43th plenary meeting of the advisory committee, where the position of the Service pertaining to the issues on the agenda to be discussed was presented. It is worth noting that the Service actively participates in the activities of the committee and, upon request, periodically shares information on the national legislation and the activities carried out by the Data Protection Supervisory Authority of Georgia.

The Service as an accredited member of the "European Conference of Data Protection Authorities", the so-called "Spring Conference" was also represented at the regular 30th Conference of 2022. In 2022, the conference was hosted by the Croatian Data Protection Supervisory Authority, within the framework of which the President of Service presented the report to the panel discussion. The report concerned the changes made for the purpose of institutional strengthening of the Data

Protection Oversight Authority of Georgia, as well as the legislative regulation of personal data protection in Georgia and the mechanisms for its enforcement, the draft law and the enhancement of international relations and the future plans. At the panel discussion, the speakers discussed the issues related to the effective enforcement of the personal data protection legislation, mutual assistance between EU member and non-member countries, the review of cross-border incidents and the exchange of best practices. The diversity of competences of the Personal Data Protection Service of Georgia was positively acknowledged during the discussion. The Service was actively involved in drafting of 2022 conference resolutions to be adopted as well as in the meetings of working party of the conference ("Spring Conference – Interim Steering Group (ISG)"). It is worth noting that the Service periodically provided the members of the conference working party with its viewpoint on various activities to be implemented by them as well as on the further plans of the conference, the amendments to the regulations and on the organization and outcomes of the "European Case Handling Workshop (ECHW)" held in Georgia in 2022 under the auspices of the Service. In addition, the Service participated in the process of editing the guidelines developed by the conference working party for organizing the European Conference of data protection supervisory authorities.

During the reporting period, the Service participated in the activities of the "Global Privacy Assembly" ("GPA"). The important news is that in 2022 the Service was granted membership of the Assembly Secretariat's Selection Committee, where it is represented alongside the data protection supervisory authorities from Mexico, the UK and Switzerland. The Service participated in the elaboration of a number of draft documents prepared by the Committee for the purpose of selection of the secretariat assembly and will be actively engaged with the mentioned process next year as well. In addition, the Service was granted the status of the Chair of "Working Group on Data Protection Metrics" of the Assembly in 2022. The Working Group was established in 2016 following the adoption of the resolution to develop the "New Metrics" of data protection regulation. It aims to develop internationally comparable statistics on data protection and privacy and, to this end, to study the experiences of data protection supervisory authorities. In addition, it is worth noting, that the Service staff represents the supervisory authority in other working groups of the Global Privacy Assembly: "COVID-19 Related Privacy and Data Protection Issues", "Digital Citizen andConsumer

and Ethics", "Data Protection in Artificial Intelligence", "Data Protection and other Rights and Freedoms Working Group". During the reporting period, the Service participated in the survey conducted under the auspices of the Assembly on the use of artificial intelligence in employment. The close cooperation between the Service and the Global Privacy Assembly is also evidenced by the fact that the information on the mandate and activities of the Personal Data Protection Service of Georgia was published in the May newsletter of the Assembly[40]. Later in the September newsletter, among other publications, there was also published the article by the President of the Service on the topic "Privacy Data Protection and Gender–Sensitive Issues in Georgia"[41]. It is worth mentioning that the President of Service represented the Personal Data Protection Service of Georgia at the annual conference of the Assembly. The conference was held in Turkey and its main topic was: "The Question of Balance: Privacy in the Era of Rapid Technological Advancements". In the closed working format of the conference, the President of Service met with the Heads of Mexican data protection supervisory body. She also held the working meetings with the heads and representatives of data protection supervisory authorities of Turkey, Spain, Uruguay and the UK. During the meetings the perspectives and activities of cooperation between the Personal Data Protection Service of Georgia and foreign supervisory counterparts were discussed in order to foster the objectives defined by the strategy of Global Privacy Assembly.

In 2022, the Service introduced the new composition of delegation to the "International Working Group on Data Protection in Technology", so called "Berlin Group" ("IWGDPT") as well as within the framework of the "Global Privacy Enforcement Network" and the "Central and Eastern European Data Protection Supervisory Authority". The Service has the close collaboration with the

[40] See, GPA, Newsletter, Issue 2, May, 2022, p. 6, <https://globalprivacyassembly.org/wp-content/uploads/2022/06/Newsletter_GPA-may2022-v.3.pdf>.
[41] See, GPA, Newsletter, Issue 2, September, 2022, p. 7-8, <https://globalprivacyassembly.org/wp-content/uploads/2022/09/>.

above-mentioned platforms and actively participates in the working meetings held periodically. In addition, it is worth noting that in 2022, the Personal Data Protection Service of Georgia was also represented at the Global Security Forum ("GLOBSEC"). The President of Service participated in the 17th forum, held in Bratislava, where the main topic for discussion was the ways to strengthen the security and stability of countries around the world, the effective steps to be taken in support of Ukraine and the reinforcement of European neighbourhood.

One of the priorities of the Service in 2022 was the expansion of international cooperation and its prime example is the fact that for the first time in the history of the Georgian Data Protection Supervisory Authority, the Service was granted the status of observer at the "International Conference of Information Commissioners". The conference is a global forum that unites the agencies sharing the common status as conference members, which implement the control over the freedom and the access to public information, and the allied agencies concerned with the field are granted the status of conference observer. Based on the assessment of the main direction of the Personal Data Protection Service of Georgia, its vision and mission in the field of data protection and the international activities, the Executive Board of the Conference successfully completed the process of granting the status of observer to the Service in December 2022. Accordingly, from 2023, the Service will actively participate in the activities of the Conference, attend the open and closed sessions of the annual meetings, and participate in researches and meetings held under the auspices of the Conference. It should be noted that up to 25 supervisory authorities in Europe have acquired the Conference status, including: the data protection supervisory authorities of Belgium, Croatia, Germany, the UK, Ireland, Spain, Catalonia and Switzerland.

The year 2022 is also worth noting in terms of the developing the international relations of the Service, as the Service joined the "Committee on Artificial Intelligence" ("CAI") and was actively engaged with the plenary debates of the Committee through the representative. One of the salient issues within the activities of the Committee is processing of personal data by means of artificial intelligence, on which the Service will offer the expert opinion and relevant recommendations.

4.1.2. MUTUAL COOPERATION WITH FOREIGN DATA PROTECTION COUNTERPART BODIES

In order to implement the best practices of data protection legislation, the cooperation with foreign data protection supervisory authorities represents the salient component of the strategic development of the Service. From this point of view, it is worth mentioning that in April 2022, within the framework of Technical Assistance and Information Exchange instrument of the European Commission (TAIEX), the staff of the Personal Data Protection Service of Georgia underwent a three-day training on the inspection methodology. The training was conducted by experts invited from the Saxon Data Protection, as well as the German Federal Data Protection and Freedom of Information Commissioner's Offices. Within the three-day online training session, the detailed discussions were held on various aspects of the inspection methodology: the scope of inspection, objectives and phases; factors to consider when drawing up the annual inspection plan; as well as the internal organizational procedures and documents of the German supervisory authorities, the types and tools of inspection; also, the rights and obligations of the data controller and the preparation of the final inspection report. The training was conducted in the online meeting format, with up to 25 staff members participating interactively.

During the reporting period, the Service enhanced its cooperation with the personal data protection authorities of Croatia and Italy. In May 2022, in Croatia, the President of Personal Data Protection Service of Georgia and the Director of the Croatian Data Protection Agency ("Agencija zaštuje prósnej datoka") signed the memorandum of cooperation between the agencies, in parallel to the European Data Protection Conference held in Dubrovnik. The Memorandum intends to jointly hold the various events and activities in the field of personal data protection, including the organization of seminars and conferences. It is important to share the experience of the Data Protection Supervisory Authority of Croatia, as the latest country to obtain European Union Member State status, so as to harmonize national legislation on personal data protection with European standards.

The memorandum of cooperation between the Italian Supervisory Authority for personal data protection ("Guarantee of Personal Data Protection") and the Personal Data Protection Service of Georgia was signed in October 2022 in Rome, Italy. The cooperation aims at organizing conferences and seminars targeted at exchanging the best practices in the field of personal data protection, including the exchange of experts. The ceremony of signing the Memorandum was followed by the working meeting between the representatives of supervisory authorities for personal data protection of Italy and Georgia, which was focused on the discussions on the further plans for institutional development of agencies and the opportunities for their cooperation.

It should be noted that in parallel to the "European Case Handling Workshop" ("ECHW")[42] the President of Personal Data Protection Service of Georgia held the face-to-face meetings with the Head of the Supervisory Authority for Personal Data Protection of Bosnia and Herzegovina, as well as the first Deputy Head of the Croatian counterpart. At the meetings the discussions were cantered on performing the coordinated work between the personal data protection supervisory bodies. During the reporting period, the Personal Data Protection Service of Georgia established the close cooperation between the data protection supervisory authorities of Gibraltar and Switzerland as host DPAs of the "European Case Handling Workshop" of 2021 and 2023. Within the mentioned cooperation, the experiences were shared on the content and technical organization of the event.

Mutual legal assistance represents one of the salient parts of cooperation with foreign data protection supervisory authorities. The year 2022 was interesting for the Service from this point of view as well. In order to share information, the Director of the Data Protection Supervisory Authority of the Republic of Moldova addressed to the President of Service in writing. As part of mutual assistance, the response letter was sent to the counterpart supervisory authority and the relevant conclusion – recommendations were offered.

[42] The detailed information about the event see in the sub-chapter: „6.3. Ensuring the Discussions Platforms and Sharing the Best Practice".

4.1.3. COOPERATION WITH DIPLOMATIC CORPUS AND INTERNATIONAL ORGANIZATIONS

In 2022, the President of Service held the introductory meeting with the Charge' d'Affaires at the Embassy of the Kingdom of Spain to Georgia, Marcos Granados Gomez. The meeting discussed the functions, activities and future plans as set out in the action strategy of the Personal Data Protection Service of Georgia, including the international relations and cooperation with the European counterpart supervisory authorities.

In addition, during the reporting period, the working meeting was held between the First Deputy President of Personal Data Protection Service of Georgia, other staff of the agency and the representatives of the British Embassy. At the meeting, the British Embassy was provided with the information on the competence of the Personal Data Protection Service of Georgia and the specificities of inspecting the lawfulness of data processing. At the same time, the special attention was focused on the competencies of the Personal Data Protection Service of Georgia and the activities stipulated in the action plan of its strategy within the National Cyber Security Strategy, as well as the necessity of information exchange between the relevant services in case of cyber and information security incidents. The representatives of the British Embassy introduced the Personal Data Protection Service of Georgia to the Torch Program that provides the support to the implementation of strategic action plan and the effective platform for information exchange in case of incidents, as well as the activities required for raising the public awareness.

During the reporting period, the meeting was also held between the First Deputy President of the Personal Data Protection Service of Georgia and Aaron Rupert, the Deputy Chief of the Political and Economic Division of the US Embassy, as well as with attendance of the representative of the Governance Programme from the USAID Office of Democracy, Governance & Social Development Office. The meeting was focused on the

importance of implementation of the mandate of the Service and the main directions of its activities as well as the institutional development strategy and the best practices in personal data protection.

It is worth noting that the Service actively cooperated with the representatives of Georgian embassies in various countries. In October 2022, in parallel to the ceremony dedicated to signing the Memorandum of Cooperation with the Italian Data Protection Supervisory Authority, the Service held the working meeting with the representatives of the Embassy of Georgia in Italy. The meeting was focused on the mandate of the Personal Data Protection Service of Georgia introducing the main areas of its activities and practices.

The Personal Data Protection Service of Georgia actively cooperates with international organizations as well. During the reporting period, the Service became the beneficiary participant of the project: "Regional Projects on Re-engineering of Public Services and E-governance and Digitalisation in the EaP". With the financial support of the German Federal Ministry for Economic Cooperation and Development (BMZ) and the German Society for International Cooperation (GIZ) the project implies the implementation of the following activities:

- Policy and strategic advisory services;
- Organizational advisory services;
- Expert advisory services on re-engineering of administrative processes;
- Strengthening the creative potential of managers and officers responsible for the processes;
- Managing networks and dialogue platforms;
- Promoting lifelong learning and change by networking stakeholders.

In the framework of this project, the first regional working meeting was held in Chisinau, Moldova with the participation of the Personal Data Protection Service of Georgia. More than 30 participants from the beneficiary agencies of Azerbaijan, Moldova, Georgia and Armenia attended the event. The working meeting was held under

the auspices of the e-Government Agency of Moldova and it was co-organized by the "Public Service Agency of Moldova and the German Society for International Cooperation" ("GIZ") Office in Moldova. In the context of public administration reform, the participants of the meeting discussed the main trends and challenges in public administration, as well as the measures to be implemented in the Eastern Partnership countries to support the digitalization of e-government and public services. The meeting also discussed the future plans of the Service and the potential of their implementation with the financial support of the project.

During the reporting period, the Service actively cooperated with the "Regional Institute for Security Studies" ("RISS"), as well as with the "United Nations Office for Project Services" ("UNOPS"), which is the coordinator of the EU project: "Support to Technical Capacity Building for Ensuring Human Security". In addition, the Service participated in meetings organized by the European Union and Council of Europe project: "CyberEast" that was focused on exchanging the information between agencies on cyber incidents and responding to them, on obtaining electronic evidences as well as the measures to be taken for raising the public awareness.

4.1.4. PARTICIPATION IN THE PREPARATION OF PERIODIC REPORTS TO BE SUBMITTED ON BEHALF OF GEORGIA

The Service was engaged with the preparation of various periodic reports to be submitted on behalf of Georgia. In July 2022, the Georgian delegation presented the 5th periodic report of Georgia on the implementation of the International Covenant on "Civil and Political Rights" to the UN Human Rights Committee in Geneva. The Georgian side provided the UN Human Rights Committee with the comprehensive information on the legislative and institutional reforms undertaken by the State to effectively ensure human rights in Georgia and proper implementation of international obligations since 2014, after hearing the previous periodic report. At the meeting, the First Deputy President of the Personal Data Protection Service of Georgia spoke about the remits of Personal Data Protection Service of Georgia within the supervision of covert investigative actions.

The 8th meeting of the EU–Georgia Association Sub–Committee on Justice, Freedom and Security was held in Brussels in December 2022, within which the Georgian delegation informed the EU bodies about the reforms implemented in the direction of justice and the rule of law. The Personal Data Protection Service of Georgia participated in the Sub–Committee meeting along with other agencies as well. Within the framework of the meeting, the representatives of the European Union were informed about the reforms carried out in the area of justice and the rule of law, including the remits of the Personal Data Protection Service of Georgia, the measures taken for the purpose of its institutional strengthening and the draft law of Georgia on Personal Data Protection.

It is also worth mentioning, that in accordance with the recommendation provided in the EU 5th report on visa–free regime suspension mechanisms in relation to Georgia, the Service presented the information on the activities carried out by the Personal Data Protection Service of Georgia during the reference period to the Ministry of Foreign Affairs of Georgia, which together with other issues concerned the institutional strengthening of the Personal Data Protection Service of Georgia. The information provided also referred to the measures taken for its institutional strengthening, as a data protection supervisory authority.

4.2. ANALYTICAL FUNCTION

4.2.1. STUDY OF FIELD-RELATED TRENDS AND RESEARCH ACTIVITIES

The salient directions of activities for the Service represent the elaboration of thematic guidelines on the issues falling within its competence, the preparation of researches, including the study of international and European standards of personal data protection as well as the best practices of other states. The studies conducted aims at the comparative legal analysis of the relevant issues identified during the examination (inspection) and their implementation in the activities of Service. The research process involves the study and analysis of guidance documents of foreign supervisory counterpart authorities and their decisions as well as the practice of international courts and various international acts or academic papers.

In 2022 the Service prepared up to 30 internal research documents on the topical issues, such as: the depersonalization and pseudonymisation of personal data; the data subject's rights and the extent of their limitation; the protection of personal data of minors; the issues about personal data protection regarding legal entities; processing of personal data on criminal records, etc.

It should be noted that on the occasion of International Children's Day, the Service published the Guide for Protecting Children's Personal Data in the Digital Environment . The document was developed on the basis of the analysis of the Law of Georgia on Personal Data Protection, the international standards of data protection and the best practices. It explains the features related to the concept of the best interests of children, the principles of processing their data, the fundamentals and rights of the child as a data subject. The guide explains the above issues in the simple language and provides the various examples and practical recommendations.

On a monthly basis, the Service published the information digest "World Practices", which reflected the current news in the field of personal data protection, the major trends, the interesting practices of the world's leading supervisory authorities on personal data protection and their recommendations, the important decisions of the European Court of Human Rights and the Court of Justice of the

European Union. The main intent of developing the briefing paper of "World Practices" was to raise public awareness of the issues on personal data protection in the wake of advancement of modern technology. Upon selecting the novelties, the Service was focused on challenges and topical issues existing in the area of personal data protection. It should be noted that the Service has published a total of 10 'World Practice' briefing papers and will continue this practice next year.

4.2.2. LEGAL EXPERTISE OF DRAFT INTERNATIONAL TREATIES AND AGREEMENTS WITHIN ITS COMPETENCE

The Personal Data Protection Service of Georgia implements the oversight of the lawfulness of data processing in Georgia, among them, in the context of cross-border transfer of personal data. In particular, the Service carries out the examination of the draft international treaties and agreements to be concluded on behalf of Georgia envisaging the possibility of trans-border transfer of personal data. Within the expertise, the Service examines the submitted draft agreement and the legislative and institutional mechanisms existing in the field of personal data protection in the state party to the agreement, as well as it assesses the general risks of the violation of human rights in data processing, based on which the recommendation to amend the draft agreement will be issued, if necessary.

When examining the agreements/treaties, the Service takes into account the list[44] of countries with adequate safeguards for the protection of personal data, in which the transfer of data (if applicable) is considered to be secure. The Service also relies on the recommendations and standards [45] developed by the European Data Protection Board for the international data transfer, which take into account the concept of personal data, the obligations of parties pertaining to the data transfer, the principles of data processing, the protection of data subjects' rights, etc.

In order to maintain the high standard in the process of transferring personal data from Georgia to other countries, in 2022 the Personal Data Protection Service of Georgia conducted the legal expertise of 19 (nineteen) draft international treaties and agreements to be signed on behalf of Georgia, out of which the recommendations were made in 6 (six) cases. With the aim to conduct the examination of the draft international treaties and agreements the Service was appealed by the Ministry of Foreign Affairs of Georgia in 18 (eighteen) cases and by the Ministry of Finance of Georgia — in 1 (one) case.

[44] The Order of the President of Personal Data Protection № 03 of March 2, 2022 on "Approval of the List of Countries with Proper Guarantees of protection of Personal Data Protection".

[45] EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14.03.2022; Also, other documents of advisory nature developed by EDPB, <http://edpb.europa.eu/our-work-tools/general-guidance/guilines-reccommendations-best practices_en?f%5B0%5D=opinions_topics%3A747>.

4.3. PARTICIPATION IN THE DEVELOPMENT OF VARIOUS STRATEGIC DOCUMENTS AND ACTION PLANS AND THEIR IMPLEMENTATION

During the reporting period, in line with the European Commission's twelve-point recommendations to grant Georgia the status of European Union candidate country,[46] the Service elaborated the concept of institutional and functional development reflecting the following priorities for strengthening the legal and institutional arrangements for the protection of personal data: the improvement of national legislation, the provision of compliance with the international standards and the establishment of homogeneous practices; the institutional development of the Service; fostering the culture of personal data protection and raising public awareness. The vision of the strategic development of the institutional enhancement of the Personal Data Protection Service of Georgia was presented by the President of Service to the working group established for further institutional reinforcement of the Personal Data Protection Service of Georgia. Consequently, the presented concept of institutional reinforcement of the Service was reflected in the package of legislative changes prepared within the remits of working group, which entered into force on 30 November, 2022.

In addition, during the reporting period the Service was actively involved in the process of developing and implementing various sectoral policy documents within its remit. It is worth noting that in 2022, according to a number of sectoral policy documents of public authorities, the Service was defined as the responsible or partner agency for various activities. Accordingly, in the process of determining the activities for 2023, the Service took into consideration the interest evinced in implementing the said sectoral policy documents and the related action plans.

[46] European Commission, Commission Opinion on Georgia's Application for Membership of the European Union, Communication from the Commission to the European Parliament, the European Council and the Council, Brussels, 17.6.2022.

FULFILLING COMMITMENTS UNDER THE EU–GEORGIA ASSOCIATION AGENDA AND ACTION PLAN

In order to ensure the EU–Georgia association and integration and the high level of personal data protection, in addition, to reinforce the capability of supervisory authorities for data protection, the Service developed the plan of 2022 for the integration of Georgia with the European Union. In order to implement the mentioned plan, the Service performed a number of activities, on the one hand, with the aim of internal institutional enhancement, and on the other hand, a number of series of campaigns were run to raise the public awareness and the informative public lectures were conducted for target groups.

The Service also developed the EU–Georgia integration action plan for 2023 reflecting the priorities determined by Georgia in the European Union–Georgia Association Agenda 2021–2027 within the competence of the Service. In response to the short– and medium–term priorities in the field of personal data protection, 17 activities have been planned for the year 2023 and their outcomes and indicators have been defined. In particular, the activities planned are as follows: strengthening the stability, independence and efficiency of the Personal Data Protection Service of Georgia and ensuring the effective levers for it; raising the public awareness about the activities of the Personal Data Protection Service of Georgia; enhancing the cooperation and coordination with the public and private sector and law enforcement bodies, holding the consultations, informational meetings and trainings; providing the employees with trainings and professional advancements with the aim to increase the effectiveness of the Service; supporting the introduction of internationally recognized standards in the national legislation, etc.

NATIONAL STRATEGY OF GEORGIA FOR HUMAN RIGHTS PROTECTION 2022–2030 [47]

The important part of the strategy is the right to privacy and the protection of personal data. In order to facilitate the effective protection of the right to privacy and its exercise, the strategy

[47] National Strategy for Human Rights Protection of Georgia for 2022-2030, 07-2/181, 05.09.2022.

sets a number of objectives focused on establishing the high standards of personal data protection: the timely and effective responses to the facts of violations of the right to privacy, disclosures of personal information and breaches of personal data; bringing the legislation closer to European standards; raising the public awareness and the professional development of employees of relevant public entities in terms of the right to privacy and the standards of personal data protection.

The Service was actively involved in defining the objectives in line with the strategy, for the implementation of which a number of activities were carried out during the reporting period. Four–, six– and nine–month statistics[48] were published periodically to keep the public informed. In order to introduce the internationally accepted standards and share the best practices in the field of personal data protection, the international cooperation with foreign supervisory counterparts was enhanced through signing the memoranda of cooperation, conducting the trainings within the EU Technical Assistance and Information Exchange Instrument (TAIEX) and participating in various discussion platforms; with the aim to raise public awareness, a number of information meetings and trainings focused on the professional advancement of different groups were held under the auspices of the Service, etc.

STATE YOUTH STRATEGY FOR 2023–2026 AND ITS ACTION PLAN 2023 [49]

In 2022, the Service participated in the development of the State Youth Strategy and its Action Plan 2023 in coordination with the LEPL — Youth Agency. As a result, one of the objectives of the Youth Strategy is focused on the protection of young people's personal data, raise public awareness and in the context of social media on dealing with the topical challenges such as "cyberbullying", "online stalking" and "identity theft". In line with the above mentioned objectives, the action plan provides for the various activities to be carried out by the Service: organizing information meetings on the topics of personal data protection and conducting the course of lectures related to personal

[48] The statistics of four-, six- and nine-month activities of the Service is accessible on the official webpage: www.personaldata.ge.
[49] "On the Approval of the State Youth Strategy 2023-2026 and Its 2023 Action Plan", Resolution of the Government of Georgia No. 606 of December 29, 2022.

data processing for target groups, as well as the publication of the Guide for Protecting Children's Personal Data in the Digital Environment.

In 2022, the protection of children's personal data was one of the prioritized issues for the Service. According to the plan of regular inspections of the legitimacy of personal data processing for the year 2022, minors were included in the target groups for inspection, and the electronic communications and modern technologies were also determined as prioritized spheres. In order to share the international best practices of protecting the personal data of children and to establish effective standards, during the reporting period a number of public lectures or information campaigns were organized by the Service, as well as the Guide for Protecting Children's Personal Data in the Digital Environment was developed.

NATIONAL CYBER SECURITY STRATEGY ACTION PLAN OF GEORGIA FOR 2021–2024 [50]

In the reporting period, the Service, as a partner agency, actively participated in the implementation of a number of activities envisaged by the National Cyber Security Strategy for 2021–2024. In order to develop the cyber culture, the Service was also engaged with the process of developing the awareness–raising strategy. In accordance with the objectives set out in the strategy, in 2022 the Service participated in various events and workshops planned in the framework of the European Union and Council of Europe project: CyberEast. In addition, the representatives of the Service participated in the meeting organized by the LEPL –Digital Governance Agency, which fostered the development of mechanisms for reporting and responding to cyber incidents and cyber threats between CERT/CSIRT, the Ministry of Internal Affairs of Georgia, the critical information system of legal entities, Internet service providers and other responsible authorities as well as creating and developing the common platform for mutual information exchange. Moreover, in 2022 the representatives of the Service participated in the 8th Internet Governance Forum of Georgia, and for the purpose of retraining the Service staff in the direction of informational security the internal

[50] Resolution No. 482 of the Government of Georgia dated September 30, 2021 "On the Approval of the 2021-2024 National Cyber Security Strategy of Georgia and Its Action Plan".

expert of the Service conducted a 3-hour training on the importance of information security and its protection.

ACTION PLAN 2022-2023 ON IMPLEMENTATION OF INTERNATIONAL HUMANITARIAN LAW [51]

The Service is represented in the Interagency Commission on International Humanitarian Law, which is the permanent advisory body of the Government of Georgia. On 19 July 2022, the commission approved 2022-2023 Action Plan for Implementation of International Humanitarian Law, in the elaboration of which the Service participated along with other agencies. One of the objectives of the approved action plan is to examine and improve the existing political and legislative basis for the purpose of considering the principles of international humanitarian law. In order to achieve the set goal, with the active involvement of the Service there was determined the activity, which, in accordance with the voluntary obligation undertaken by Georgia at the 33rd International Conference of the Red Cross and Red Crescent, envisages the enhancement of implementation of legislation on personal data

The harmonization of national legislation on personal data protection with the internationally recognized standards is the indispensable priority for the Service. Accordingly, at the meeting held on 9 December 2022, the Human Rights and Civil Integration Committee of the Parliament of Georgia discussed the Draft Law on "Personal Data Protection" at the first reading with the active participation of the Service.

THE SECOND E-GOVERNANCE STRATEGY AND RELEVANT ACTION PLAN (2023-2024)

In coordination with LEPL – Digital Governance Agency, the Service participated in the development of the second e-governance strategy and the relevant action plan. To this end, during the reporting period the Service, within its competence, determined a number of activities planned within the framework of digital governance for 2023-2024 in terms of improving the communication system

[51] Approved on July 19, 2022 by Inter-agency Commission on International Humanitarian Law https://justice.gov.ge/?m=articles&id=dbzmJic05Y [11.02.2023].

at the intra-service level, saving human resources and launching an effective monitoring system.

PARTICIPATION OF SERVICE IN THE DEVELOPMENT OF UPDATED NATIONAL ANTI-CORRUPTION STRATEGY AND ACTION PLAN OF GEORGIA

In accordance with the Ordinance of Government of Georgia №390 of December 30, 2013 on the "Approval of Composition and Statute of Inter-Agency Coordination Council for Combating Corruption" the President of Personal Data Protection Service of Georgia is a member of Anti-Corruption Council. During the reporting period, the service actively participated in the activities of working group set up within the Anti-Corruption Council. Accordingly, during the reporting period, the Service, within its remits, provided the Anti-Corruption Council with the priority topics and situational analysis relating to the issues to be included in the updated national anti-corruption strategy and action plan of Georgia.

2022 ACTION PLAN OF THE SERVICE "ON THE RIGHTS OF PERSONS WITH DISABILITIES AND ITS IMPLEMENTATION"

During the reporting period, the Service developed the "Action Plan on the Rights of Persons with Disabilities 2022"[52]. The goal of 2022 Action Plan was determined to be the promotion of rights and freedoms of disabled people. It encompassed the objectives, such as: raising the awareness about personal data protection of persons with disabilities and considering their needs in the national legislation and relevant legal acts of the President of Personal Data Protection Service of Georgia.

In order to achieve the above-mentioned objectives, the following activities were carried out:

a) The scientific article covering the topics about personal data protection of persons with

[52] Approved by the Order of the President of the Personal Data Protection Service of Georgia, No. 01/86 of July 7, 2022.

disabilities was published in the first issue of the bilingual scientific publication "Legal Journal on Personal Data Protection" founded by the Personal Data Protection Service of Georgia. The article deals with the special categories of data of disabled persons, in particular, the lawfulness of processing the information on their health condition.

b) Within the planned inspection, the Service examined the lawfulness of processing the personal data of adults declared as persons with legal incapacity/limited legal capacity through electronic database of LEPL – Chamber of Notaries of Georgia. In order to address the shortcomings identified during the data processing, the data controller was given 5 mandatory instructions to perform. The Service also examined the lawfulness of processing the minors' data through the creation, storage and transfer of the individualized education program to the third parties by LEPL – Tbilisi Public School No. 198, within which there were carried out the inspection of data processing of students with special educational needs conducted by the school. With the aim to remedy the shortcomings detected by the examination, 2 mandatory instructions were issued to the data controller to perform. In order to introduce the relevant standards by educational institutions, the said decision was published on the website of Service.

c) In order to facilitate the referral to the Service made by persons with disabilities, the Rule on Proceedings of Personal Data Protection Service of Georgia[53] envisaged the assistance to be rendered by the Service employee in drafting paper documents by a natural person. In particular, in the event of the request for assistance, the Service employee concerned is obliged to assist him/her and, in accordance with the person's needs, prepare the paper document under his dictation. In such a case, the note is made in the paper document stating that the Service employee has drawn up the document on behalf of the natural person, which is signed and/or otherwise agreed on by the natural person. The rule ensures the existence of necessary safeguards for the needs of persons with disabilities and for their recourse to service.

[53] Order N 01/170 of the President of the Personal Data Protection Service of Georgia, as of September 15, 2022.

5. RAISING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES

Raising public awareness represents one of the main functions and, at the same time, the challenge for the Personal Data Protection Service of Georgia. Accordingly, the introduction of the culture of personal data protection in the society and raising public awareness of the oversight body of personal data protection is one of the salient objectives of the Service. As the activities of Service are based on the principles of accountability, transparency and openness to public, the Service periodically actively provides the public with information about the state of data protection in Georgia and the related important developments. It should be noted that in order to form the independent, impartial and human rights-oriented supervisory body, as well as to raise public awareness of the Service and gain public confidence, the Service carried out a number of important activities during the reporting period.

5.1. NEW LOGO AND BRAND BOOK OF THE SERVICE

As of 1 March 2022, the Personal Data Protection Service of Georgia, having become an independent supervisory authority, launched the rebranding process. There was created the logo of the agency and the associated branding materials.

THE LOGO OF THE SERVICE AND ITS DESCRIPTION

პერსონალურ მონაცემთა დაცვის სამსახური
PERSONAL DATA PROTECTION SERVICE

At the top of the rhombus-shaped space, a digital data icon is shown in dark turquoise, while the circles characteristic of fingerprints and network connections are integrated into the lower part of the logo in light emerald. On the right side of the logo there is the Georgian and English versions of the full name of Service – "Personal Data Protection Service of Georgia ". Overall, the symbol depicts the necessity of link between identity, information security and modern technology, which are harmoniously integrated in the Personal Data Protection Service of Georgia.

In parallel with the rebranding process, the branded materials of the Service were created, including: signboards, banners, printed materials and others. It should be noted that the signboard in front of the headquarter of the Service (Add.: Tbilisi, N. Vachnadze Street, N7) contains the name of the Service in three languages – Georgian, English and Abkhazian. In this way, the Service respects Abkhazian as a language whose status is protected by the Constitution.

5.2. ACTIVITIES FOCUSED ON RAISING AWARENESS

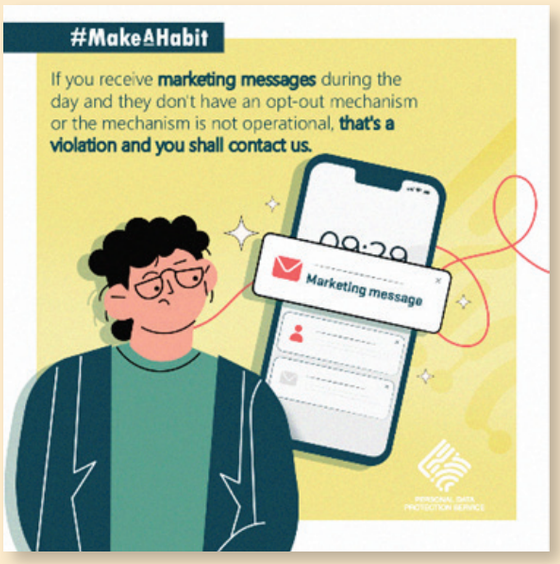
Since its inception, the Service has been intensively implementing a variety of activities, including online campaigns for the purpose of raising public awareness. It should be noted that, the information about the Service as a whole, its mandate and mission was posted online through special thematic cards. Citizens were provided with the information about the occasions and communication channels through which they could contact the Personal Data Protection Service of Georgia. In addition, there were published the posters titled: "Dictionary on Personal Data Protection", explaining to the public the basic terms from the law on personal data protection.

CAMPAIGN: "MAKE A HABIT PERSONAL DATA PROTECTION"

In the second half of the year 2022, the campaign "Make a Habit Personal Data Protection" was implemented, which pursued the preventive policy and presented the key advice in a simple and straightforward as well as visually-explicit way to be considered by citizens and organizations. The illustrated cards with the important tips written on them highlighted the importance for citizens to think about and ask themselves why they are being asked for certain information and whether it meets the requirements of the mentioned law.


#MakeAHabit
After using electronic devices, or when leaving them temporarily unattended, be sure to log out of personal systems or lock them.
Log out
PERSONAL DATA PROTECTION SERVICE


#MakeAHabit
Document
Remember accepting the requirements of a privacy policy or signing documents without reading them involves certain risks.


#MakeAHabit
If you receive marketing messages during the day and they don't have an opt-out mechanism or the mechanism is not operational, that's a violation and you shall contact us.
Marketing message


#MakeAHabit
Obtain permission before sharing the personal information of others or posting it on a social network.


#MakeAHabit
When entering passwords online or on devices/systems, ensure that it is not visible to others.
Enter the password
Sign in


#MakeAHabit
Do not open suspicious links from unknown and untrusted senders.
DANGER
You are clicking on a suspicious link.


#MakeAHabit
Before giving out personal information, always ask:
Who do you share data with?
Why are you being asked for this data?
For what purpose will this data be used?
How long will this data be stored?


#MakeAHabit
When talking about the details of someone's personal life in public, remember that it is easier to identify a person than we think.


#MakeAHabit
Never! nobody! Do not transfer or share information obtained in the course of professional activities about users' personal information for non-professional purposes.


#MakeAHabit
Do not leave documents containing the customer's personal information in a place accessible to others.


#MakeAHabit
Do not publish user's photo/video material without consent.
Photo/Video
send


#MakeAHabit
Do not request from the user more information than it is necessary for the intended purpose.

BLOG CONTEST: "MY PERSONAL DATA AND EYES WIDE OPEN"

At the end of 2022, a blog contest named "Me My Personal Data and Eyes Wide Open" was held for school students. About 60 students of IX–XII classes from different regions of Georgia, including Kvemo Kartli, Shida Kartli, Adjara, Imereti, Samegrelo, Guria, and Kakheti, participated in the competition. The competition aimed to raise awareness among schoolchildren about the importance of personal data protection. The best authors participating in the competition were selected by the representatives of the Service together with the specially invited jury – writer Davit Gorgiladze. The winning students: Giorgi Ivanidze, a student of Public School No. 199 of Vladimir Komarov Tbilisi Physics and Mathematics School; Mishiko Beradze, a student of Khidri Village Public School of Kharagauli municipality; and Ana Giglemian, a student of Samebi Village of Tsalki Municipality, were hosted by the President of the Service and were presented with certificates, and prizes —— tablets and branded items.

ENGAGEMENT WITH THE MEDIA

During the reporting period, the Service engaged in extensive collaboration with various media outlets, encompassing television, radio, and online platforms. The representatives of the Service actively participated in diverse programs and conducted numerous interviews that were subsequently published. Information about the meetings (including regional ones) and events held by the Service or important, visits abroad were sent to the media. It should be noted that the total of 43 press releases were disseminated to the media over the reporting period.

It should be noted that representatives of all media outlets were invited to all the important events organized by the Service, including:




- The 6-month summary event where the report was presented to members of parliament, representatives from non-governmental organizations, diplomatic personnel, and the academic sector.

- "European Case Handling Workshop" (ECHW) which was held on 17-19 November, 2022 organized by the Personal Data Protection Service in Tbilisi.

- Conference — "Personal Data Protection in Digital Environment" which was held in December, 2022 by the Service.

- Ceremony for awarding the winners of the blog contest. In addition, during the reporting period there occurred the proactive publication of cases of high public interest as well as of the activities and original or precedent-setting decisions taken by the Service.

SOCIAL MEDIA

Having regard to the modern reality, the social network is one of the best way to communicate to the public. The mentioned platforms make it possible to provide information to different segments of society – people of different ages, interests or professions. Accordingly, apart from the traditional media resources, the Personal Data Protection Service of Georgia actively utilizes various social platforms to communicate with citizens, including: Facebook, LinkedIn, Twitter, YouTube.

During the reporting period, together with the materials reflecting meetings the Service periodically published the quarterly reports and documents containing the statistical data on the activities of the Service on the official website and platforms of social media. The published materials included the information on the number of referrals to the Service, consultations, inspections carried out and other important activities. There were also published the information banners, tests, recommendations, information on job vacancies and the major trends in the legal area of personal data protection. The information about the best employee of the month was also publicized each month. The Service responded to important dates with thematically and, if necessary, contextually

loaded posts via social media, including:

- World Health Day
- International Down Syndrome Day
- Independence Day of Georgia
- Mother Language Day;
- International Children's Day
- School Starting Day;
- International Human Rights Day and etc.

In the reporting period, the total of 503,509 users accessed the posts shared on Facebook, the number of visitors to the page amounted to 72,751 and 1,239,502 users responded to the content posted on the page. As regards the website, the number of its visitors during the reporting period equalled to 89,786.

5.3. TRAININGS AND PUBLIC LECTURES

Since the first day of its establishment, the Personal Data Protection Service of Georgia has been actively holding educational events, as a result of which the representatives of public and private sectors — local authorities, schools, universities — and students were offered the opportunity to enhance their knowledge on the subject of personal data protection. The Service paid particular attention to awareness-raising campaigns among academic, administrative staff and students of educational institutions. It should be noted that during the reporting period, 11 events were held for students, teachers and administrative staff of various private and public schools, as well as for students, academic and administrative staff of various higher education institutions. The meetings were held in a lecture and discussion format, within which the total of 253 people gained the information on personal data protection. In parallel to the informative lectures, the special module was created due to the high interest evinced by students.

It is worth noting that with the support of the Faculty of Law at Ivane Javakhishvili Tbilisi State University the Service organized the thematic lectures to be conducted for the persons concerned almost every month during the reporting period. The topics to be discussed in the format of public lectures were as follows: the legislation on personal data protection; the Personal Data Protection Service of Georgia and its mandate; the citizen's rights; video surveillance; direct marketing; personal data processing in employment relations; the legal regulation and practical aspects of international data transfer, etc. In the framework of informative public lectures encompassed five events which were attended by 177 people.

During the reporting period, on the initiation of the training centre of the Chamber of Notaries the Service retrained 270 notaries within 6 training sessions. It should be noted that the topics of the trainings were elaborated and tailored to the needs and wishes of notaries encompassing both theoretical and practical topics, as well as exercises and the discussion part.


Apart from the above mentioned, the Service conducted the interactive training for the staff of the National Statistics Office of Georgia, which was related to the basic issues of personal data protection, including the basics of data processing, data minimization, the purpose and storage limitation. Also, taking into account that the National Statistics Office of Georgia, in its part, is a data controller, the special attention was focused on the security measures for the personal data stored in the institution.

During the reporting period, the representatives of Service provided a series of trainings for the Investigation Police and General Inspection of the Ministry of Defence, as well as for the staff of Special State Protection Service on personal data protection and covert investigative actions.


It should also be noted that the First Deputy President of Personal Data Protection Service in collaboration with the Institute for Development of Freedom of Information (IDFI) held training sessions with the students participating in winter school, during which they were informed about the mandate of the Service and the significance of personal data protection.

5.4. PUBLIC MEETINGS AND CONFERENCES

It should be noted that the representatives of the Service intensely held the meetings with the representatives of various fields and professional groups to discuss the future cooperation and field-related challenges and various thematic issues. Meetings were held with the representatives of the private and public sector, law enforcement bodies, as well as with the non-governmental sector and international organizations.

During the reporting period, the President and the First Deputy President of the Service held a number of introductory or working meetings with the representatives of legislative, executive and judicial branches, as well as the public, private, non-governmental and academic sectors. In addition, it should be noted that the President of Personal Data Protection Service of Georgia and the First Deputy President were actively involved in the working group of the European Commission's Twelve Priorities of the Legal Affairs Committee of the Parliament of Georgia on the issues pertaining to institutional strengthening of the Personal Data Protection Service of Georgia.

During the reporting period, the staff of the Service actively participated in the various inter-agency meetings and events held in different directions, including the discussions on national and other different types of action plans.

The implementation of various activities for the purpose of raising public awareness were prioritized not only in Tbilisi but in the regions as well. For this reason, during 2022, the President of Personal Data Protection Service of Georgia, the First Deputy President, and the heads of the professional departments held a number of meetings in eight regions of Georgia, within which they conducted the informative lectures to the employees of municipalities. The cycle of regional meetings was launched in Adjara and ended in Telavi. The meetings were attended by 182 employees of the municipalities. The Personal Data Protection Service of Georgia will actively continue the close and coordinated cooperation with the municipalities and will run the informative campaigns for the regions in the future as well.

In the course of the reporting period, the managers and staff of the Service participated in a number of local and international conferences as participants as well as speakers. Among them, the conference dedicated to the International Human Rights Day should be specially pointed out, which was organized by the European Union (EU), the United Nations Development Programme (UNDP) and the Office of the United Nations High Commissioner for Human Rights (OHCHR). Within the event, the First Deputy President shared the information about the mandate and functions of the Service.





The Service was also represented at the 8th Internet Governance Forum of Georgia, within which the personnel of the Service made speeches about the importance of personal data protection of children and international legal instruments regulating the issue; the participants of the event were also introduced to the best practices of foreign counterpart oversight bodies of data protection and the internationally recognized standards, so as to create the proper safeguards for the protection of personal data of children in digital environment. During the reporting period, the representatives of the Service actively participated in various conferences and workshops on the issues about cyber security.

6. DEVELOPMENT OF THE PERSONAL DATA PROTECTION LAW AND THE ROLE OF THE SERVICE

6.1. RECENT AMENDMENTS TO THE LAW OF GEORGIA "ON PERSONAL DATA PROTECTION"

In order to accomplished the prioritized objectives defined by the European Commission Opinion of 17 June 2022 and to prepare the relevant legislative changes to be implemented for granting Georgia the EU candidate status, the package of legislative acts has been prepared within the activities of working group established by the Legal Affairs Committee of the Parliament of Georgia, with the active participation of the Service.[54] It aimed at the institutional strengthening of the Personal Data Protection Service. It is worth mentioning that the amendments of 30 November 2022 made to the Law of Georgia on Personal Data Protection fostered the institutional enhancement of the Service, the effective performance of its functions and the social protection of persons employed in the Service.

According to the above-mentioned modification of the legislation, the President of the Service was granted the power to determine the working procedures for the employees of the Personal Data Protection Service of Georgia. At the same time, the issues related to the social protection of employees were defined, in particular: state insurance, the guarantees of social protection in case of bodily injury or death during the performance of professional duties. The legislative amendment was made to the Code of Administrative Offences of Georgia, and the term of imposing administrative liability was increased up to 3 months. The above-mentioned is extremely important for the Service to effectively ensure the control over the lawfulness of personal data processing and to provide the appropriate response. Occasioned by a rather complex procedure for controlling the lawfulness of data processing and, in frequent cases, the delayed appeals of data subjects, the two-month deadline for imposing administrative penalties set by the Administrative Offence Code of Georgia significantly interfered the core function of the Service to supervise data protection. As a result of legislative changes, within the framework of implementing the supervision over the data protection in

[54] The Law of Georgia № 2199 of November 30, 2022, Legislative Herald.

the country, the Service will no longer be limited to the 2–month limitation period, which, according to current experience, did not suffice in many cases. Within the framework of the legislative package, the amendment was made to the Rules of Procedure of the Parliament of Georgia, based on which it was defined that upon the request, the President of Personal Data Protection Service is allowed to provide the Committee with the information on legislative shortcomings identified in the process of its activities and to share the opinions on their elimination as well as on the measures to be taken for increasing the efficiency of the Service.

6.2. RENEWAL OF THE REVIEW OF THE DRAFT LAW OF GEORGIA "ON PERSONAL DATA PROTECTION"

In the reporting period, Human Rights and Civil Integration Committee of Georgian Parliament discussed the general principles and basic provisions of the draft Law of Georgia "On Personal Data Protection" within the first hearing [55]. The Personal Data Protection Service was also actively involved in the discussions on the draft law as well.

It is worth pointing out that having been developed as a response to bringing the legislation in force on personal data protection closer to the European standards, to fulfilling the international obligations and establishing the internationally acknowledged principles by Georgia as well as to respond the challenges existing in public and private entities and law enforcement bodies, the draft Law of Georgia "On Personal Data Protection" redefines the legal guarantees and rules of personal data protection in a new way. The draft law increases the safeguards to protect the rights and interests of the data subject and establishes their rights as well as the relevant duties of a data controller pursuant to the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR). In particular, the draft law defines the right to data portability; the right to reject such decision–making that constitutes the legal consequences for the data subject only in the automated form (e.g. using artificial intelligence) and as a result of profiling; in addition, as regards the right to familiarize oneself with the data presented and obtain its copy as well as the right to block the data will be enshrined as a separate Article.

The draft law also envisages the grounds and scopes of restrictions on the data subject's rights. In particular, the right to be informed about data processing, the right to be familiarized with and receive a copy of the data, the right to correct, update and complete the data, the right to delete, destroy or terminate data processing and other rights may be restricted, if the said is expressly provided for by the legislation and does not violate the fundamental rights and freedoms as well as represents the necessary and proportionate measure in the democratic society; also, if the exercise of these

[55] The Draft Law of Georgia on Personal Data Protection, № 07-3/353/9, 22/05/2019.

rights may prejudice: the prevention of crime, the investigation of crime, criminal prosecution, the administration of justice, the execution of imprisonment and deprivation of liberty, the enforcement of non–custodial sentence and probation, the operative–investigative activities, as well as if the said rights may pose threat to the interests of national security and/or national defence, the interests of public safety, the protection of state, commercial, professional and other secrets provided for by law, to the exercise of justice and constitutional control by the court, as well as if the mentioned infringes the rights and freedoms of the data subject and/or those of other persons, including the freedom of expression.

The draft Law specifies the terms "controller" and "processor" in the following way: "person responsible for processing" and "person authorized to process". The statute also spells out the obligation to notify the Personal Data Protection Service of Georgia of an incident. Accordingly, the data processor is obliged to record the incident, the outcomes produced, the measures taken and, no later than 72 hours following the detection of incident to notify the agency in writing or electronically in accordance with the rule established by the President of Personal Data Protection Service, except for the case when the incident is unlikely to pose any treat to the cause of protecting the fundamental human rights and freedoms.

In addition to the above mentioned, the significant changes affect video surveillance and audio monitoring as well as the rules on data processing for direct marketing purposes. According to the draft law, in order to carry out video surveillance, the data controller is obliged to define in writing the purpose and extent of video surveillance, the duration of video surveillance and the period of storage of recordings, the procedure and conditions of the access to video recordings, their storage and destruction, and mechanisms for protecting the rights of the data subject in compliance with the principles of data processing.

The draft Law provides the legal provisions on audio monitoring and determines the grounds for its implementation. Audio monitoring is defined as processing of data through utilizing the technical means placed/installed in public or private places, particularly, audio monitoring and/or audio recording. The implementation of audio–monitoring is admissible: with the consent of the data

subject; for the purpose of producing the minutes; when rendering the remote services; in order to protect the obviously prevailing legitimate interests of the data processor, in case the appropriate and specific measures are defined to ensure the rights and interests of the data subject; and in other cases expressly provided for by Georgian legislation. The data controller is obliged to notify the data subject prior to or immediately after the commencement of audio–monitoring. According to the draft law, the burden of proof to inform the data subject lies with the data controller/processor.

Data processing for direct marketing purposes is only admitted with the (prior) consent of the data subject (instead of the current rule, according to which the data subject has the right to request termination of processing his/her data after it has been occurred). According to the current legislation, the data obtained from publicly available sources can be processed for direct marketing purposes. And the draft law states that regardless of the basis of data collecting/obtaining and its availability, data processing for direct marketing purposes may only be carried out on the grounds of the consent of data subject.

An important innovation in the draft law is the introduction of the institute of data protection officer. The public entity (other than religious or political organizations), as well as the insurance company, commercial bank, microfinance organization, credit information bureau, electronic communication company, airline, airport or the health care institution rendering services to at least 10,000 data subjects per year as well as the person responsible/authorized to such processing, who processes a large number of data subjects or conducts systematic and extensive monitoring of their behaviour, will be obligated to designate or determine the data protection officer. The function of the Data Protection Officer is to analyze the applications and complaints received regarding the data processing and respond to them within the remits of its authority and other important tasks.

At the same time, the procedure and criteria for obtaining the data subject's consent to personal data processing is specified. It is also established, that, if the data subject expresses his/her consent as part of the written document regulating other matters as well, the request for consent must be presented in the way that is clearly distinguishable from other matters, straightforward and easy to

understand and written in simple and comprehensible language. Any part of the written document that violates this rule is not binding.

The draft law also provides the mechanism for assessing the impact of data protection. In particular, if, given the category, extent, purposes and means of data processing, there is constituted the high probability of the breach of fundamental human rights, the data processor is required to conduct the evaluation of impact of data processing in advance. The aforementioned obligation will apply to the data controller only if she/he takes the decision producing the legal, financial or other significant consequences for the data subject only in the automated form, among them, as a result of profiling and in case of carrying out the systematic and extensive monitoring of data subjects' conduct in public places or processing a large amount of special categories of data.

Administrative fines for breaches of personal data protection legislation have been increased. Also, fines will vary depending on the annual turnover of the data processor (below/above GEL 500 000). In addition, according to the draft law and occasioned by the international standards, in case of committing two or more administrative offences by the offender, the administrative fine will be imposed for each of them separately.

The draft law proposes the mitigating and aggravating circumstances for administrative offences specific to personal data protection. In addition, the following circumstances are also envisaged to aggravate the liability for administrative offences: the repeated commission of the same offence, for which the person has already received the administrative fine within one year; processing special categories of data in breach of the requirements of the legislation; processing large volumes of data in breach of the legislation or creating such threat; processing minors' data in breach of the legislation; committing the administrative offence for the sake of mercenary purposes. The circumstances mitigating the responsibility for committing administrative offences are deemed to be: ending unlawful actions and compensating for the harm caused as a result of the offence and/or taking the appropriate organizational and technical measures to prevent the commission of similar offences in the future; the commission of the offence by a minor; the sincere repentance of the offence and cooperation with the President of the Personal Data Protection Service of Georgia as

well as the other circumstances such as: the nature of the offence committed and the degree of culpability of an offender, which the President of the Personal Data Protection Service of Georgia considers to be mitigating circumstances in resolving the case.

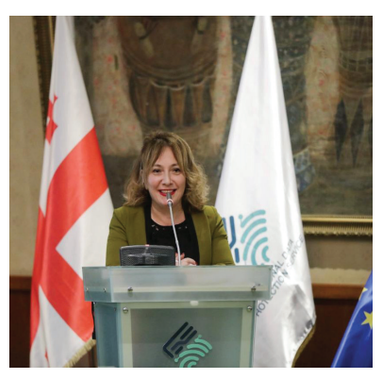
It should be noted that apart from elevating the standard of personal data protection and defining the new provisions in response to the current challenges in the country, the adoption of the draft law will foster the process of integration into the Single Euro Payments Area ("SEPA") to the extent that the adoption of the draft law will bring the national regulation of personal data protection into functional compliance with the EU legal framework. Over the next year, the Personal Data Protection Service will continue its close cooperation with the Parliament of Georgia and will actively participate in the further discussions on the draft law.

6.3. PROVISION OF DISCUSSION PLATFORMS AND SHARING THE BEST PRACTICES

The personal data protection supervisory bodies play the key role in creating the field-related platforms for discussions. The aforementioned greatly contributes to the purpose of effective cooperation between supervisory bodies and the exchange of their experiences. This format of cooperation aims at the comparative legal analysis of the sectoral challenges and the development of the unified approach in response to them.

HOSTING THE "EUROPEAN CASE HANDLING WORKSHOP"

In 2022, the Personal Data Protection Service, as an active partner of the counterpart foreign supervisory authorities in personal data protection, made a significant contribution to supporting the platforms for discussions about the relevant topics of modern legislation on personal data protection. In particular, it should be noted, that for the first time in the history of Data Protection Supervisory Authority of Georgia, the European Case Handling Workshop (ECHW) 2022 was hosted by the Personal Data Protection Service of Georgia. The European Case Handling Workshop is an annual international forum aimed at sharing the best practices in the field of privacy and personal data protection with the participation of data protection supervisory authorities from different countries. The seminar has held since 1999 and originally emanated from the Spring conference in Helsinki, where European supervisory authorities of data protection agreed to hold the seminar with the practitioners engaged in the field of data protection participating in it. The aforesaid was aimed to compare the procedures for reviewing the complaints and facilitate handling the cross-border complaints. The working meeting represents a kind of continuation of the "European Conference of Data Protection Authorities" (the so-called "Spring Conference"), however, in a different format, in



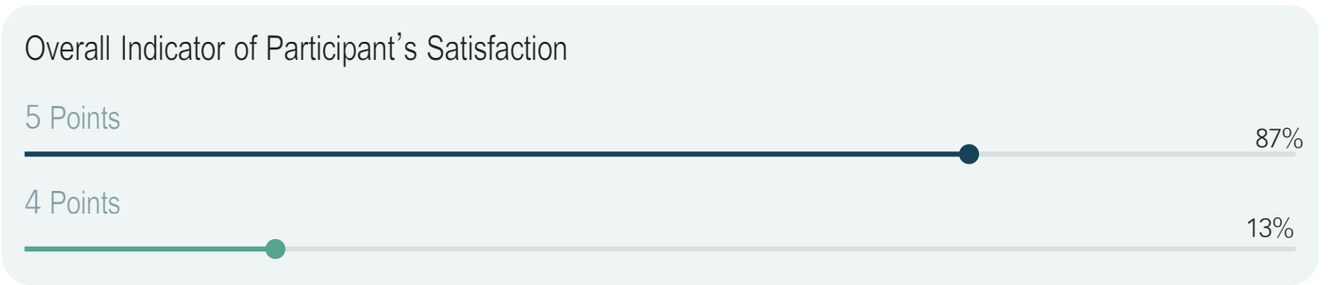
particular, as a working forum. It forms the platform for the purpose of holding discussions about the relevant practical issues as well as conducting the analysis of challenges emerged in the process of case handling by supervisory authorities and the discourse on their solutions. Every year, various issues about the enforcement of legislation on data protection as well as the international standards of case handling for the supervisory authorities of data protection are discussed within the working meeting. Thus, the goal of the workshop is to share experiences with the practitioners working in the field of data protection on topical issues, such as: the complaints received in relation to the protection of data subjects and their identification; the key challenges encountered by the data protection supervisory authorities in the process of their activities; the sectors relating to which the data protection supervisory authorities receive the majority of complaints or the potential complaints to be received in the future.

The President of Personal Data Protection Service of Georgia officially opened and delivered the speech to the participants of the 2022 event. The welcome speech was also given to the participants by the Chairman of the Human Rights and Civil Integration Committee of the Parliament of Georgia, Mikheil Sarjveladze. The workshop covered the topical issues in the field of personal data protection and privacy, such as: the stages of inspection carried out by the personal data protection supervisory authorities; data protection in social media and exceptions in the national legislation; the international data transfer; personal data and artificial intelligence, etc.
In total, the workshop combined 6 panel sessions. At the end of the event, the participants were familiarized with the concept of 2023 workshop by the representative of the next host country, in particular, the Swiss Data Protection Supervisory Authority.

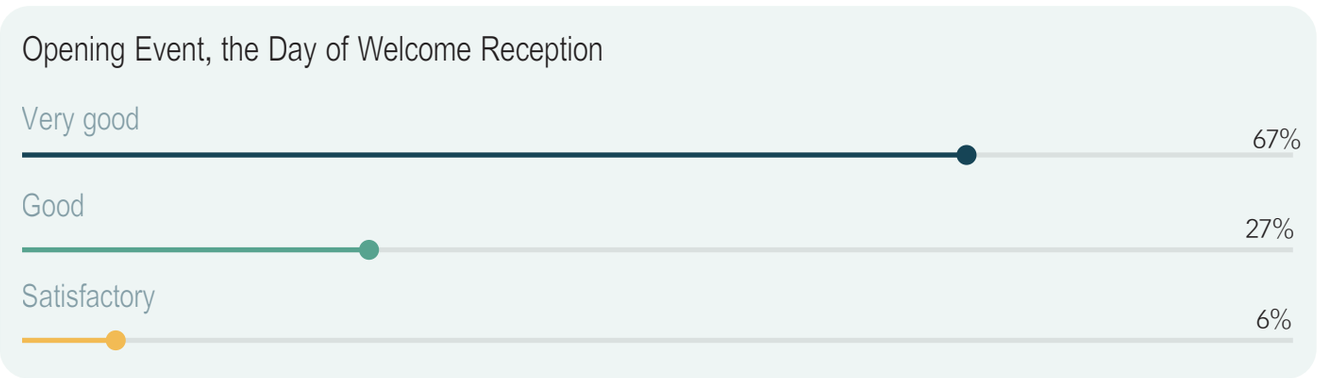
It is worth noting that more than 50 delegates from the counterpart supervisory authorities of data protection from 26 countries participated in the seminar. Twenty-seven speakers from 16 countries shared their experiences with the participants of the event. The representatives of the European Data Protection Supervisor (EDPS) and the International Committee of the Red Cross (ICRC) also addressed the workshop. Apart from the working format, the various social activities were intended to familiarize the participants with Georgian history and culture as well. It should be noted that the President of the International Committee of the Red Cross delegation to Georgia, Anne Montavon, as well as the representative of the European Union delegation to Georgia, Anne Birgitte Hansen,

took part in the event.

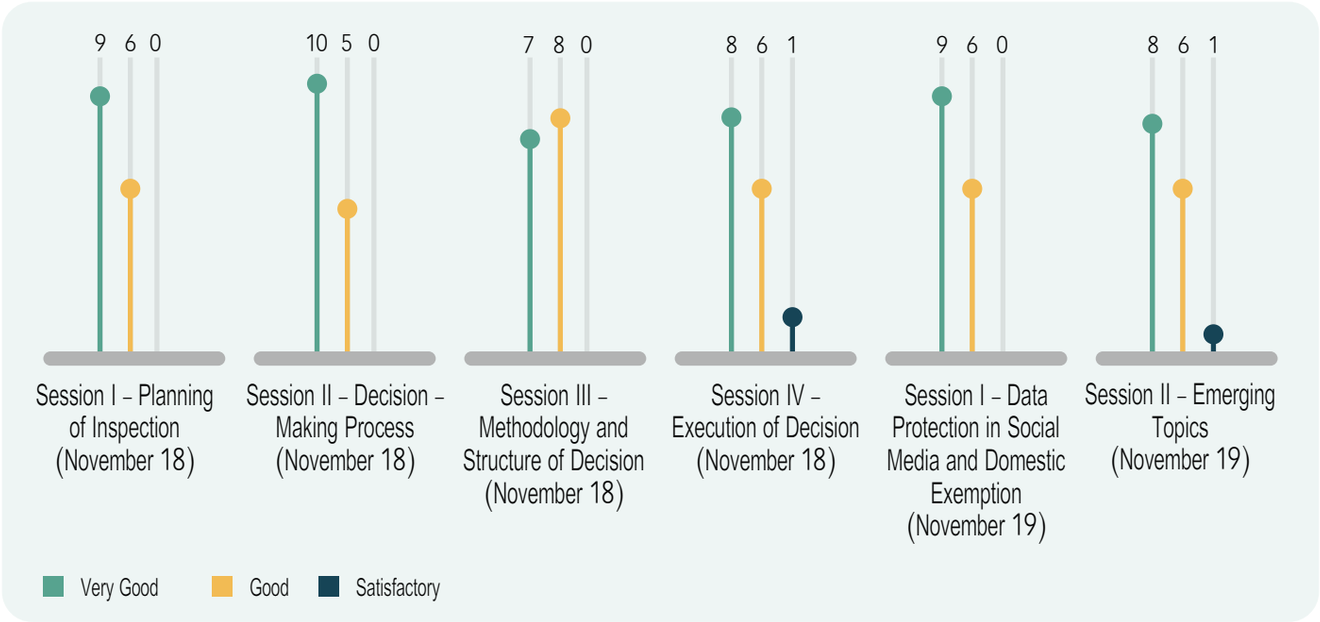
In order to study the participants' satisfaction with the European Case Handling Workshop, the Service developed the questionnaire regarding the speakers and moderators of workshop, the substantive and technical organization of the event as well as the cultural activities. According to the results of the satisfaction survey, the participants highlighted and appreciated the presentations given at the event, but at the same time they wished that they had had more time for the question and answer session and interactive discussion. Based on the survey findings, the estimates of the individual components are as follows:



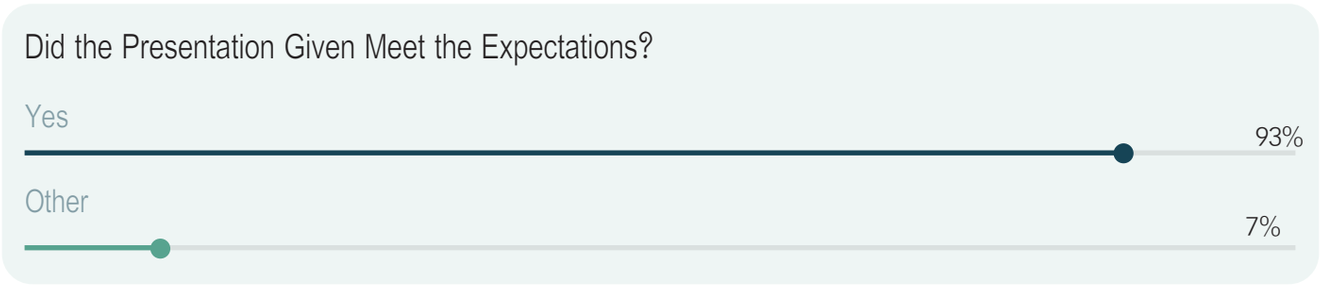
The overall level of satisfaction of the surveyed participants was rated as 4.87, where 5 points corresponded to Very good and 4 points – to a Good.



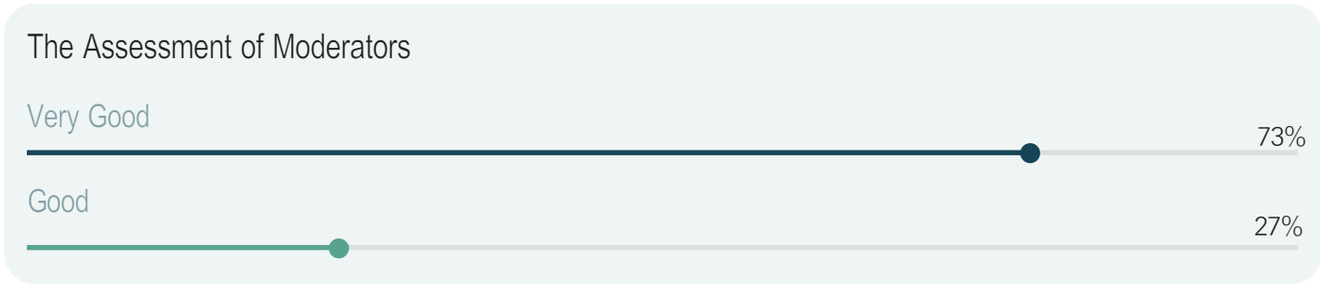
67% of the attendees of the workshop evaluated the Welcome Reception as Very good, and 27 % of them — as Good. The official welcome reception was not assessed negatively by any participants.



The majority of attendees of the workshop were satisfied with the sessions held on 18 and 19 November. Only in two cases, the individual panel sessions were evaluated as satisfactory.



93% of workshop participants said that the quality and content of the presentations met their expectations, and 7% declared that despite the fact that they were satisfied with the quality of the presentations, they deemed it expedient to change the format and add more practical elements to the sessions.



73% of the participants gave the role of moderators the highest rating and 27% gave a positive rating. There was no negative evaluation.

THE ESTABLISHMENT OF "JOURNAL OF PERSONAL DATA PROTECTION LAW"

The bilingual, scientific, full open access periodical publication: "Journal of Personal Data Protection Law" was established by the decision of the President of Personal Data Protection of Georgia, in order to develop the field of law on personal data protection and foster the scientific forum for discussions. Its establishment marks the fourth anniversary of the application of the "General Data Protection Regulation" (GDPR), which entered into force on 25 May 2018. The establishment of Journal of Personal Data Protection Law is also noteworthy in the view that it is the first periodical scientific publication founded in the history of Personal Data Protection Supervisory Authority of Georgia.

The Journal's primary focus is conducting the comparative legal discourse on public law and creating the scholarly forum for researchers. The Journal publishes scientific papers in the field of fundamental human rights and freedoms, especially in the area of personal data protection law and aims to provide the legal analysis of topical issues, to highlight the best practices and raise public awareness. The mission of the Journal is to facilitate the process of harmonization of Georgian Law "On Personal Data Protection" with European legislation and internationally recognized standards, as well as to share the outcomes of the field-related studies with the academic circle, legal practitioners and, in general, individuals concerned with the subject matter of data protection and the right to privacy. To strengthen the internationalization component, each issue of the Journal combines the scholarly papers of Georgian and foreign authors in both Georgian and English languages. The Journal is published in print and electronic form and is publicly accessible.

The Journal is published twice a year in paper and electronic form and is publicly available to

the persons concerned [56]. It should be noted that the first issue of the Journal was dedicated to the International Data Protection Day 2023, which is celebrated every year on 28th of January in accordance with the decision of the Council of Europe of 26 April 2006 and is connected with the date of opening the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data for signature. The academic articles published in the first edition are written by the representatives of academic circle and legal practitioners, namely, the particular salience is attached to the scientific publications written by the authorship of the leading scholars in the field, such as the Professor of Ivane Javakhishvili Tbilisi State University, Prof. Dr. Paata Turava; the Retired Judge at the Federal Social Court of Germany, Professor at Philipps University of Marburg (Germany), Dr. Norbert Bernsdorff; as well as the President of Data Protection Supervisory Authority of Hungary, Prof. Dr. Attila Péterfalvi and the colleague of the same authority, the expert of artificial intelligence — Dr. Dániel Eszteri. The research papers published in the first edition of the Journal cover the topical issues such as: Legal Status of the Personal Data Protection Service of Georgia; Right to be Forgotten; Personal Data Protection Policy as a Transparency Indicator in Data Processing; Childrens' Personal Data Protection in Digital Environment with Different Expectations Between Parents and Children; Interdisciplinary Analysis of Institutional Role of Data Protection Officer in the System of Corporate Governance; Legal Assessment of the Use of Vehicle Marking of People with Disabilities to be Affixed on Vehicles in Terms of Personal Data Protection. The establishment of Journal was responded with the welcoming letters published in the first edition of the Journal by the following authors: the Rector of Berlin Steinbeis University, Professor at Ivane Javakhishvili Tbilisi State University, Dr. Giorgi Khubua; European Data Protection Supervisor — Prof. Dr. Wojciech Wiewiórowski; the President of the Personal Data Protection Supervisory Authority of Italy (Garante per la protezione dei dati personali) — Prof. Dr. Pasquale Stanzione; the President of the Personal Data Protection Supervisory Authority of Croatia (Agencija za zaštitu osobnih podataka) — Zdravko Vukić; the Coordinator of the project of German Foundation on International Legal Cooperation (IRZ) in Georgia — Assoc. Prof. Dr. Sulkhan Gamkrelidze.

[56] The official webpage of the Journal is: <www.journal.pdps.ge>.

THE INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE: "PERSONAL DATA PROTECTION IN THE DIGITAL WORLD"

In order to provide the platforms for discussions about the law on personal data protection, it is also noteworthy that the Service actively cooperates with the representatives of academic corpus and research-scientific institutions. The Service has launched the cycle of regular scientific conferences. From this point of view, the significance is attached to the International Scientific-Practical Conference on Data Protection in the Digital World organized by the Personal Data Protection Service of Georgia in December 2022. The first session was opened with welcoming speech by the President of Personal Data Protection Service of Georgia. The welcome speech to the participants of the event was given by the Chairman of the Human Rights and Civil Integration Committee of the Parliament of Georgia, Mikheil Sarjveladze and Advisor to Prime Minister of Georgia on Human Rights Issues, Niko Tatulashvili. Within the first session of the event, the audience was given the presentation by Professor Giorgi Khubua, the Rector of Berlin Steinbeis University; Stephan Breidenbach — Professor Emeritus at Viadrina University and Professor Emeritus at the University of Vienna (online) as well as Professor Zviad Gabisonia, the Director of the Research Centre at the University of Business and Technology. Speakers gave talks about the technological advancement and its legal aspects in terms of personal data protection. At the second session of the event, Lado Sirdadze, the Associate Professor at the University of Business and Technology and Legal Engineer at Knowledge Tools International GmbH, gave the presentation on innovative legal technologies. In the final part of the meeting, the presentations about the digital challenges facing the Personal Data Protection Service of Georgia, the analysis of the current legislation and its legal assessment were given by the employees of the Service.

The event was attended by more than 50 participants, including judges, members of the public, academic and the non-governmental sector.

A VISIT OF THE DELEGATION FROM KAZAKHSTAN SCIENTIFIC—RESEARCH INSTITUTE OF PRIVATE LAW

The delegation from Kazakhstan Scientific — Research Institute of Private Law Kazakhstan paid a visit to the Service in 2022. As part of the meeting, the Director of the Institute, Academician Maidan Suleimenov, and other researchers familiarized themselves with the mandate, activities, functions and legal organization of the Service. In order to share the experience of Georgian party in the field of personal data protection, the joint research projects are planned for the future.

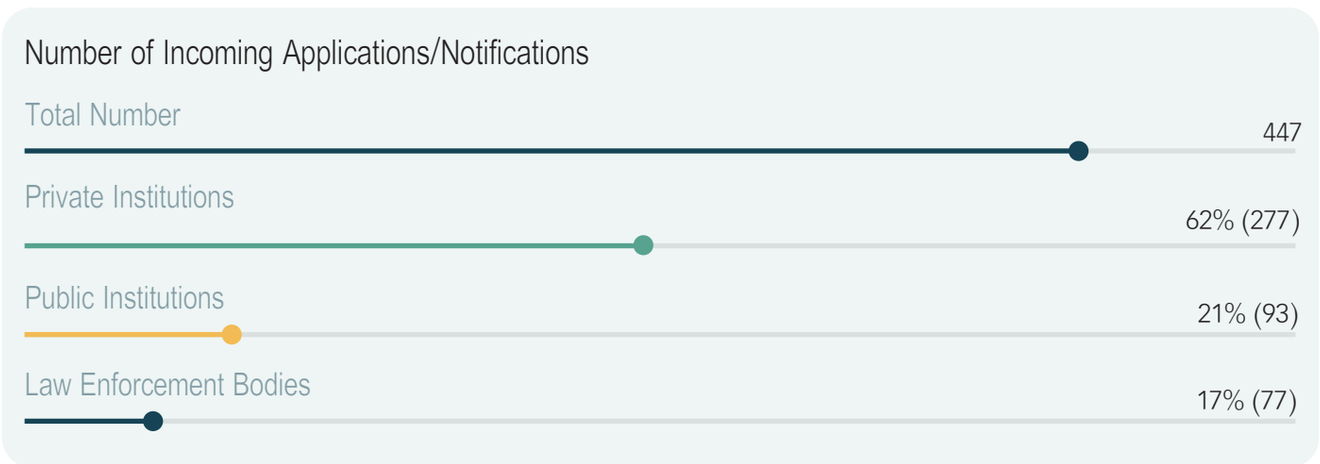
ANNEX №1: STATISTICAL DATA

1. STATISTICS ON MONITORING THE LAWFULNESS OF DATA PROCESSING

TOTAL NUMBER OF CONSULTATIONS HELD

3292

The Service conducts the consultancy activities on the issues about personal data processing. For this purpose, the Service is contacted by the representatives of private and public sector, law enforcement bodies as well as citizens. The consultations are provided both verbally (through telephone and face-to-face meetings) and in writing. In total, during the reporting period, the Service held 3,292 consultations on monitoring the lawfulness of personal data protection and other legal issues.



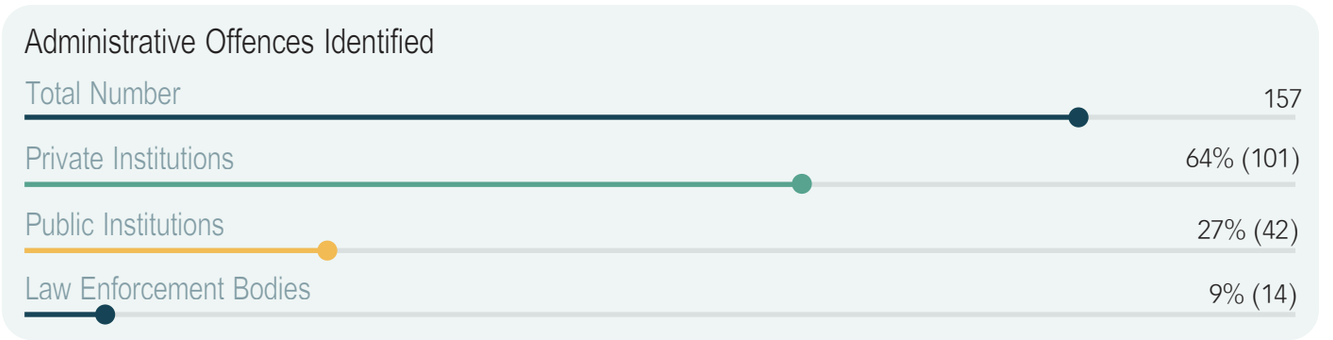
The total of 447 applications/notifications were received by the Service during the reporting period, out of which 64% (287) were applications and 36% (160) of them were notifications. 62% (277) of the applications/notifications received were related to data processing by private institutions/ natural persons, 21% (93) of them were regarding the data processing by public institutions and 17% (77) — law enforcement authorities.

AUDITS / INSPECTIONS CONDUCTED

According to the Order of the President of Personal Data Protection Service of Georgia No. 04 of 02.03.2022 "On Approval of the Procedure for Examination of the Lawfulness of Personal Data Processing", the planned examination (inspection) of the lawfulness of personal data processing is carried out in accordance with the annual inspection plan approved by the individual legal act of the President of the Service, while the unplanned examination (inspection) of the lawfulness of data processing is performed by the Service on its own initiative or by the notification of the person concerned.

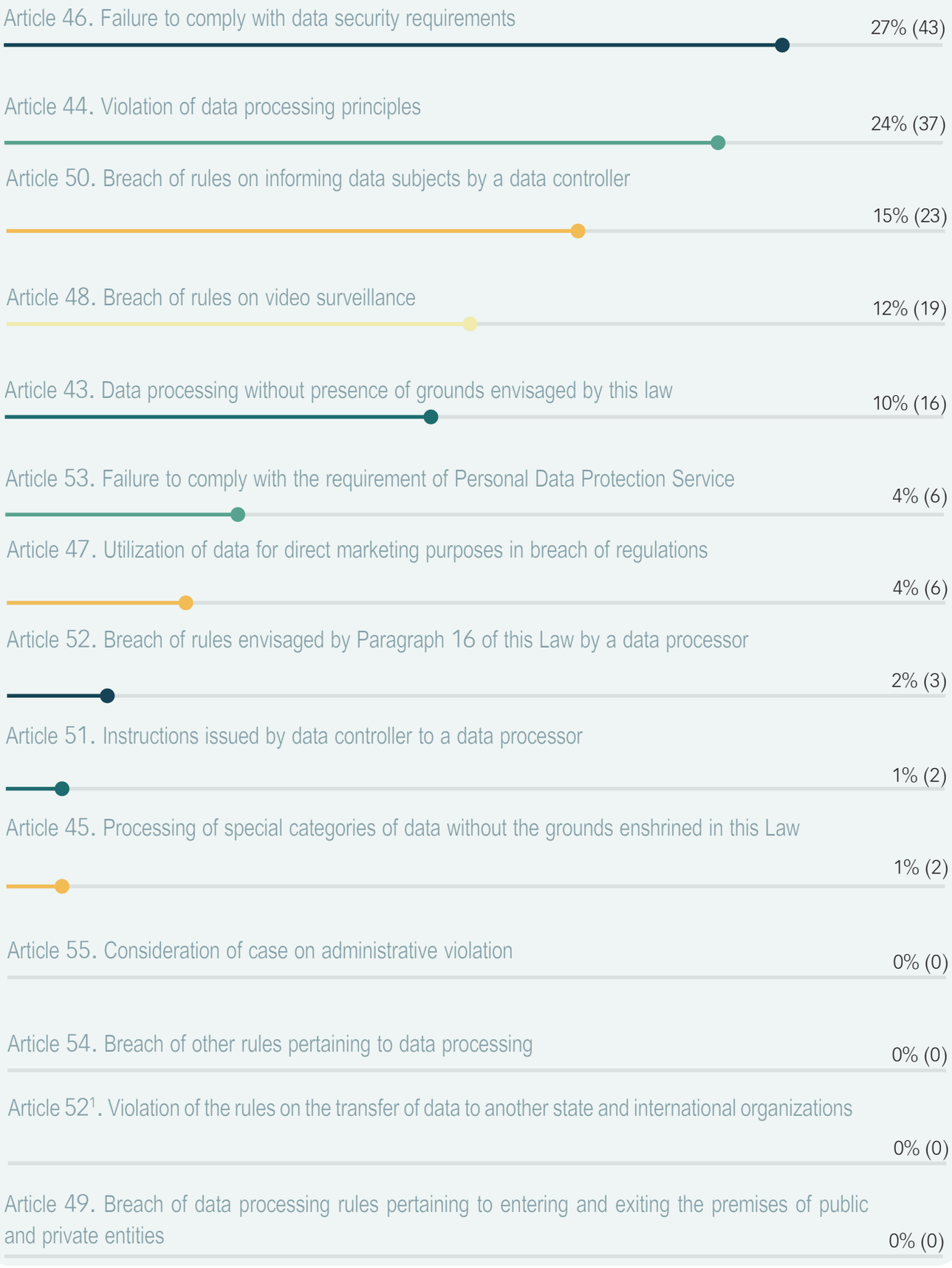
Based on the applications/notifications received, as well as on its own initiative, during the reporting period the Service carried out 149 examinations (inspections) of the lawfulness of personal data processing, out of which 68% (101 inspections) were unplanned and 32% (48 inspections) of them were planned.

Out of the 149 examinations (inspections) carried out, 54% (81) concerned the examination of the lawfulness of data processing by the private sector, 28% (42) — by public entities and 18% (26) of them was related to the processing of personal data by law enforcement bodies.



During the reporting period, the Service identified 157 cases of illegal processing of personal data. 64% (101) of administrative offences detected by the Service related to the private sector, 27% (42) of cases were identified in the public sector and the unlawful processing of data in law enforcement bodies amounted to 9% (14).

Administrative Offences Identified

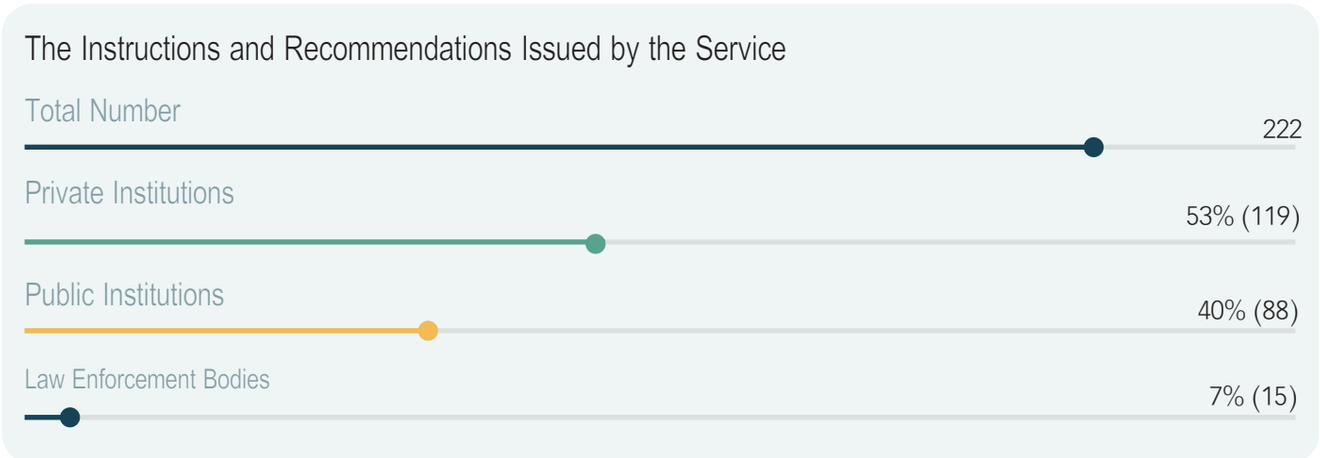


In the reporting period, 27% (43) of the 157 violations identified by the Service related to non-compliance with data security protection requirements, 24% (37) — violation of data processing principles, 15% (23) — breach of rules on informing the data subject by the data processor.

ADMINISTRATIVE PENALTY APPLIED

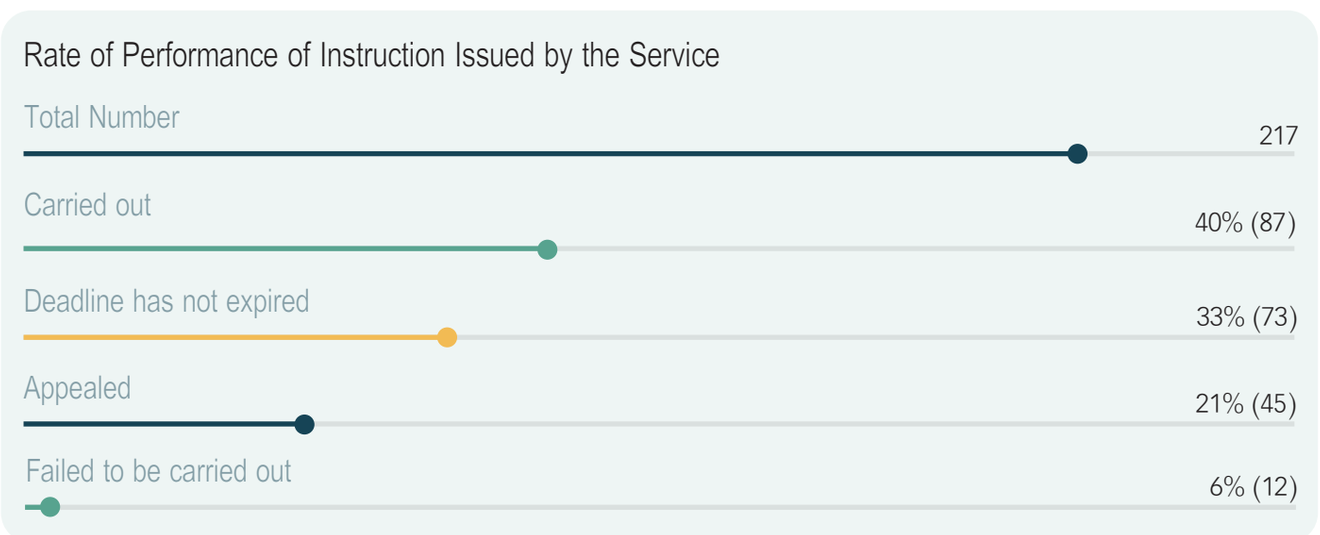
As a result of examinations (inspections) carried out during the reporting period, the total of 123 people were imposed the administrative penalty. Out of the identified administrative offenders, 86 persons (70%) were imposed the administrative fine and the warning was issued to 37 persons (30%).

Out of the administrative penalties imposed, 62% (77) related to private entities, 27% (33) – on public entities and 11% (13) was imposed on the law enforcement bodies.



In addition to imposing administrative fines, the Service issued the mandatory instructions[57] and recommendations[58] in order to eradicate the shortcomings and remedy the deficiencies identified in the institutions.

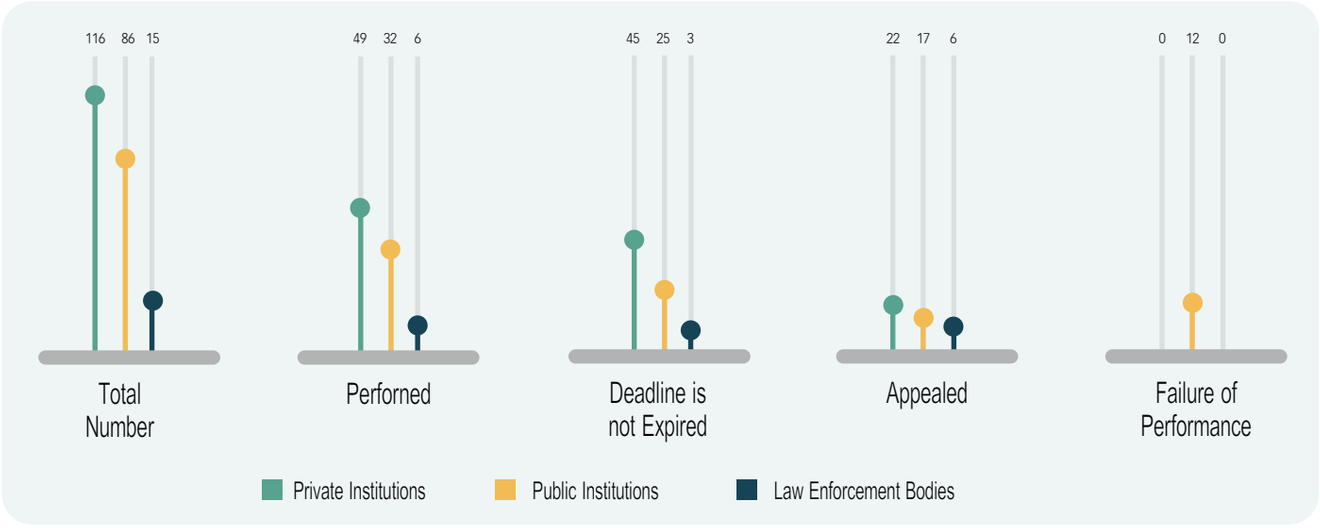
The Service issued the total of 217 instructions and 5 recommendations during the reporting period. 53% (119) of the instructions and recommendations issued addressed to private institutions, 40% (88) to public entities and 7% (15) was imposed on law enforcement bodies.



[57] Instruction is a mandatory direction to be fulfilled on implementation of events envisaged by sub. para. "a" –"d" of Art. 40[14] (1) of the Law of Georgia on Personal Data Protection issued to a data controller or/and data processor in writing by the Service.
[58] Recommendation is the advice issued to a data controller/data processor in writing by the Service in order to reduce the risks of violations in the course of data processing.

It is worth noting that out of the 217 instructions issued during the reporting period, 40% (87) of them were fully carried out, 21% (45) were appealed, 6% (12) were not carried out and as regards 33% (73) of instructions the deadline has not expired.

RATE OF PERFORMANCE OF INSTRUCTIONS ISSUED BY THE SERVICE ACCORDING TO SECTIONS

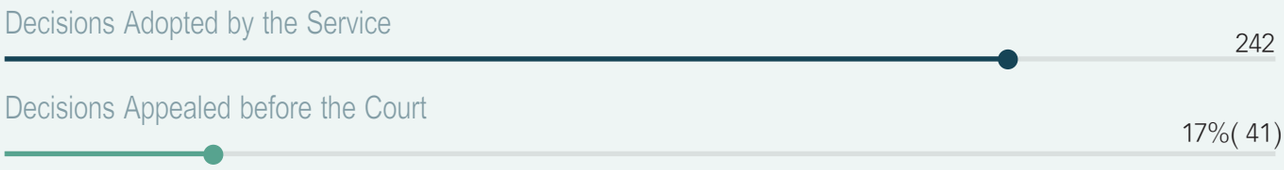


Out of the 116 instructions issued to private entities, 42% (49) of them have been performed, in case of 39% (45) the deadline for the performance of instructions have not expired and 19% (22) of them have been appealed.

37% (32) of the 86 instructions issued to public entities have been performed, the deadline of performing the instructions has not expired in case of 29% (25), and 20% (17) of instructions have been appealed and 14% (12) of them failed to be performed.

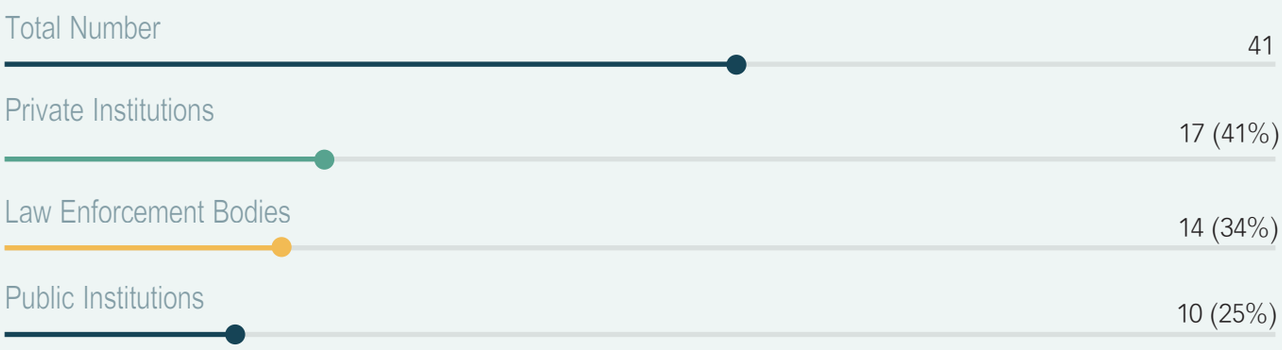
As regards the law enforcement authorities, 40% (6) out of the 15 instructions issued to them has been performed, 20% of the instructions are not overdue (3), 40% (6) of the instructions have been appealed.

RATE OF DECISIONS OF THE SERVICE APPEALED BEFORE THE COURT



17% (41) of the 242 decisions adopted in the reporting period are appealed, out of the mentioned 41 cases, the court examined 5 of them and left the decisions adopted by the Personal Data Protection Service of Georgia unchanged. Proceedings in 36 cases are still pending.

RATE OF DECISIONS OF THE SERVICE APPEALED ACCORDING TO THE SECTORS

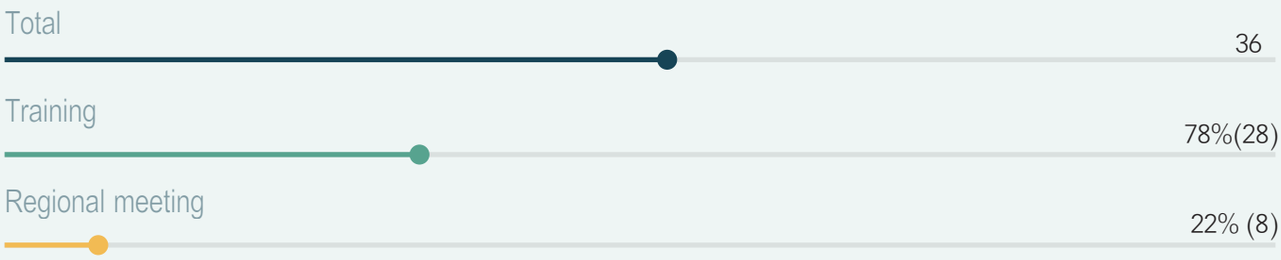


It should be noted that 41% (17) out of the 41 decisions appealed concerned the private entities, 34% (14) – law enforcement bodies and 25% (10) of appeals were against the decisions taken towards the public entities.

PUBLIC AWARENESS-RAISING,
INFORMATION MEETINGS AND TRAININGS

1007

THE NUMBER OF INFORMATION MEETINGS AND TRAININGS



It should be noted that 78% (28) out of the 36 meetings held were training meetings and 22% (8) represented the regional meetings.

2. OTHER STATISTICAL DATA

THE INTERNATIONAL TRANSFER OF DATA

In 2022, four private law entities contacted the Personal Data Protection Service of Georgia regarding the international data transfers. The personal data should have been transmitted by legal entities to the subjects existing in those states which are not included in the list of countries with the adequate safeguards for the personal data protection that is approved by Order №3 of March 2, 2022 of the President of Personal Data Protection Service of Georgia. Upon determining the above mentioned list, in particular, the so called "White List", the Service took into account the circumstances such as: the legislation of data protection being in force in the country, the existence of the data protection supervisory authority and its independence, etc.

The Service examined the applications and the documentation enclosed to determine the extent to which the proper safeguards are provided to protect data and the fundamental rights of data subjects pursuant to the International Data Transmission Agreement. When examining the appeals, the Service took into account such circumstances as: whether the grounds for data processing provided by the Law of Georgia "On Personal Data Protection" exist; whether the compliance with the principles for data processing envisaged by the mentioned law is ensured by the agreement; whether the exercise of the data subject's rights prescribed by the law is ensured by the data controller according to the agreement, etc.

As of December 31, 2022 the proceedings were completed in respect of 3 applications, all of which were authorized for data transmission, while the Service has not completed the discussion on the 1 application.

With the aim to ensure the high standards of personal data protection, the Personal Data Protection Service of Georgia carries out the legal expertise on the draft legislative acts and bylaws on the basis of referrals from the other agencies.

During the reporting period the Service assessed the compliance of 111 draft laws, 10 draft ministerial orders, 10 draft governmental resolutions and one draft order of the Head of another authority with the Law of Georgia "On Personal Data Protection".

In order to develop the expertise of the draft legislation and by-laws, apart from considering the written submissions, the representatives of the Personal Data Protection Service of Georgia were involved in oral discussions within the scopes of drafting the legal acts. A number of meetings were held between the representatives of the Personal Data Protection Service of Georgia and the state institutions, within which the Services shared its views on the respective project.

It is worth noting that as part of the expertise of legal acts, the Service identified a number of challenges. In particular, the draft legal acts developed by public entities did not properly ensure the compliance with the principles of data processing. In certain cases, there was not singled out the clear and specific purpose for data processing, which, in turn, created the risks of disproportionate data processing. There were identified the cases, in which the basis for determining the specific deadlines for data processing stipulated in the relevant Acts were ambiguous or no data storage

period was established at all. In a number of cases the project could not ensure the compliance with the principle of proportionality of data processing and envisaged the processing of such personal data, the necessity of which was not required at all. At the stages of creating and introducing a certain product, platform or database, the institution, in frequent cases, had not outlined the pre-formulated vision of the functionality of the particular product, platform or database and the need or necessity to process specific data in it due to the certain tight deadlines or other reasons. The above-mentioned, in turn, leads to the real risks of processing the irrelevant or disproportionate data. In such cases, a while later, having accumulated the relevant practice or experience, the institutions planned to implement the principle of data minimization and to revise the drafts of already adopted legal acts. It should be noted that in some cases data controllers were given the recommendations to regulate the technical and organizational security measures and rules on data by the legal act.

Apart from the above mentioned, as regards the special categories of data, it was detected that in some cases, processing of such data may not fall within the grounds laid down in Article 6 of the Law of Georgia "On Personal Data Protection".

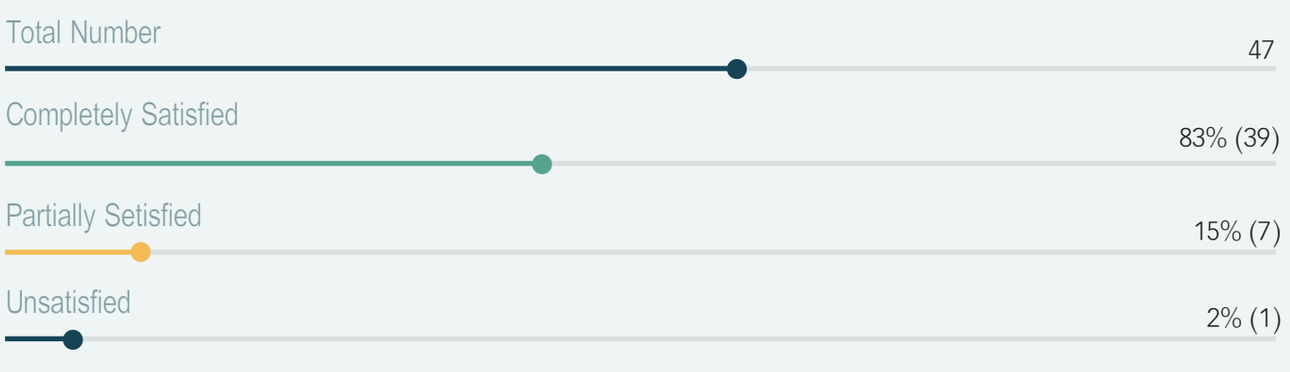
In some cases, the feedback was received from the public authority regarding the recommendations issued by the Personal Data Protection Service of Georgia within the expertise of the legal act. In particular, the Personal Data Protection Service of Georgia was notified which recommendation was or was not considered and their reasons.

The Personal Data Protection Service of Georgia will continue to actively liaise with the state entities within the evaluation of the compliance of draft legislative acts and bylaws with the Law of Georgia "On Personal Data Protection".

AGENCIES HAVING APPLIED TO THE SERVICE FOR THE PURPOSE OF CARRYING OUT LEGAL EXPERTISE

In order to assess the compliance with the Law of Georgia "On Personal Data Protection", the Service has been addressed by 7 state institutions for the expertise of draft legislative acts and bylaws. These institutions are as follows: The Parliament of Georgia; the Administration of the Government of Georgia; the Ministry of Internal Affairs of Georgia; the Ministry for Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs of Georgia; the Ministry of Education and Science of Georgia; LEPL – National Statistics Office of Georgia and LEPL – Emergency Management Service of Georgia.

Number of Requests Received Related to the access to public information



During the reporting period, the Service received 47 requests related to the access to public information, and in 7 of the cases the requests were partially satisfied because:

- In 1 case, the case file was requested together with the ruling and the person making the request did not represent the party to the proceedings;
- In 3 cases, the information requested was not fully stored/recorded in the Service;
- In 3 cases, the requested document was still being processed.
- In 1 case, the request was not satisfied because the information requested did not constitute the matter falling within the competence of the Service.

COMPLAINTS RECEIVED BY THE SERVICE AGAINST ITS DECISIONS

10

According to the Order of the President of Personal Data Protection Service No.04 of 02.03.2022 "On Approval of the Procedure for the Examination of lawfulness of Personal Data Processing" the individual legal acts of the structural unit of the Service may be appealed to the Service or to the court. During the reporting period, 10 decisions of the Head of the structural unit were appealed to the Service. In all ten cases, the Service upheld the decision taken by the Head of the structural unit of the Service.

LEGAL DRAFTING AND RELATED ACTIVITIES

11

In order to ensure the high quality of work performance of the Personal Data Protection Service and its institutional enhancement, the Service developed 11 by-laws.

PART II
INTERNAL ORGANIZATIONAL REPORT

1. INTRODUCTION

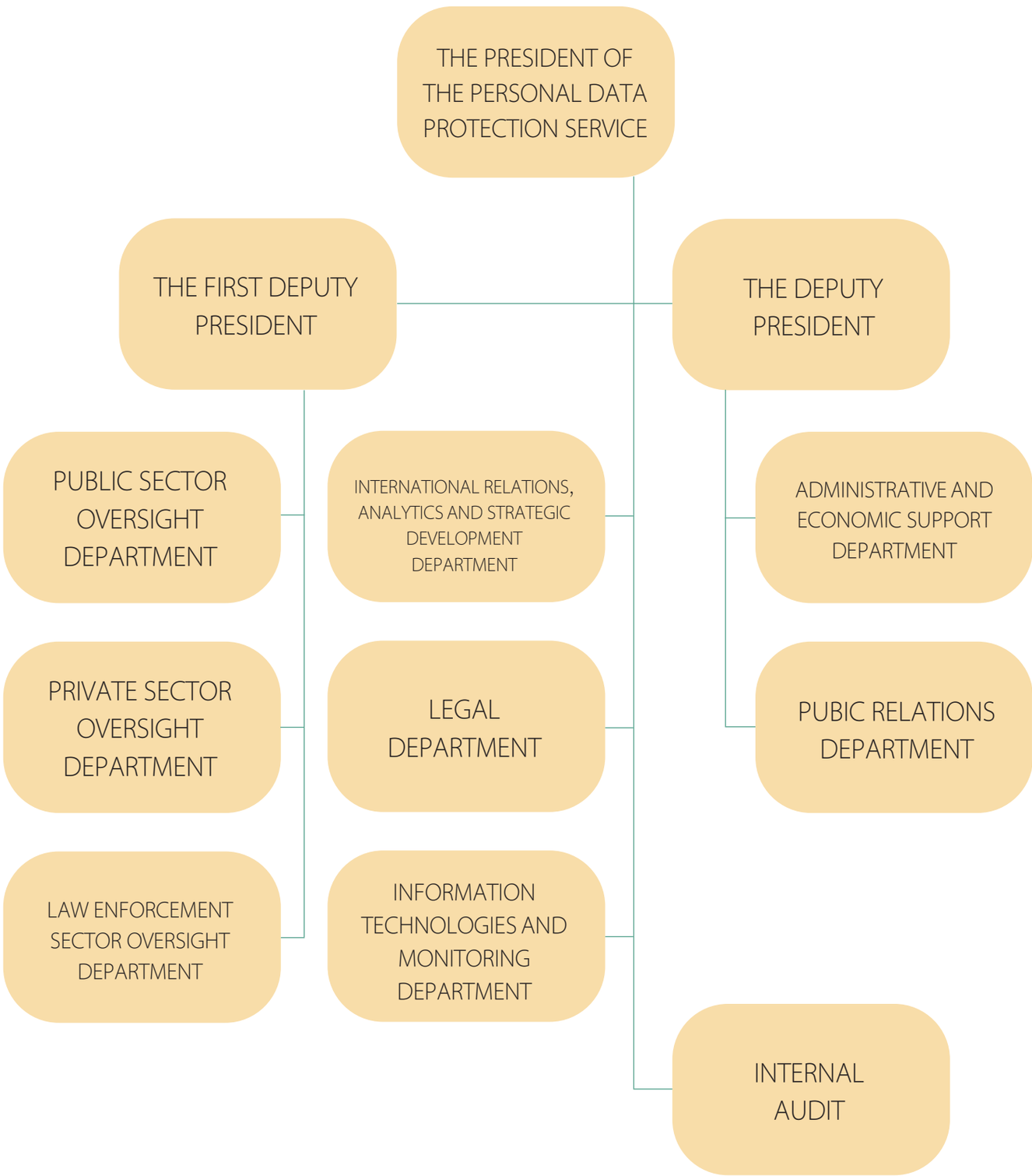
The organizational and financial autonomy of the Personal Data Protection Service of Georgia is regulated at the legislative level. The Service has an adequate logistical and technical basis for the effective performance of its mandate. The organizational structure of the Service, rules of distribution of activities and competences between the employees are stipulated by the statute of the Service. All the positions important for its autonomous functioning is defined by the staff list. The Service has the job descriptions for individual staff positions, staff appraisal rules, as well as the internal regulations and other documents of intra-institutional policy.

The Personal Data Protection Service is guided by the President, who is elected by the Parliament of Georgia for a 6-year term, and has two deputies. As of 1 March 2022, 50 staff positions were defined for the Service and 40 civil servants were appointed to the equivalent posts, and in accordance with its structure and staffing table, the Service is represented by 8 departments.

MARCH 1, 2022	QUANTITY
PRESIDENT OF SERVICE	1
FIRST DEPUTY PRESIDENT	1
DEPUTY HEAD	1
CAREER CIVIL SERVANT	40
VACANCY	8

2. ORGANIZATIONAL STRUCTURE

As of March 1, 2022, the intra-organizational structure of the Service was defined as follows:



3. ORGANIZATIONAL DEVELOPMENT

In order to fully and effectively fulfil the statutory functions and responsibilities as well as, having regard to the challenges posed to the Service, the decision was taken on making the intra-organizational changes until 2023. Considering the anticipated staffing level and existing plan, the Service developed such an organizational structure that ensures the high quality of citizen-oriented service delivery, reduced bureaucracy, simplified decision-making mechanisms, the increased rate of involvement and effective management.

3.1. REGIONAL COVERAGE

Depending on the mandate of the Service, within the relevant applications, notifications or planned examinations (inspections) the staff often have to travel on business trips to regions of Georgia, especially the Autonomous Republic of Adjara, which involves the additional budgetary costs and time. Occasioned by other functions of the Service, with the support of the Government of the Autonomous Republic of Adjara, by Order № 01-01-3/470 of 22 September 2022 the Service received free of charge and temporarily (for the period until the request of the Ministry) the premise and building area of 133.34 sq.m. and the land plot adjoining it in shares — c/k 05.29.04.001.01.500, which is on the balance sheet of the Ministry of Finance and Economy of the Autonomous Republic of Adjara and is located at N48, Bako Street in Batumi, so as to systematically implement the necessary measures to actively educate and raise awareness of citizens on thematic issues of personal data protection.

3.2. INSTITUTIONAL ENHANCEMENT AND CHANGES IN INTRA-ORGANISATIONAL STRUCTURE

For the purpose of institutional enhancement of the Service, the draft amendment to its regulation was prepared during the reporting period. According to the draft, from 2023, the strategically important staff positions will be defined in certain units and new functional units will be established. At the initial stage, there was discussed the necessity of establishing the Planned Inspections Department, the objectives of which are as follows: a) the planned control of the lawfulness of personal data processing in the public and private sectors, as well as by individuals; b) fostering the introduction of standards for processing and protection of personal data in the public and private sectors, as well as by individuals; c) promoting raising awareness of the public sector, the private sector, and individuals in terms of the personal data processing issues. Here it should be noted, that the competence of the department of planned inspection does not apply to the law enforcement bodies and those other public entities enshrined in Article 10 of the Service Statute, which fall within the competence of the Law Enforcement Oversight Department. Accordingly, the major functions of the Planned Inspections Department are as follows:

- Planned examination (inspection) of the lawfulness of personal data processing in the public and private sectors, as well as by individuals;
- Development of the draft annual plan for the inspections of lawfulness of personal data processing in the public and private sectors, as well as by individuals, and submit it to the President of the Service;
- Presentation of draft individual legal acts relating to the commencement, continuation, completion and other matters of the planned examination (inspection) to the President of Service or the person authorised by him/her;
- Within the scope of its competence, providing the consultations related to the personal data processing and analysing the issues arising in the course of the consultations as well as in case of identifying the legal deficiencies, preparing the appropriate proposals and recommendations for their elimination;

- Initiating the proposals for educational activities and trainings within the scope of its competence, as well as conducting them or participating in their implementation;
- Within its competence, the initiation of proposals and participation in their implementation in order to raise awareness of the target groups as well as the public about the activities of the Service and personal data protection;
- Based on the analysis of its activities in the public and private sectors, as well as by individuals, identifying the drawbacks with regard to the issues about personal data protection and preparing the appropriate proposals and recommendations to address them;
- Within the limits of its competence, reviewing the correspondence received by the department;
- Participation in commissions/working groups set up within the Service;
- Periodical recording and updating of the statistical data on the activities of department and submitting them to the Department of International Relations, Analytics and Strategic Development;
- Participation in the development of the Service strategies and action plans and their implementation within their competence;
- In order to inform the public, providing the information to the Department of Public Relations about the relevant projects, events and meetings planned by the department.

The functioning of the Planned Inspections Department as an independent structural unit will facilitate the active planning of inspections initiated by the Service and the effective verification of the lawfulness of data processing in this format. In addition, the department set up for this purpose better ensures the perfect assessment of risks existing in the area of data processing and the timely implementation of measures to counteract the mentioned risks in the form of planned inspections.

It should also be noted that the Office of the President of Personal Data Protection Service was set up as an independent structural unit. Its most salient objectives represent ensuring the uniform practice in decision–making process of the President of the Service, the coordination and control of the execution of decisions of the President of the Service and the organizational support of its activities as well as facilitating the communication of the President of Service with its various structural units in the framework of the inspection of the lawfulness of personal data processing.

Thus, the functions of the Office of the President of the Personal Data Protection Service of Georgia are as follows:

- Organisational, technical and informational support for the meetings of the President of Service and the Deputy Presidents of Service;
- Organisation of discussions/meetings of the President of the Service with the structural units and employees of the Service;
- Processing the information received on the name of the President of Service and coordinating its implementation;
- Upon the instruction of the President of Service, coming to agreement on certain issues with the relevant unit(s) of the Service and coordinating their implementation;
- Providing support for the preparation of public speeches and reports of the President of the Service;
- Developing/presenting the proposals and recommendations to the President of the Service on the effective functioning of the Service;
- The acceptance/correction of the draft decisions of the President of the Service prepared by the relevant structural units and their submission to the President of the Service;
- Analysis of draft decisions of the President of the Service prepared by the relevant structural units and the preparation of recommendations for the introduction of uniform practices;
- Coordination of accomplishing the decisions (including instructions and recommendations) taken by the President of the Service;
- Maintenance of the paper and electronic registry of protocols drawn up within the examination of the lawfulness of personal data processing and the decisions of the President of the Service;
- Identifying the shortcomings related to the case-handling and developing the appropriate recommendations in coordination with the internal audit, as well as encouraging the active cooperation with other departments and obtaining the relevant information, so as to foster the performance of activities.

3.3. CAREER MANAGEMENT AND THE NUMBER OF EMPLOYEES

The human resource of the Service is created by the employees who represent the workforce of the structural units of the Service. The career management of employees is one of the key factors for the Service to ensure the retention of professional staff in civil service, the development of their professional skills, the appreciation of their work performance and planning their carrier advancements. In this respect, it is worth mentioning that during the reporting period, the employees of the Personal Data Protection Service of Georgia participated in the internal competitions announced to fill the vacant posts exiting in the Service, which resulted in the selection of highly qualified and motivated staff. Also, in accordance with the legislation the employees of the Service were offered the opportunity to move horizontally to the vacant positions in the Service.

At the end of 2022, in accordance with the legislation, the evaluation of employees' work performance was carried out in the Service (10 months). Based on the results of the assessment, some employees were promoted to the civil servant ranks and given monetary awards.

As regards the number of persons employed, it is noteworthy, that as of March 2022, there were 42 persons employed on regular basis (40 — professional civil servants, 2 — state officials) and 8 persons were employed on contractual basis; As of December 2022, the number of regular employees made up 46 (43 — professional civil servants, 3 — officials), while the number of contract employees remained the same.

	March, 2022	December, 2022
State Officials	2	3
Professional Civil Servants	40	43
Contract Employees	8	8

As of December 31, 2022 the Number of Employees in the Personal Data Protection Service According to the Category Indicated, as well as from Gender Perspective

N	INFORMATION ABOUT EMPLOYEES	NUMBER	NUMBER OF WOMAN	NUMBER OF MAN	WOMAN %	MAN %
1.	TOTAL AMOUNT OF ACTING EMPLOYEES	54	27	27	50%	50%
2.	STATE OFFICIALS	3	1	2	33%	67%
3.	PROFESSIONAL CIVIL SERVANTS APPOINTED TO A MANAGERIAL POSITION	13	9	4	69%	31%
4.	PROFESSIONAL CIVIL SERVANTS APPOINTED TO NON-MANAGERIAL POSITION	30	16	14	53%	47%
5.	CONTRACT EMPLOYEES	8	1	7	13%	77%

The efficient and smooth operation of the Service depends on the professionalism and qualifications of its staff. Accordingly, the properly selected staff is the prerequisite for the success of any service. In this respect, the measures implemented by the Service in the area of recruitment during the reporting period are worth noting. In order to replenish the Service with new personnel, the competition for filling 13 vacant posts was launched in 2022. The recruitment was implemented on the basis of the open and internal competitions. In the process of decision–making about the recruitment and employment of the staff, the great attention was focused on the candidates' education, qualification, work experience, professional skills, personal qualities and motivation. It should be noted that the announced competitions went smoothly and all the positions were appropriately staffed.

COMPETITION WAS DECLARED IN 2022	TOTAL NUMBER OF APPLICATIONS/ CANDIDATES	WOMAN (CANDIDATE)	MAN (CANDIDATE)
13 VACANT POSITIONS	569	358	197

During the reporting period, 13 persons, among them 7 women and 6 men, were employed/ appointed to the post of professional civil servant in compliance with the competition.

COMPETITION WAS DECLARED IN 2022	SELECTED WOMAN (CANDIDATE)	SELECTED MAN (CANDIDATE)
13 VACANT POSITIONS	7	6

3.4. RAISING THE QUALIFICATION OF EMPLOYEES AND SOCIAL GUARANTEES

RAISING THE QUALIFICATION

Professional development and raising the qualification of employees of the Personal Data Protection Service of Georgia is a continuous process. In line with the new challenges, the Service constantly took care of the development of knowledge, competences, professional and social skills of employees during the reporting period. Each staff member was provided with the appropriate resources, equipment, as well as laptops, which is an important factor in the process of effective implementation of activities. In addition, in accordance with the competencies, all staff members were given the secure access providing the connection to electronic services.

In order to improve the professional qualification of staff, a three-day distance training on the methodology of inspection was successfully implemented in April 2022 within the framework of the EU Technical Assistance and Information Exchange Instrument (TAIEX). It should also be noted that in order to foster the internal organisational culture and actively share the experiences among the employees, the "Staff for Staff" project was successfully implemented at the intra-institutional level during the reporting period. As part of the project, the Service staff conducted the training sessions and workshops on various thematic issues: the prevention of sexual harassment and response mechanisms using the victim-oriented approach; the practical aspects of applying the Strasbourg Court judgments; the basics of information security, etc. It is also worth noting that the employees of the Service were actively involved in the series of trainings organised by the Civil Service Bureau, which were held remotely for civil servants.

In line with the new challenges, the initiative of the Service is to train the team of internal trainers for the purpose of ensuring their active participation in the educational activities organised by the Service. The aim of implemented and planned training activities is to foster the enhancement of the professional abilities of the employees and raise of their qualification. The above-mentioned ensures the consolidation of professional knowledge and development of skills for the staff, as well as the incorporation of the best internationally recognised intra-institutional standards into the day-to-day operations of the Service.

SOCIAL GUARANTEES

In November 2022, the package of legislative amendments was drafted in line with the prioritized objectives set by the European Commission Opinion of 17 June 2022 and in order to institutionally strengthen the Personal Data Protection Service of Georgia. It is noteworthy, that according to the amendments made to the Law of Georgia "On Personal Data Protection", the employees of the Personal Data Protection Service of Georgia will be subject to the state compulsory insurance starting from 2023; Also, the President of the Service is entitled to confer the state special rank to the employees of the Service in accordance with the legislation. The creation of the solid social guarantees aims, on the one hand, at strengthening the autonomy of the Service and the efficient functioning of human resources, which, on the other hand, conditions its institutional development and establishing itself as a desirable employer. In the institutional context the aforementioned will put in place the appropriate system for motivating the Service personnel, maintaining the qualified workforce and fostering the effective work culture, which will also be positively reflected in the growth of human resources and the attraction of new personnel.

3.5. ORGANIZATIONAL ETHICS AND DISCIPLINE OF THE STAFF

The internal regulations of the Service define the internal organizational culture and standards of conduct of employees. It aims to contribute to the effective management of the Service and the coordination of decision–making process. The internal regulations maximally provide the working conditions which is adapted to the interests of employees, including the preferential conditions, such as:

- Opportunity to work remotely for the defined number of days;
- By prior agreement, an employee is entitled to be released from the performance of his/her official duty on the days specified;
- Employee may be granted the right to engage in the scientific, pedagogical and creative activities during working hours for a specified period;
- Employee may be granted the right to carry out the activities for his/her professional development during working hours for a specified period of time.

It is noteworthy, that the general rules of ethics and conduct at work were fully complied with during the reporting period. The work performed by staff members and the decisions taken were based on the core values of the Service. The ethical environment was created in the Service and the relevant professional standards were set, which in turn ensures the increased public confidence in the impartial, objective and collegial public service.

The purpose of protecting the principles of employees' conduct at work is to prevent the cases of disciplinary misconduct, the abuse of authority granted by law, the cases of corruption, as well as to protect the principle of integrity and professional ethics. Accordingly, the Service steadily continues promoting the exemplary behaviour among the staff and the establishment of strong internal organizational culture.

3.6. ADOPTION OF INTERNAL INSTITUTIONAL DOCUMENTS

Since launching its functioning, the Personal Data Protection Service of Georgia has necessitated the establishment of the essential legal framework for its activities. To this end, during the reporting period, the President of the Service issued a number of normative acts approving: the regulation on the Personal Data Protection Service; the procedure for authorizing the transfer of personal data to another state and international organizations; the procedure for examining the lawfulness of personal data processing; the list of countries with proper safeguards for personal data protection; the rule and amount of remuneration of the employees of the Personal Data Protection Service; the samples of forms of the Personal Data Protection Service; the rule and conditions for the proactive placement of public information in the Personal Data Protection Service of Georgia and the standard for requesting public information electronically; the form of the protocol of administrative offence of the Personal Data Protection Service of Georgia, the procedure for its storage, use and the accounting-reporting rule, as well as the procedure for granting the employee the state special rank and his/her demotion to the special rank determined by Sub-paragraph "f", Paragraph 1 of Article 40^2 of the Law of Georgia on Personal Data Protection.

The Personal Data Protection Service of Georgia is empowered to carry out the controls of any data controller and/or processor on the basis of the application of the interested party, as well as on its own initiative. It should be noted that during the exercise of this authority the Service identifies the existing problems as a result of the analysis of the issues emerged in the process of the consultations related to the personal data processing, within its competence. The Service also assesses and takes into account the challenges pertaining to personal data protection that are detected as part of the messages received by the Service regarding a particular data controller/ processor. As a result, the Service determines the scope, subject matter and target groups for which the examination (inspection) of lawfulness of personal data processing is considered relevant and necessary. In addition, the Service defines the specifics, in terms of which the planned examination (inspection) is deemed expedient (whether it is the amount of data, the rights of the data subject or others). Having regard to the above mentioned, the relevant annual examination (inspection) plan for the lawfulness of personal data processing shall be approved by the corresponding Order

of the President of the Service. In the reporting period, for the purpose of improving the efficiency of activities of the Service, according to the Order № 11 of December 30, 2022 of the President of Personal Data Protection Service of Georgia, the Statute of the Personal Data Protection Service of Georgia was amended, under which a new structural department — the Planned Inspections Department was created.

In addition to the regulations, since the operation of the Service was launched, the individual administrative and legal acts necessary for its smooth and efficient functioning have been adopted. Among them, it is important that in order to organize the proceedings and document flow in the office, to create the necessary conditions for processing information through modern technical means and to increase the efficiency of activities of the Service, the rule on case handling of Personal Data Protection Service of Georgia was approved. The mentioned rule ensures determining the rule on the document flow by the Service and also simplifies the referral of the persons concerned.

Apart from the above mentioned, in order to implement the powers prescribed by Article 40^{16} of the Law of Georgia "On Personal Data Protection", which implies carrying out the covert investigative measures and the control of activities implemented in the central databank for electronic communications identification data, the Order of the President of Personal Data Protection Service № 01/250 of 28 December 2022 approved the procedure of taking the relevant measures. In particular, within the implementation of this mandate, the functions of the relevant structural units and the issues related to the management of electronic control system in the Service were defined. The latter will facilitate the smooth performance of covert investigative actions and the monitoring of activities carried out in the central databank for electronic communications identification data.

Apart from the above mentioned, the Service developed and approved the salient internal organizational documents, such as: the job description required for each position of the Service; additional and special qualification requirements for employees; employee assessment rules, etc.

PART III

FINANCIAL REPORT

1. BUDGET OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA AND ITS PERFORMANCE

According to Article 40[8] of the Law of Georgia "On Personal Data Protection", the activities of the Service are financed from the state budget of Georgia, while the necessary allocations are determined by the separate code. The approved budget for 2022 was GEL 2,750,000. As of March 1, 2022, 50 full-time positions were determined for the Service and 40 civil servants were appointed to the equivalent position, and in accordance with the structure and staffing table, 8 departments are represented in the Service. The cash flow of the budget amounted to GEL 2 671 862. It should be noted that the percentage of the cash flow performance in relation to the annual (10-month) plan makes up 97.16%.

N	ARTICLE OF BUDGET CLASSIFICATION	DETAILED PLAN	CASH FLOW PERFORMANCE
1	LABOUR REMUNERATION	1 710 105	1 709 544,78
2	GOODS AND SERVICES	662 929	586 856,17
3	SOCIAL SECURITY	8 806	8 805,46
4	OTHER EXPENSES	5 200	4 974,44
5	NON-FINANCIAL ASSETS	362 960	361 680,75
	TOTAL	2 750 000	2 671 861,60

It should be noted that the budget for 2023 amounts to GEL 5 million and the staff number is determined by 67 individuals.

2. SALARY, ALLOWANCE AND MONETARY AWARDS

During the reporting period, the employees of the Personal Data Protection Service of Georgia (including the President and Deputy Presidents of the Service) were issued the official salary in the amount of GEL 1,547,221.19, and the rank salary in the amount of GEL 293.55.

During the reporting period, GEL 45,467.54 was allocated as supplementary allowance to the employees of the Service, out of which GEL 2,740.81 was issued to the employees with special title within the obligatory supplementary allowance stipulated by the Law of Georgia "On Personal Data Protection"; GEL 9,935.73 was allocated within the mandatory allowance provided for in Article 26 (1) of the Law of Georgia "On Civil Service" and GEL 32,791.00 for additional functions and overtime work. In 2022, the bonus of GEL 116,562.50 was awarded to the employees of the Service.

The total amount of remuneration of persons hired under an employment contract (8 employees) during the reporting period equalled to GEL 155,366.51.

3. MEANS OF TRANSPORTATION

After the inception of the Personal Data Protection Service of Georgia in 2022, the total of 7 out of 28 vehicles were handed over to the Service, the actual cost of maintenance amounted to GEL 7,964.00 and the fuel cost made up GEL 31,050.91. Out of the mentioned vehicles, 1 vehicle, which was technically defective and could not be repaired, was handed over to the State Property Agency.

Occasioned by the above mentioned, in 2023, within the consolidated tender there is planned to purchase 4 vehicles, which the Service will receive in the 3rd quarter of this year.

4. REAL ESTATE LISTED ON THE BALANCE SHEET OF THE SERVICE

In 2023, with the purpose the organizational development of the Service, its institutional enhancement and fulfilment of its strategic objectives, the Service created new organizational units and the existing staff number was complemented by 17 units. In order to facilitate the establishment of the regional representations and staffing of new structural units, as well as the full and uninterrupted exercise of the powers conferred on the Service by the law, the great importance is attached to providing the employees with the work space. Occasioned by the above mentioned, 2 structural units of the Service will be housed in privately leased property in 2023.

During the reporting period, the Service was handed over the premises situated in str. Baku, Batumi, where the western office of the Service is intended to be housed. In order to provide the building with amenities, repair and renovation, the appropriate works will be carried out in 2023.
As of 2022, two real estates were listed on the balance sheet of the Service.

N	REAL ESTATE, ADDRESS	TYPE OF RIGHT	PURPOSE
1	TBILISI, VACHNADZE STR. 7	STATE PROPERTY, RIGHT OF USE	ADMINISTRATIVE BUILDING WHERE 8 DEPARTMENTS (ORGANISATIONAL UNIT) OF SERVICE ARE LOCATED
2	BATUMI, BAKU STR. 48	ADJARA A/R PROPERTY, RIGHT OF USE UNTIL DEMAND	ADMINISTRATIVE BUILDING WHERE WESTERN REPRESENTATION WILL BE LOCATED.

5. BUSINESS TRIPS AND OTHER EXPENSES

During the reporting period, the expenses of business trips within the country amounted to GEL 9,885.00 and outside the country to GEL 69,423.00.

During the reporting period, telecommunication (local and international telephone calls) expenses of the Personal Data Protection Service of Georgia made up GEL 8,220.00.

Also, the cost of advertising of the Service in 2022 made up GEL 5,756.41. It should be noted that only the events intended to raise public awareness were subject to advertising.

6. FINANCIAL AID PROVIDED BY DONOR ORGANIZATIONS

During the reporting period, the donor organization, in particular the United Nations Office for Project Services (UNOPS), provided assistance to the Personal Data Protection Service of Georgia with the acquisition of technical equipment:

DONOR ORGANIZATION	FORM OF ASSISTANCE	CONTENTS OF ASSISTANCE	COST	STATUS
UNITED NATIONS OFFICE FOR PROJECT SERVICES (UNOPS)	FIXED ASSETS	VIDEOCONFERENCING EQUIPMENT	GEL 2 728	COMPLETED

ANNEX № 2: PUBLICLY AVAILABLE INFORMATION ON FUNDING AND FINANCIAL ESTIMATE OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

The information on financial assistance (grants, loans) allocated to the Service by foreign governments, international organisations, public authorities at other levels

N	NAME OF ORGANIZATION	NAME OF THE PROPERTY GRANTED	GRANT VALUE (GEL)
1	UNITED NATIONS OFFICE FOR PROJECT SERVICES (UNOPS)	VIDEOCONFERENCING EQUIPMENT	43 405
2	LEPL – NATIONAL AGENCY OF STATE PROPERTY	ADMINISTRATIVE BUILDING TBILISI, VACHNADZE STR.7	1 505 438
3	MINISTRY OF FINANCE AND ECONOMICS OF A/R ADJARA	ADMINISTRATIVE BUILDING BATUMI, BAKU STR. 48	412 574
4	LEPL – NATIONAL AGENCY OF STATE PROPERTY	OFFICE FURNITURE AND EQUIPMENT	523 549
5	LEPL – NATIONAL AGENCY OF STATE PROPERTY	MEANS OF TRANSPORTATION	351 053

THE LIST OF VEHICLES ON THE BALANCE SHEET OF THE SERVICE, INDICATING THE MODEL AND THE YEAR OF MANUFACTURING

N	NAME OF VEHICLE	THE YEAR OF MANUFACTURE
1	KIA OPTIMA; LG917GL	2014
2	HONDA CRV; OO781GG	2013
3	TOYOTA CAMRY; PP643FF	2019
4	HYUNDAI ACCENT WW825UW	2021
5	HYUNDAI ACCENT WW816UW	2021
6	HYUNDAI ACCENT WW817UW	2021

In total, the public procurement amounted to GEL 657,500 in 2022, including the public procurement of GEL 607,450 for full operation of the Service and that of GEL 50,050 for the representation expenses.

PART IV

CONCEPT FOR STRATEGIC DEVELOPMENT OF THE SERVICE AND FUTURE PLANS

1. INTRODUCTION

During the reporting period, the Personal Data Protection Service of Georgia implemented a number of salient measures in the direction of improving the level of personal data protection in the country, as well as strengthening the mechanisms for controlling the lawfulness of processing personal data and covert investigative actions and the activities carried out at the central databank for electronic communications identification data. In 2023, the Service will continue its institutional development considering the following priorities:

- Improving the national legislation on personal data protection and ensuring its compliance with international standards;
- Organizational advancement of the Service;
- Strengthening the culture of personal data protection in the country and raising public awareness;
- Enhancing the international institutional recognition of the Service and deepening the international cooperation.

2. REFINING NATIONAL LEGISLATION ON PERSONAL DATA PROTECTION AND ENSURING ITS COMPLIANCE WITH INTERNATIONAL STANDARDS

The institutional advancement of the Service and the effective implementation of its mandate is directly proportional to the perfection of the legal regulation of personal data protection. The mentioned can be achieved by ensuring the compliance with internationally recognized standards and its consistent introduction in practice. Accordingly, there is no alternative to the priority placed on the further development of the Service with the aim to improve the legal framework and bring it even closer to internationally recognized standards.

From this point of view, the work carried out by the Service to ensure the compliance of the draft Law of Georgia "On Personal Data Protection" with European standards is noteworthy. It should be also noted that at the meeting held at the end of 2022, the Human Rights and Civil Integration

Committee of the Parliament of Georgia discussed the draft law at its first hearing with the active participation of the Service. It is noteworthy, that according to the action plan of the Human Rights and Civil Integration Committee up to 2023 the support to and preparation of the package of relevant changes to be discussed in the plenary sessions of Parliament, within all three hearings, represents one of the priorities for next year, in order to raise the standards for improving privacy and personal data protection. [59]

3. ORGANIZATIONAL DEVELOPMENT OF THE SERVICE

The development of infrastructure of the Service and its regional coverage as well as strengthening its personnel resource will be one of the topical issues for the Service in the upcoming year as well. The expansion of regional representation is an important priority for the Service, so as to effectively exercise its mandate, ensure the access to the Service and raise public awareness. Accordingly, in terms of fulfilling the mandate of the Service and its accessibility throughout Georgia, the Service plans to provide the regional representations, establish branches and equip them with the appropriate infrastructure and human resources.

As noted, in the reporting period the Service received the building for use located in Batumi, which will house the western representation of the Service. The offices are planned to be opened in Kutaisi and Telavi. The mentioned intends to make the process of examining the lawfulness of personal data processing in the regions easier and more flexible, as well as to raise awareness among the local population about the importance of personal data protection. In addition, the regional representation will create new employment opportunities for the local population.

In order to ensure more effective organizational development and activities, new structural units were created in the Service in 2022. These departments will start exercising their competence from 2023. The appropriate reinforcement of the newly created structural units and introducing

[59] See, 2023 Action Plan for the Committee of Human Rights and civil Integration of the Parliament of Georgia, <https://web-api.parliament.ge/storage/files/shares/Komitetebi/adamianis-uflebebi/samoqmedo-gegma/samoqmedo-gegma-adamiani-2023.pdf>.

further changes in the organizational structure of the Service, as necessary, will ensure the effective redistribution of workload of the Service units and the timely response to the challenges identified in practice.

In addition, the most important objective of the Service is to ensure the adequate working conditions for the staff, to encourage their professional development and to reflect the internationally recognized best internal standards in the day-to-day activities of the Service. The aforementioned will ensure the effective internal organizational culture, high quality of the Service activities and the maintenance of highly qualified staff.

4. STRENGTHENING THE CULTURE OF PERSONAL DATA PROTECTION IN THE COUNTRY AND RAISING PUBLIC AWARENESS

The strategic objective of the Service is to raise public awareness of personal data protection. Thus, the implementation of awareness-raising campaigns and various information events in the coming year will be one of the supporting measures to strengthen the culture of personal data protection in the country, raising public awareness and trust in the Service.

In order to create more efficient and organized mechanism for raising public awareness as well as to introduce the modern approaches and best practices in the field of personal data protection, the Service will organize information meetings and public lectures with relevant target groups next year as well. The said will have the positive impact on the exercise of the rights of data subjects and the quality of the realisation of their legitimate interests, and on the part of the data controllers, on the timely fulfilment of their statutory obligations.

5. ENHANCEMENT OF THE INTERNATIONAL INSTITUTIONAL RECOGNITION OF THE SERVICE AND DEEPENING ITS INTERNATIONAL COOPERATION

One of the main priorities for the upcoming year is to foster the international institutional awareness of the Service, deepen the cooperation with counterpart supervisory authorities of data protection abroad and with the international organisations in the field of personal data protection. This is directly proportional to the introduction of the best practices of the mentioned law on personal data protection. Accordingly, occasioned by the interest of maintaining the high institutional reputation at the international level, the Service aims to participate in the various international events planned in the field of data protection and privacy law, as well as to support or initiate modern approaches to the problem.

The Service is represented in a number of international committees and is an active participant in relevant discussion forums. The agenda is set for the expansion of the existing international cooperation. Accordingly, in the upcoming year the Service aims to deepen international partnerships, obtain the status of a member or observer in the forums of various fields. In addition, the Service will continue to actively cooperate with foreign supervisory counterparts on various thematic issues through consultations and sharing information about national legal regulations as well as the exercise of mandate of the Service. The Service plans to sign memorandum of mutual cooperation with supervisory counterparts and implement the joint projects within its scopes. Also, in order to enhance the internationalization and analytical component, the Service aims at studying the best practices and introducing modern approaches in daily activities of the Service with the support of leading experts and researchers in the field of personal data protection law.

PERSONAL DATA
PROTECTION SERVICE

Add.: Georgia, Tbilisi, N. Vachnadze N7, 0105
www.personaldata.ge
Tel.: (+995 32) 242 1000
E-mail: office@pdps.ge