PERSONAL DATA PROTECTION SERVICE OF GEORGIA

ACTIVITY REPORT 2023

PERSONAL DATA PROTECTION SERVICE

PERSONAL DATA
PROTECTION SERVICE

2023 ACTIVITY REPORT OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

The following report is prepared in compliance with Article 48 of the Law of Georgia “On Personal Data Protection” and Article 169 of the rules of procedure of the Parliament of Georgia, pursuant to which the President of the Personal Data Protection Service is required to submit an annual report to the Parliament of Georgia, no later than March 31st, regarding the status of data protection in Georgia, monitoring of the conduct of covert investigative actions, and the activities carried out in the electronic data identification central bank. The report contains details of the Service’s activities conducted from January 1, 2023, to December 31, included, in compliance with the prevailing legislation during the reporting period.

TABLE OF CONTENTS

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

We present the 2023 report of the Personal Data Protection Service of Georgia, addressing the status of data protection in Georgia, monitoring of the conduct of covert investigative actions and the activities carried out in the electronic data identification central bank.

In the age of artificial intelligence and technological advancement, safeguarding fundamental human rights and freedoms, including the right to privacy, personal and family life, as well as communication, demands particular emphasis.

In the current context, as Georgia has attained the status of a candidate country for the European Union and progresses towards European integration, it becomes imperative to align our legislation concerning personal data protection with that of the European Union. Consequently, implementing new standards at the national level is paramount. In this regard, the adoption of the new law marks a significant stride forward in the advancement of Georgian personal data protection regulations, protection of fundamental human rights and freedoms, and the institutional reinforcement of the Personal Data Protection Service of Georgia, a recognition emphasized by international experts.

In the pursuit of fortifying the institutional framework of the Personal Data Protection Service of Georgia, the year 2023 witnessed significant strides in cooperation with European Union institutions. Notably, the Service was granted the observer status of the "European Data Protection Board" ("EDPB"), and a novel model of collaboration with the "European Data Protection Supervisor" ("EDPS") was inaugurated. This signifies a profound endorsement of our Service by our European counterparts, which we consider a great honor and, concurrently, a responsibility.

The provided report encompasses the principal directions and trends in enforcing the lawfulness of personal data processing for representatives from both the public and private sectors, as well as law enforcement agencies. It delves into distinct topical matters, including: ensuring data subjects' access to their own data; safeguarding the personal data of minors; managing the processing of personal data pertaining to vulnerable groups; the protection of personal data in labor relations; the processing of personal data within healthcare, financial sectors, etc. Additionally, it outlines significant directions for overseeing covert investigative activities and operations conducted within the central databank of electronic communication identification data.

Additionally, the report encompasses precedent decisions made by the Personal Data Protection Service of Georgia, as well as assignments and recommendations issued following evaluations of personal data processing procedures by representatives from the public and private sectors, along with law enforcement agencies. Moreover, it provides details regarding the activities undertaken by the Service to implement the new Law of Georgia "On Personal Data Protection".

A primary focus of the Service's endeavors is enhancing public awareness and fostering a culture of personal data protection. To achieve this objective, the Service organized numerous scientific and

informative events. The statistical data from the Service's activities in 2023 underscored heightened public engagement with the Service and the extensive examination of the lawfulness of personal data protection and its outcomes. This report provides insight into matters concerning the internal organizational management of the Personal Data Protection Service of Georgia as well as its financial resources, offering the public comprehensive understanding on these fronts.

The Personal Data Protection Service of Georgia remains committed to fostering a culture of safeguarding personal privacy within the country, while upholding European values.

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

I

PERSONAL DATA PROTECTION STATUS

CHAPTER I. PERSONAL DATA PROTECTION STATUS

Data Processing Within the Public Sector

Throughout the reporting period, the Service examined approximately 100 cases of personal data processing within the public sector, addressed over a thousand advisory inquiries, disseminated essential information on data protection to stakeholders in the health and social sectors, and engaged in numerous coordination meetings regarding the development of various electronic systems and relevant databases to facilitate the implementation of appropriate preventive measures.

The incidents uncovered within the public sector are multifaceted and encompass various processes, including: employee-employer relations; data disclosure within the healthcare system; inadequate security measures; deficiencies identified in the layout of Service premises and shortcomings in specified data processing; data disclosure via websites; infringements upon the right to personal life inviolability of minors, such as detailed data disclosure about children within multi-member social network groups; dissemination of unnecessary information regarding numerous students on websites; operation of electronic security systems with configurations leading to unnecessary data acquisition; inappropriate organizational-technical measures posing risks of data disclosure; instances of restricting individuals' access to personal data across different contexts, and others.

1.1 Important Directions and Trends

During the reporting period, data subjects actively enjoyed the right to informational self-determination, applied to various public institutions and were interested in the materials in which they expected their personal data to be reflected. This, on the one hand, indicates the tendency of raising public awareness, although it is worth noting that frequently the same applicants are the ones utilizing the rights of data subjects. Moreover, several cases unveiled instances where the requirements outlined in the appeals were vague, impeding the timely provision of information to concerned individuals.

Among the cases identified in the public sector, there is a notable prevalence of violations concerning the transparency of data processing and the availability of information for individuals. This circumstance largely arises from the lower priority accorded to requests from individuals seeking information/materials regarding personal data, as well as from public servants' lack of familiarity with the legislative framework that provides guarantees, specific forms, and deadlines for individuals to access their data and relevant materials containing them. As an example, in accordance with personal data protection legislation, individuals have the right to actively engage in updating, correcting, and modifying their data. Additionally, they are ensured the right to attain a clear understanding of the processes involved in the processing of their data and to access the documents containing their recorded data. The aspects mentioned are bounded by the applicant's discretion in selecting the method of receiving information, the legal specification of acceptable information content, and the establishment of specific mandatory timeframes. For instance, within 10 calendar days, individuals must be informed about the processing of their information, and within 15 calendar days, any necessary changes, updates, or deletions must be made to unlawfully processed data, or the applicant must be informed of any rejections etc. Ignorance or inadequate attention to these factors often leads to violations of personal data protection legislation.

The challenge lies in accurately identifying information as personal data, which often results in incomplete or inadequate responses to data subjects' requests, consequently leading to their lack of awareness. It's crucial to note that the concept of personal data is extensive, encompassing any information (including opinions, facts, circumstances, evaluations, etc.) that pertains to an identified or identifiable individual in any manner. A precise understanding of personal data and its lawful processing is fundamental for the proper implementation of every provision outlined in the Law of Georgia "On Personal Data Protection."

To ensure transparency in data processing and provide timely and comprehensive responses to individuals' requests, institutions must tailor each process to accommodate the rights of data subjects. For instance, information should be processed in a manner where legitimate purposes are identified from the outset, details about the methods of data collection also the individuals for whom the data is provided should be maintained, and timestamps should be recorded for each such action, among other measures. It's worth noting that public institutions often experience delays in responding to citizens' requests for their own data, primarily because they must manually process the requested information, recall it, and then provide it.

During the reporting period, the Service underscored the significance of furnishing documentation containing their own data to minors, even in cases where they lacked a legal representative or were represented by individuals with disabilities. The Service did not accept institutions' justifications regarding resource constraints and resulting delays in responses. Instead, they were provided considering the best interests of the minor, within a reasonable timeframe, and with appropriate measures in place. For instance, engaging a social worker to communicate with children, allowing the social worker to read relevant materials to the minor in order to inform them, providing materials containing personal data in Braille for visually impaired minors, among other measures.

Disciplinary proceedings, particularly in terms of the lawfulness ofpersonal data processing, emerge as one of the most critical issues. Throughout the reporting period, instances of disclosing unnecessary information concerning the outcomes of disciplinary proceedings were observed, alongside cases where data subjects' requests for disciplinary proceedings materials were unreasonably responded by public institutions. These institutions often withhold case materials from data subjects, citing the belief that the right to access their own data supersedes the right to protect the personal data of witnesses, civil servants involved in administrative proceedings, officials, and others. It's crucial to emphasize that the law delineates both the right to information of the data subject and the grounds for restricting this right. Specifically, in accordance with Article 24, paragraph 1, subparagraph "e" of the Law, the data subject's right outlined in Article 21 of this Law may be curtailed if the realization of this right could jeopardize the rights and freedoms of the data subject and others. Furthermore, even in cases where there is a basis for restricting the data subject's right, such as the interest in safeguarding the rights of third parties, it is imperative to maintain a fair balance between the data subject's rights and those of third parties. To achieve this, it is imperative for data controllers to evaluate the extent of their legal interest and the proportionality of this interest in relation to the interest of protecting the rights of third parties, considering the context and content of the data subject's request. In line with both European and Georgian legislation, an outright refusal to fulfill the data subject's right solely on the grounds of protecting the rights of other individuals does not align with the standards of personal data protection. Typically, documents frequently contain the data of multiple individuals simultaneously, and imposing blanket restrictions on rights based on this premise renders guaranteed opportunities for individuals illusory. With modern technological capabilities, it's feasible to process

materials in a manner that either modifies them or conceals the identifying information of individuals and other data. Consequently, this approach not only safeguards against unlawful disclosure but also ensures that physical persons retain access to materials containing their data.

The cases identified suggest that disciplinary proceedings in labor relations are at times initiated based on communication from concerned citizens to public institutions. For instance, individuals may observe inappropriate behavior by a public servant and subsequently request the employer to assess it through disciplinary proceedings. In such a scenario, on one hand, there's the imperative to uphold the confidentiality of the data subject's (employee's) personal data, as highlighted by the Law of Georgia "On Public Service" conversely, there's the legitimate interest of a publicly accountable data controller a public institution, which aims to reassure an informed member of the public regarding impartial decision-making and effective responses by administrative bodies. It's important to note that confidential information may be shared with specific individual or group if there are legitimate purposes and legal grounds provided by law. However, imposing complete limitations without exceptions may unfairly restrict access to the activities of administrative bodies, diminish accountability to the public, and the risk of arbitrary decision-making. Accordingly, based on information provided by a third party, which is related to the illegal actions of a public servant, the agency may need to demonstrate its responsible approach by restoring or strengthening trust in the administrative body. It may also have a legitimate interest in disclosing the results of disciplinary proceedings to protect the reputation of the said body. However, there is a common tendency in such cases to disproportionately focus on the volume of information disclosed. Often, it suffices to inform the public merely about the fact that disciplinary proceedings were conducted, an unfair act was uncovered, and a penalty was imposed, without delving into specifics or divulging other details about the violation. In each unique circumstance, the data controller is obligated to adhere to the principle of minimizing the volume of processed data and, when processing personal data, to strike a fair balance between the legitimate purpose of data processing, the privacy of the data subject, and the right to protect personal data.

For public institutions, considering that their activities are regulated by legislation, the primary basis for data processing is typically the fulfillment of obligations defined by regulatory acts or directly provided by law. Additionally, data may be processed to protect legitimate public interests. Furthermore, agencies often seek the consent of the data subject as an additional basis for data processing, beyond the aforementioned reasons. When this is conducted through agreements, individuals often perceive granting consent as a mandatory condition. In such instances, it may be more advantageous for institutions to allocate a more informative burden to the contractual record rather than requiring consent. Instead, institutions can explain to individuals that they have specific legal grounds for data processing and legitimate, transparent, and specific purposes served by obtaining or further utilizing information about the contracting party.

Special caution must be exercised when publishing data through websites, as this medium makes information accessible to an unlimited audience. Therefore, the volume, necessity, and timing of the published information should be critically assessed. Public institutions typically engage in proactive information dissemination, which is an acceptable and necessary practice for transparency and good governance. However, it's common to encounter situations where published data becomes outdated due to changes in the statuses, positions, and organizational affiliations of individuals mentioned. In many cases, agencies lack written or established instructions regarding the content of data to be processed on their websites, as well as defined responsible individuals accountable for updating and removing information even after it has been published. The aforementioned practices lead to viola-

tions of the regulations stipulated in the Law of Georgia "On Personal Data Protection" and result in the unlawful processing of extensive personal data.

When instances of illegal data processing are uncovered, institutions frequently attribute them to human errors, with employees often acknowledging their actions. It's worth noting that, given the structural composition of public organizations, decision-making and execution typically involve multiple individuals. This arrangement serves to safeguard public processes from uninformed and incorrect decisions. Human errors in cases of verifying the lawfulness of data processing are primarily linked to institutions' failure to adopt preventive measures, inadequate assessment of risks and insurance, insufficient attention to enhancing employees' professional skills regarding the importance of personal data protection, and the absence of monitoring mechanisms to identify and address illegal activities, which results to the guilt of organizations;

During the reporting period, issues related to the correct assessment of their roles by public institutions and other agencies involved in data processing processes remain problematic. In one discussion, a case came to light where a public agency disclosed personal data to all other courts and The High Council of Justice, except for the court hearing the case because the agency considered them, as representatives of the judicial authorities to be a single data controller. According to the provisions clearly outlined by the law, the Service did not endorse similar argumentation and acknowledged each instance court, as well as The High Council of Justice, as distinct data controllers. They independently determine the means and purposes of data processing, based on the procedural legislation of Georgia. Furthermore, their level of intervention and participation in the dispute resolution process varies, and in some cases, a dispute may not even progress to any instance. Accurately identifying the statuses of institutions plays a crucial role in ensuring the lawfulness of data processing processes. During 2023, in accordance with the current version of the law, both data processor and data controller may engage in data processing. Their obligations and responsibilities differ, and the law outlines various forms for regulating the relationship between such individuals (such as agreements or legal acts), as well as conditions etc. While the primary responsibility for ensuring the lawfulness of data processing lies with data controlling organizations, if they enlist the Services of data processors, obligations are also extended to the latter, particularly concerning data security. Therefore, it is imperative for institutions to accurately assess the extent, duties, and functions of their own and others' involvement in these processes before commencing data processing.

Out of the violations identified during the reporting period, data security breaches are more prevalent. Electronic systems, often outdated, and at the stage of creation, little attention was paid to the functionalities necessary for the legal processing of data, frequently fail to comprehensively log actions conducted within databases. The latter is particularly critical for detecting unauthorized access, tracing illicit activities, implementing preventive measures, and so forth. Typically, various content operations are executed within databases, including creating, deleting, editing, downloading, viewing, forwarding, etc., records containing data. In each instance, it is crucial to record the content of the action, timestamp, identity of the person performing it, basis, etc. Additionally, such actions should be logged within the database, particularly in cases of direct access by individuals with administrator rights. Unfortunately, it is common to encounter situations where actions related to viewing data, as well as instances of direct database access, are not adequately logged in electronic systems. The primary risk of illicit actions against data arises from these unrecorded activities. Consequently, the investigations conducted by the Service aim, among other objectives, to identify and rectify such instances.

With the advancement of digital technologies, the responsibility for implementing adequate data security measures significantly intensifies. The effective operation of electronic systems largely influences compliance with the principles and fundamentals of data processing. The cases examined during the reporting period unveiled that electronic systems often collect more data than organizations require to fulfill legitimate objectives. Consequently, a significant volume of information is retained, such as the computer activities of employees, even though the institution's objective is solely to safeguard its information and identify hazardous files, computer programs, and links. Therefore, the pivotal stage at which institutions should commence implementing preventive measures for data protection is during the development of electronic systems and the issuance of instructions regarding their configuration to minimize the risks of unauthorized acquisition, disclosure, or other processing of personal information.

During the reporting period, instances of illegal data processing concerning minors by educational institutions and their staff were observed. Concerns were raised regarding deficiencies in informing them, numerous occurrences of disclosing detailed information about children's school activities to unauthorized individuals, and the implementation of video surveillance processes without adhering to security protocols. Every decision concerning a child must prioritize their best interests. Therefore, before obtaining, disclosing, or processing minors' data in any manner, schools and teachers, both in formal and informal settings, should prioritize evaluating their interests and strive to identify data processing methods that minimize unjustified interference with children's right to privacy.

Cases of illegal data processing in labor relations continue to be relevant. The Service reviewed several requests where the unauthorized collection of detailed information about employees' computer activities through electronic systems was contested. In some cases, similar electronic programs were identified, and mandatory directives were issued, promptly complied with by the data controller. This dynamic is further exemplified by requests from current and former employers for materials or information containing their personal data, often met with unconventional responses. Institutions frequently cite the significance of safeguarding the rights of other individuals in extensive materials, refrain from encrypting documents, thereby restricting the rights of the data subject.

During the reporting period, particular emphasis was placed on the security and accuracy of health-related data. Several electronic programs were identified that failed to meet data security requirements; for instance, they did not log information regarding data viewing, deletion, and/or downloading. Moreover, program users lacked personalized usernames and passwords. These instances pose a threat to the privacy of a sensitive category of human data. In cases of unlawful processing of information, including disclosure by an authorized individual without comprehensive action logs, the relevant details may go undetected, and the responsible party may remain unidentified. Additionally, recording actions performed on electronically protected data, along with regular monitoring of their legality, significantly diminishes the likelihood of unauthorized data access and prevents illicit data processing.

In the specific cases examined during 2023, particular attention was directed towards the necessity for doctors in medical institutions to conduct consultations with patients in private settings. An instance was uncovered where the consultation environment was arranged within the shared office of multiple doctors. Such a setup poses risks of data disclosure to third parties, which should be minimized given the extent and sensitivity of the data processed during the consultation process. For instance, when an individual attends a consultation involving two doctors sharing an office, there's a risk

that the presence of the other person may prevent privacy due to various circumstances, leading to the inadvertent disclosure of unnecessary information. Moreover, upon leaving the room, materials containing personal data may inadvertently remain visible to the next person receiving the Service. Additionally, it's conceivable that due to the volume of patients, all doctors' workspaces may need to be utilized. Considering these scenarios, the Service evaluated the necessity of modifying consultation spaces to safeguard the security of health-related data.

1.2 Instructions and Recommendations

The instructions issued by the Service during the reporting period encompassed the following matters:

- In instances where the risks of unlawful data processing cannot be adequately mitigated through a standardized practice, and where employees within agencies interpret established approaches differently, the agencies were instructed with developing written regulations, instructions, and employee training programs. It is noteworthy that oral regulations and practices, when compared to written internal organizational documents (such as statutes, instructions, rules, etc.), may exert less binding effect on individuals engaged in the data processing process. Therefore, it is advisable to document the sequence of data processing processes, specifying the precise volume of data to be processed, the timeframe, analyzing the categories of data and the legal bases for their processing, as well as outlining the organizational measures necessary to ensure the secure processing of data.
- In cases where instances of unlawful data disclosure were identified, directives were issued to delete information posted in social network groups.
- The instructions issued are designed to implement organizational and technical measures, ensuring that authorized individuals can access the electronic database solely through personal user accounts secured by appropriate passwords.
- The institutions were directed to implement organizational and technical measures guaranteeing the logging of all actions carried out on the data, inclusive of the identification of the individuals conducting the inspection, in the respective electronic systems.
- The instructions assigned to data subjects in cases of accessing information about them encompass sending specific documentation and/or information to natural persons. Additionally, the instructions involve redacting the data of other individuals, processing audio recordings, and providing partially depersonalized materials to ensure the accessibility of materials to data subjects.
- Instructions were assigned to modify the electronic systems to allow for the display of updated, highly reliable information about individuals upon their request and to present suitable evidence.
- An order was issued to ensure data security by transferring/exchanging information between electronic systems using an encrypted method. Additionally, a medical institution was instructed to modify its medical space to guarantee the confidentiality of patient information.
- During the reporting period, instructions were issued to ensure legal video surveillance, including changing the warning sign and placing it in a visible location, positioning the video recording device in a physically protected area (e.g., in a locked box), securing users of the electronic system with passwords, and recording all actions performed on data in video recording systems.

2. Data Processing Within the Private Sector

The Private Sector Oversight Department, aiming to ensure the lawfulness of personal data processing, conducted a series of inspections, both spontaneously and in response to notifications and complaints from concerned parties. They examined various instances of data processing by private organizations and individuals. Furthermore, to proactively address potential issues, consultations were provided to relevant individuals and organizations to implement preventive measures.

Specific issues regarding the lawfulness of data processing were addressed, including:

- ***Individuals' access to their personal data;***
- ***Protection of minors' personal data;***
- ***Personal data protection in employment relations;***
- ***Processing personal data in the healthcare sector;***
- ***Processing personal data in the financial sector;***

2.1 Important Directions and Trends

Individuals' Access to Their Personal Data

Ensuring individuals have access to their own data stands as a primary objective of data protection legislation and serves as a fundamental requirement for upholding various human rights. On one hand, this right enables individuals to stay informed about how their data is being processed, while on the other, it plays a crucial role in facilitating the exercise of other rights mandated by law. The right to access one's data is essential, as it empowers individuals to request deletion, blocking, and correction of their data as necessary. The necessity of the right to access data lies in providing the data subject with the ability to delete, block, and correct their data. Each individual plays a unique role in advancing a robust standard of personal data protection. Consequently, one of the primary challenges faced by the Service during the reporting period was promoting the fulfillment of data subjects' rights and implementing effective mechanisms for informing individuals and facilitating their meaningful utilization.

During the provision of access to personal data by an individual, instances of non-compliance or incomplete fulfillment of legal obligations by the data controller were identified:

☑ Instances were observed where data subjects were not provided with documentation containing their data within a reasonable timeframe or experienced delays in transfer. While personal data protection legislation may not stipulate a specific deadline for documentation transfer, this absence cannot justify unfair practices by data controllers or hinder the data subject's right to access their own data. Hence, it is crucial for data controllers to furnish requested documentation to individuals within a reasonable timeframe, considering the nature and volume of the requested material, to ensure timely preparation and transfer to the data subject.

☑ Through the analysis of the studied processes, instances were found where natural persons, acting as data subjects, were not informed within the 10-day period mandated by the law. In certain cases, data controllers cited legislative or by-law provisions as their basis for the timeframe for pro-

viding information to a natural person, which surpassed the deadline set by personal data protection legislation for informing the data subject. Data controllers are required to assess the content of the application or request from the data subject. In cases where an individual requests information about the processing of their personal data, data controllers should adhere to the 10-day notification period stipulated by personal data protection legislation. This timeframe accounts for factors like the volume and complexity of data collection, ensuring timely and objective transmission of information to the data subject. To safeguard compliance with the deadline, it is essential for data controllers to delegate responsibilities to staff effectively, preventing resource constraints from leading to breaches of the 10-day timeframe for providing information to the data subject. Data controllers must establish processes that offer an efficient means for data subjects to exercise their rights effectively.

In certain instances, there were occurrences where the rights of data subjects were restricted without their knowledge. Even if there are any legal justifications for restricting the rights of a data subject as outlined in personal data protection legislation, data controllers must ensure that the data subject is informed of the reasons for such restrictions in a manner that does not undermine the purpose of the restriction itself.

In certain instances, data controllers declined the data subject's request to provide documentation containing their data, citing prior provision of the requested documentation to the individual. It is important to consider that in order to uphold the data subject's rights as guaranteed by personal data protection legislation, data controllers should assess factors such as the timing of the last documentation delivery, any changes in circumstances since the initial request, and subsequently make an appropriate decision.

Cases of failure to provide information in accordance with personal data protection legislation were identified during the collection of data from natural persons. The law mandates that the data controller provides the data subject with the information outlined in Article 15 of the law during the process of obtaining information directly from the data subject, including during website registration. Data controllers must fulfill this obligation proactively, regardless of whether or not the data subject expresses an interest in this information. Furthermore, in accordance with the legal standards for data processing, providing this information is essential for effectively exercising the data subject's rights, as long as the information provided by the data controller allows the data subject to assess the need to provide/issue their data and also provides information about ways to protect their rights in the future.

Protection of Minors' Personal Data

The right to data protection for minors necessitates special attention due to their limited understanding of the potential risks associated with personal data processing. Minors often lack the knowledge and ability to independently utilize data protection mechanisms to safeguard their rights. Consequently, violations of their right to data protection can have detrimental effects on their psychological well-being and developmental trajectory. Therefore, institutions and organizations entrusted with handling significant volumes and sensitive categories of data concerning minors bear a critical responsibility in ensuring the protection of their personal data.

During the reporting period, the Personal Data Protection Service investigated several cases involving the processing of minors' data by private institutions and individuals as part of their entrepreneurial or professional activities, based on referrals. In accordance with the provisions of the Georgian Law "On Personal Data Protection," the Service undertook appropriate measures to address any

identified non-compliance or deficiencies in fulfilling obligations mandated by the law. The following performance facts were observed:

— During the reporting period, instances were found of the processing of personal data of minors without the legal basis stipulated by personal data protection legislation. Illegally processing personal data can be especially detrimental to minors due to their vulnerability, as they are less aware of the potential negative consequences of such processing. Therefore, data controllers must exercise special care when handling the personal data of minors and ensure that data processing is conducted strictly in accordance with the requirements outlined by law.
— Instances were identified where data controllers failed to implement adequate and effective measures to ensure data security. For instance, the personal data of minors stored in electronic form within the electronic system were accessed by authorized employees of the data controller using a shared user account. The use of a common account makes it challenging to determine who accessed the data, when, for what purpose, and to what extent. This lack of accountability increases the risks of unauthorized or accidental processing of minors' personal data. Therefore, data controllers must establish robust security systems that effectively prevent illegal and/or accidental processing of minors' personal data.

Personal Data Protection in Employment Relations

A significant volume of personal data is processed within the scope of employment relationships, stemming from its coverage of contractual, pre-contractual, and post-contractual interactions. Throughout the employment journey, employers handle the personal data of job applicants, current employees, and former employees for various purposes. These purposes include, among others, the recruitment of qualified personnel, the execution of employment contracts, compliance with legal obligations, and other relevant functions.

Employers commonly process personal data using various electronic systems. Given the volume of data involved, multiple individuals typically participate in the data processing process, potentially granting access to electronic systems to several personnel. Without the implementation of adequate organizational and technical measures to safeguard data confidentiality, there is an elevated risk of accidental or unlawful processing of personal data. Recognizing these challenges, protecting the rights of data subjects in labor relations remained a priority for the Service. In 2023, several measures were implemented to achieve this goal, including providing information on legal requirements for processing employees' personal data and raising public awareness on this issue.

During the reporting period, several instances of non-compliance or incomplete fulfillment of obligations mandated by legislation were brought to attention:

— During the reporting period, it came to light that employees' data was processed in violation of personal data protection legislation, particularly concerning video monitoring. The Service found that the data controller did not deem the purpose of video monitoring in the workspace as an exceptional case required by law. It is essential that data controllers, when conducting video monitoring in the workspace and processing employees' personal data, carefully assess whether a fair balance will be maintained between the legitimate interests of the data controller and the data subject's right to privacy and data protection. Additionally, they should determine whether there are exceptional circumstances warranting video surveillance in the workplace.

— Through the examination of various processes, it was uncovered that personal data of employees, including negative evaluations, were disclosed to third parties within the context of the employment relationship without the legal basis stipulated by law. It is crucial to consider that such disclosure of a negative evaluation to third parties can significantly impact the future professional advancement of the individual and may also result in reputational damage, undermining their fundamental rights and freedoms. Data controllers must therefore strive to strike a fair balance between the legitimate interests of the employer and the privacy rights of employees when disclosing employee data.
— During the processing of employees' data in labor relations, instances of violating the rules established by law regarding informing employees during video surveillance implementation were uncovered. For instance, entries in the bylaws concerning video surveillance in the workplace were of a general nature, and employees lacked specific information directly related to video surveillance in their workplace. In accordance with the requirements of personal data protection legislation, data controllers must provide clear and written information directly to employees regarding video surveillance in their workplace, without ambiguity to ensure a fair balance between the legal interests of the data controller and the data subject's right to privacy and data protection.

Processing Personal Data in the Healthcare Sector

Given the sensitive nature of information about a person's health, it is subject to a stringent standard of protection. Health data comprises highly intimate details about an individual's lifestyle, habits, mental, and physical condition. Its illegal disclosure can inflict significant harm to a person's personal and familial life, as well as their employment and societal integration. Regarding this matter, the following facts of non-fulfillment or incomplete fulfillment of the obligations imposed by the legislation were highlighted in the reporting period:

— During the reporting period, it was discovered that data controllers did not implement differentiated access to defined data for medical staff at the initial stage of data processing. For instance, a doctor from one department of a medical institution, who was not involved in the treatment of a particular patient, had access to information about another patient's health status. To enhance data security, it is imperative for data controllers to implement appropriate organizational and technical measures that effectively restrict unauthorized access to data as much as possible.
— Instances were identified where data controllers failed to implement adequate and effective measures to protect data security. For example, data exchange between a computer and a program server in a medical institution occurred without encryption, posing risks of accidental or unlawful data processing by third parties. To ensure data security, it is crucial for data controllers to implement appropriate organizational and technical measures, including encryption of data during exchange through the computer network.
— It is important to highlight that the issue of accurately accounting for all actions conducted regarding data in electronic form remains pertinent. For instance, while a program may record authorizations and changes made to data (such as additions, edits, and deletions), it may not log actions such as patient searches and views of data stored in the program in non-documentary form. Additionally, recording all actions performed with electronic data through a database presents challenges. Considering these factors, it is imperative to record all actions taken with data in electronic form accurately.

— Protecting the security of medical records maintained in physical form within medical institutions by their staff presents a challenge to avoid the risk of inadvertent disclosure to third parties. Processing organization is required to implement suitable organizational and technical measures to ensure the adequate protection of such documentation.

Processing Personal Data in the Financial Sector

The financial sector, encompassing commercial banks, microfinance organizations, lending entities, and distressed asset management companies, stands as one of the largest data controllers. Within this sector, a wide array of information is processed, spanning data concerning individuals' addresses, workplaces, financial obligations, transactions, and familial connections.

With the advancement of modern technologies, the instances of creating electronic databases through them and utilizing them for diverse purposes are steadily increasing within the financial sector every year. With automated data processing, the risks of errors and violations also grow. In the current reporting period, safeguarding personal data in the financial sector emerged as a significant challenge for the Personal Data Protection Service. Similar to the previous year, the Service persisted in examining cases of data processing in the mentioned sector and based on the urgency of the matter, implemented various types of measures.

Throughout the reporting period, the following instances of non-compliance or partial compliance with legislative obligations were underscored:

— Based on the processes analyzed, instances were identified within the financial sector where contact with third parties was made to locate a borrower. It's imperative for the financial sector to engage in such actions only when necessary, as contacting third parties and disclosing the purpose (e.g., locating a borrower) inherently involves revealing information containing the borrower's personal data. Therefore, representatives of the financial sector should ideally attempt to contact the borrower using the contact details they possess. Only if this method fails to achieve the intended goal should they resort to contacting third parties to locate the borrower.
— During the reporting period, instances were noted within the financial sector where contact with third parties to locate borrowers persisted despite their requests to cease. In cases where a financial sector representative seeks to locate a specific individual by engaging a third party, and the third party declines communication and requests cessation of data processing, the data controller is obligated to immediately halt and cease processing the third party's data for the stated purpose.
— Given the volume of data stored in electronic systems and databases and their ease of retrieval, systematic monitoring of access to such stored data is crucial for ensuring data security within the organization.
— Given the vast amount of data stored in electronic systems and databases, coupled with their ease of retrieval, it is imperative to implement suitable technical measures to safeguard the data within such systems, especially for the security of institutional data. During the reporting period, it came to light that a representative of the financial sector was offering users the option to transfer money by specifying a phone number in its application. Consequently, the name and surname of the owner of the specified number became known to the transfer initiator. The representative of the financial sector created a risk of unauthorized disclosure

of personal data in these instances. Specifically, individuals could potentially exploit the application not for money transfers, but to ascertain the identity of a phone number owner. Therefore, in accordance with Article 17 of the Law of Georgia "On Personal Data Protection," it is crucial for representatives of the financial sector to ensure that when transferring money via a telephone number, the recipient's data is modified to prevent their connection to the data subject, or that establishing such a connection necessitates a disproportionately large effort, costs, and time.

2.2 Instructions and Recommendations

During the period of 2023, the Private Sector Supervision Department issued 158 mandatory instructions and 2 recommendations to data controllers as part of their assessment of the lawfulness of personal data processing.

- Data controllers were given the following instructions:
- Transferring copies of documents containing personal data to the applicant;
- Removing the text containing the applicant's data, as well as photos and video recordings featuring the applicant's image, from the "Facebook" social network account;
- Under the agreement terms, furnishing the borrower with the requisite information for borrower identification and payment, inclusive of personal identification number and loan number;
- When gathering data directly from data subjects, informing them about "Personal Data Protection" in line with Article 15 of the Law of Georgia.
- Deleting personal data obtained through video monitoring conducted via surveillance cameras;
- Adjusting the viewing areas of surveillance cameras to align with their intended purpose, ensuring proportional surveillance coverage;
- Securing the video storage device with user credentials (username and password);
- Logging all activities involving electronically stored data.
- In the Internet Bank, when initiating a money transfer to a user's account within the same bank via phone number, altering the recipient's data to make it unidentifiable or requiring significantly disproportionate efforts, costs, and time to establish a connection with the data subject;
- Positioning the video recording device in a secure location inaccessible to unauthorized individuals;
- Identifying individuals requiring access to electronic data within the program and granting access solely to authorized employees pertinent to their roles;
- Establishing individual user accounts for authorized personnel who need access to the video surveillance system.
- Implementing suitable organizational and technical safeguards to prevent inadvertent or unlawful processing, including disclosing the identity of the data controller and data processor (if applicable) to the data subject(s). Additionally, supervising data processing activities conducted by data processor.;

- During data processing for direct marketing, informing the data subject of their right to request cessation of their data's use for direct marketing purposes at any time, and establishing an effective and accessible mechanism for exercising this right.
- Ceasing the processing of phone numbers for direct marketing;
- Informing the data subject about the procedure for requesting termination of data processing for direct marketing each time data is processed for such purposes;
- Discontinuing audio monitoring via the video surveillance camera positioned on the residential house's balcony;
- Ensuring the results of the patient's clinical-diagnostic examination are stored on the server for the shortest duration possible.

3. Personal Data Processing by Law Enforcement Bodies

3.1. Important Directions and Trends

Law enforcement agencies process personal data to conduct policing and preventive measures, investigations, criminal prosecutions, and the execution of punishments, as well as to protect and prevent threats to public safety. During data processing and the execution of their functions within criminal or administrative proceedings, they have access to various information databases containing extensive and sensitive personal data of individuals.

Reviewing the lawfulness of personal data processing by law enforcement agencies during legal proceedings, conducting covert investigative actions, and monitoring electronic activities enables the Service to identify trends and challenges in this domain.

In conducting covert investigative actions and overseeing activities within the Central Databank of Electronic Communication Identification Data, one of the primary function of the Service, adherence to Article 40[16] of the Law of Georgia "On Personal Data Protection" guides the Service. The Service carries out oversight of such activities in electronic communications companies by checking and inspecting the lawfulness of data processing in the electronic control and special electronic control system.

To comply with legal obligations and regulate issues outlined in the annual plan, a methodology for developing a plan ensuring the lawfulness of personal data processing was established. This methodology incorporates the assessment of risk factors that may lead to violations of human rights and freedoms during data processing.

In accordance with Order №01/20 issued by the President of the Personal Data Protection Service on January 31, 2022, the "Themes of the 2023 Plan for Lawfulness inspections of Personal Data Processing" and the corresponding "2023 Plan for Lawfulness inspections of Personal Data Processing" were endorsed. Considering the impact on specific target groups or areas, critical issues of personal data processing have been identified. The need for these issues arose from statements or messages submitted to the Service addressed to law enforcement agencies, either on their own initiative or based on a general analysis of planned inspections from the previous year, informed by practical experience and generalization.

Consequently, the planned inspections targeting law enforcement agencies prioritized examining the lawfulness of processing personal data, including special categories, pertaining to specific demographic groups such as minors, women, and individuals under state control. These inspections comprehensively addressed the activities of nearly all law enforcement agencies and encompassed various areas including covert investigative actions, electronic communications, modern technologies, labor relations, and more.

Planned inspections were conducted across various governmental entities, including the Prosecutor's Office of Georgia, the Ministry of Internal Affairs of Georgia, and the state sub-departmental institution under the Ministry of Justice of Georgia known as the Special Penitentiary Service (hereinafter referred to as the "Special Penitentiary Service"). Additionally, inspections were carried out at the LEPL "Operative-Technical Agency of Georgia" and Electronic Communications Company, the Ministry of Defense of Georgia, Investigation Service of the Ministry of Finance of Georgia, the State Security Service of Georgia, the Special Investigation Service, the National Agency for Crime Prevention, Enforcement of Non-custodial Sentences and Probation, and the Ministry of Justice of Georgia. Furthermore, ongoing inspections initiated in 2023 are being conducted at the Public Safety Command Center "112," as well as the Special Investigation Service and Operative-Technical Agency of Georgia.

The purpose of both scheduled and unscheduled inspections is not only to detect violations. To ensure unequivocal compliance with legal requirements, a uniform practice is developed, and appropriate recommendations or instructions are issued to law enforcement agencies. The Service actively assists law enforcement officials in enhancing awareness through a variety of activities.

3.2 Instructions and Recommendations

Considering the cases examined by the Service, identified trends, and specifics, law enforcement bodies should take into account the following in order to ensure the steadfast protection of human rights and freedoms, including personal life, as stipulated by the main purpose of the Law of Georgia "On Personal Data Protection", based on the areas outlined above:

- When examining the lawfulness of data processing, particularly disclosure, it's crucial to consider specific circumstances related to data processing, including: the public interest involved, the identity and status of the data subject, prior actions of the data subject, the data controlling entity, methods of data acquisition and it's accuracy, the content and form of disclosed data, the implications of data availability to the public, the predictability of these implications, etc;

- Given the heightened risks, even when law enforcement authorities have a legally defined basis, once this data becomes available to the public for an indefinite period, the risk of further dissemination or prevention becomes practically impossible to control. It is imperative to proactively evaluate the consequences of disclosure, striking a balance between public interest and the protection of personal data, as well as the rights of data subjects and interests of data controllers. In each specific instance, it is essential to assess whether disclosure is warranted and determine the amount of information necessary to achieve the intended objective;

- Law enforcement agencies are required to deploy video surveillance systems to fulfill lawful objectives, provided there is a relevant legal basis;

- To ensure the placement of video cameras in positions that guarantee video monitoring aligned with legitimate objectives, maintaining proportional coverage;
- Place warning signs, clearly displaying the description and complete data as specified by law, in visible locations where video monitoring is conducted;
- Develop a written document governing the administration of the video surveillance system, outlining rules and conditions for its management, including designating the individual responsible for system oversight;
- Guarantee the physical security of the video surveillance system;
- Provide access to records to a restricted group of individuals, considering their roles and operational requirements;
- Grant system access exclusively via individual usernames and passwords;
- Log all actions related to video recordings, including viewing, scrolling, downloading, deletion, etc. along with timestamps;
- When transferring video recordings to third parties, adhere to the requirements stipulated by the relevant law, strictly observing cases defined by law;
- When disclosing data for legitimate public interest, adhere to the principle of proportionality and refrain from disclosing data of third parties;
- Maintain records of all instances of video recording transfers to third parties;
- Facilitate the exercise of data subjects' rights, including the right to obtain a copy of the video recording, request deletion, blocking, or correction of the recording, receive information about the individual conducting the surveillance, the purpose and legal basis of the surveillance, or details about any transfers of the recording to others (including the basis and purpose);
- Ensure the deletion of deactivated or unregistered users from network video recording devices;
- Distinct periods for the retention of information regarding convictions should be established, aligning with the purpose of data processing and eliminating the indefinite storage of data. Additionally, clear guidelines for archiving, issuance, and access to such data should be outlined;
- The principles of data processing must be meticulously followed, and upon achieving the relevant purpose(s), data should be deleted, destroyed, or stored in a manner that precludes individual identification;
- Law enforcement authorities should consider that when processing data based on the written consent of data subjects, the consent form must explicitly specify the precise purpose, duration, and extent of the data subject's consent to processing. Additionally, data subjects must be informed of their right, as guaranteed by the Law of Georgia "On Personal Data Protection," to withdraw their consent at any time without providing a reason, and to request the cessation of data processing and/or the deletion of processed data;
- Law enforcement authorities must prioritize the significance of informing data subjects. Considering the nature of their operations, they should accurately assess data subjects within the timeframes stipulated by the law and ensure the timely and equitable fulfillment of data subjects' rights as

per the legally defined timeframe. Failure to provide information or documentation, or delays in doing so, could potentially result in irreparable harm to the data subject. Additionally, information may lose its relevance and no longer serve the interests of the applicant after the expiration of the deadline;

- Efforts should be intensified to implement measures or establish mechanisms aimed at mitigating the risks of delaying the fulfillment of data subjects' requests;

- When restricting the rights of data subjects, citing the relevant legal basis of the Law of Georgia "On Personal Data Protection," authorities should provide comprehensive information to the data subject in a manner that does not compromise the purpose of the right restriction;

- During the course of the investigation or administrative proceedings, it is imperative to adhere to reconciliation with imperative laws. For example, a fair balance should be maintained between the norms regulated by the Criminal Procedure Code and the requirements of the law on personal data protection;

- Law enforcement authorities must implement all requisite organizational and technical measures to safeguard personal data against inadvertent or unlawful disclosure, acquisition, and/or unauthorized use in any manner;

- All actions taken concerning electronic data must be meticulously recorded, enabling the identification of the individual accountable for specific actions;

- Access/authorization to various systems containing personal data should be granted to authorized individuals using individualized or personalized usernames and passwords;

- For recruitment purposes, data controllers should gather only the essential data required for candidate selection and competency assessment. Additionally, when collecting candidate data, consideration should be given to the acceptable type of work and the genuine requirements associated with its performance;

- Employers must evaluate the duration for which it is necessary and pertinent to retain the data of job applicants. After this period expires, employers should ensure that the data is either deleted, destroyed, or stored in a non-identifiable format;

- Even if there is a legitimate interest in monitoring employee behavior, the right to respect the employee's personal life should be upheld. Employees should be informed in advance about the nature and scope of video/audio monitoring to fulfill the legal requirement of providing written notification;

- When processing data based on consent, data subjects must be informed about their right, as guaranteed by the Law of Georgia "On Personal Data Protection," to withdraw their consent at any time without providing an explanation. They may also request the cessation of data processing and/or the deletion of processed data;

- When processing data of minors, it is paramount to prioritize their best interests throughout the data processing activities;

4. Planned Inspections of the Lawfulness of Data Processing

4.1 Important Directions and Trends

One of the methods for verifying the lawfulness of personal data processing is through planned inspections, conducted in accordance with the annual inspection plan approved by the President of the Service. It's important to highlight that the Department of Planned Inspections, established in 2023, is tasked with conducting planned inspections to assess the lawfulness of data processing in both public and private sectors, as well as by individuals. Additionally, the Department of Planned Inspections is obligated to develop the annual inspection plan project and submit it to the head of the Service.

It should be noted that the purpose of developing the annual plan of inspections is to ensure the efficiency and consistency of the Service's activities amidst the diversity, dynamism, and complexity of data processing processes in everyday life. The annual plan is formulated through a comprehensive examination of data processing legislation and practices, identification of priority and high-risk areas/processes in various regions of Georgia, and analysis of specific risks associated with these processes. This approach facilitates the purposeful and effective allocation of the Service's resources. It is worth noting that the absence of an inspection plan or its improper preparation creates the danger of not allocating sufficient attention to high-risk areas or processes regarding potential personal data breaches. Hence, it is crucial to formulate a plan based on predefined and clearly understood criteria and stages, aimed at effectively identifying priority and high-risk data processing areas/processes within the available resources. To achieve this goal, the Service developed a methodology document during the reporting period. This document outlines the procedure and criteria for selecting organizations engaged in activities within the public and private sectors for the purpose of examining the lawfulness of data processing.

It's important to highlight that the criteria (risk factors) outlined in the aforementioned methodology document identify areas with a high likelihood of human rights and freedoms violations. These criteria encompass: Processing large volumes of data; A substantial number of employees within the organization processing personal data; Processing special category data, biometric data; and personal data of vulnerable groups (such as disabled individuals, minors, women, socially vulnerable persons, etc.) by the organization; Utilization of modern technologies in personal data processing; Data processing within the context of employment relationships; Processing data that is made public; among others. Considering the mentioned criteria, public and private organizations subject to inspection during the reporting period were identified, where the likelihood of violating the right to personal data protection was deemed high. Consequently, the 2023 plan for scheduled checks (inspections) of the lawfulness of personal data processing was endorsed by the President of the Personal Data Protection Service through Order №01/20 issued on January 31, 2023.

Throughout the reporting period, the planned studied activities regarding data processing revealed significant trends and directions across various sectors, particularly concerning the processing of personal data related to vulnerable groups and data security protection. Notably:

Data Processing Within the Framework of the Labor Relationship

Processing personal data within the scope of employment relationships necessitates specific protection. In this process, organizations must operate with consideration for the interests of both employees and job seekers. An analysis of planned cases studied conducted by the Service consistently un-

covers instances of violations and deficiencies in data processing by diverse public and private entities within the context of labor relations:

— In some cases, organizations keep the personal data of job seekers indefinitely in order to consider their resumes for various vacancies in the future. It is worth noting that storing the data of persons seeking employment for an indefinite period cannot be considered legal, since after a certain period of time, the data about this or that person in the resume/questionnaire/application may become outdated or change, or the person may no longer be interested in employment in a particular organization. In order to make a decision regarding the employment of a candidate within the framework of a new vacancy, the organization will need updated information about the person;

— In certain instances, job seekers are not adequately informed about the processing of their data. This issue becomes apparent when data controllers fail to disclose the identity of the authorized person responsible for the processing and their registered address during the data collection process. Additionally, the rights of the data subject are not communicated, thus contravening the regulations regarding informing the individual concerned.

— An incident came to light where the organization, without the Service's authorization, provided the data of job seekers to a company registered and operating in another country. This action constitutes a breach of regulations governing international data transfers.

— Most organizations have failed to implement adequate and effective measures to safeguard data security. In numerous cases, certain organizations either failed to document or incompletely documented the actions taken concerning the data. Furthermore, employees within these organizations accessed data in electronic systems using a shared username and password, and instances of data sharing to unauthorized individuals were also detected. Without proper documentation of data-related actions, organizations are unable to conduct comprehensive monitoring to determine who accessed the data obtained within the scope of employment relationships, when, for what purpose, and to what extent. Consequently, in specific instances such as illegal disclosure of personal data, identifying the individual responsible for the breach becomes challenging or even impossible.

— Instances were identified where organizations utilized biometric data of employees to monitor entry and exit from buildings. While it is true that the nature of the employment relationship necessitates tracking working hours and attendance, the use of biometric data for this purpose is not lawful. The Law of Georgia "On Personal Data Protection" specifically governs the logging of employees' entry and exit from the workplace, specifying the data that can be collected for this purpose and the maximum duration of its retention. Employers are permitted to collect only specific data (such as name, surname, identification document number, facial image, employee address, entry and exit dates and times, and reasons) to monitor entry and exit from buildings.

— The majority of organizations lacked a formal rule or instruction to govern the process of requesting and receiving detailed statements regarding communication means (telephone numbers) assigned to employees in a manner that prevents access by employers. In certain instances, the procedure for requesting extracts was informally regulated verbally, which fails to ensure the establishment of a consistent and predictable data processing process.

— Instances were identified where video surveillance in changing rooms and the consequent processing of employees' personal data occurred. It should be noted that depending on its function, the changing room constitutes a highly private space. Therefore, monitoring individuals in this area is unjustified for any purpose.

Data Processing of Vulnerable Groups (Minors, Persons with Disabilities and Women).

The processing of personal data pertaining to vulnerable groups demands heightened standards, necessitates enhanced protection, and imposes substantial obligations on organizations. This is because unlawful processing of data concerning vulnerable groups can inflict irreparable harm upon their interests, reputation, and future prospects. An examination of cases conducted systematically by the Service indicates that various public and private organizations exhibit certain violations and deficiencies in their processes of data processing involving vulnerable groups:

- In one school, it was discovered that video surveillance was conducted in violation of the law, specifically in areas designated for hygiene. In certain instances, it was observed that the toilet area within the restroom fell within the field of view of video surveillance cameras installed in the corridor, particularly when the entrance door of the toilet was left open. While hygiene spaces typically feature closing doors, minors, who may be less conscious of privacy risks, might inadvertently leave the entrance door open while using the area, thereby exposing their actions in the hygiene space to the view of video surveillance cameras.

  In certain instances, organizations fail to establish defined retention periods for minors' data and instead retain personal data indefinitely. However, certain data become outdated over time, lose their relevance, and no longer necessitate storage. Indefinitely retaining such information can be particularly detrimental to minors, considering the significance of their integration and development within society.

- In certain cases, organizations neglect to update the data stored in databases concerning minors, despite the potential changes that may occur over time. This approach exposes the organizations to the risk of processing inaccurate data, which can result in significant harm to the child.

- A situation arose where students' data was not completely archived in the electronic system following the termination of their active status. It is worth noting that data archiving serves to minimize access to data by individuals who may not require it to fulfill their assigned duties.

- In certain instances, organizations process and retain data of vulnerable groups, including students falling under special categories, to a greater extent and for a longer duration than necessary to fulfill a legitimate purpose. It's important to note that acquiring and storing unnecessary data heightens the risk of disproportionate data processing.

- Even in the processes of data processing concerning vulnerable groups, most organizations have failed to implement adequate measures to ensure data security. For instance, organizations either do not record or incompletely record all actions taken on data. The potential for accessing the organization's electronic system from the open Internet network was also emphasized. In certain cases, the password complexity and character requirements were not predefined in the program, allowing for the selection of any password, including simple ones. Furthermore, there have been instances where individuals had the opportunity to access data of women who were victims of violence, even though such access was unnecessary for the performance of their assigned duties.

Data Processing of Young People

One of the objectives of the state youth strategy is centered on safeguarding the personal data of young people. As outlined in the 2023 plan, young people were identified alongside other target

groups for inspections. An analysis of cases examined systematically by the Service indicates that various public and private organizations exhibit certain violations and deficiencies in their processes of processing data concerning young people:

- Instances were identified where certain universities processed the data of a special category of students without a corresponding need and with a disproportionate scope of purpose. Furthermore, certain universities lacked clear definitions or did not establish terms for the storage of data processed through educational portals, thus violating data processing principles.

- In numerous cases, organizations enlist the services of various entities for the administration and maintenance of electronic databases used in processing youth data (such as hosting data on servers and providing technical support for websites). However, when entering into contracts for such services, the requirements outlined in Article 16 of the Law of Georgia "On Personal Data Protection" are often overlooked. These requirements would regulate the obligations of the contracting organization regarding the protection of personal data, including the implementation of security measures. The written formulation of data protection guarantees and the mechanisms for their implementation represent one of the effective methods for ensuring the legal processing of personal data when providing services.

- Instances were identified where the security of young people's data was inadequately protected, leading to significant risks of improper processing. For instance, employees of the data controller utilized a shared username and password to access electronic systems used for processing youth data. Furthermore, depending on the functions and responsibilities of certain employees, it was unclear why they required access to complete and/or specific types of youth data. These circumstances, coupled with the broad range of individuals authorized to access the data, heightened the risks of illegal data processing and their utilization for non-business purposes.

- In certain instances, information pertaining to professional activities was processed through employees' personal systems, such as personal computers and email accounts. This practice poses risks from a data security standpoint. The data controller lacks control over these systems, consequently lacking an effective means to implement adequate organizational and technical measures to mitigate data risks and protect the processed data. Moreover, in the event of termination of the employment relationship with the respective employee, there is a significant risk that data will continue to be stored in these systems, potentially allowing unauthorized access by former employees of the data controller.

Data Processing within the Framework of Other Topics

Various violations and deficiencies are also noted in the processes of data processing by both public and private organizations across different fields:

— In specific instances, data controllers formed large-scale databases and obtained data without the subject's consent. Additionally, they lacked any other legal basis for data processing, which is a crucial requirement for ensuring the lawfulness of data processing.

— As a result of the study of various data processing processes, individual cases of data processing with a disproportionate volume were also identified. In addition, data controllers could not specify the period for which they needed to store data, which created risks of violating data protection principles;

— In numerous instances, electronic programs utilized by public institutions lacked adequate security measures. This limitation restricted access to the processed data for individuals who did not require it to fulfill their duties. Additionally, unauthorized persons, including former employees, were able to access data through the electronic system.

— Instances of physical data security breaches were also uncovered. For instance, one public institution stored documentation in physical form on a shelf in a room where employees other than the authorized personnel also worked. Another public institution stored a significant portion of its material documentation on the floor, posing risks of accidental or unauthorized data processing in various forms.

4.2 Instructions and Recommendations

The cases systematically examined by the Personal Data Protection Service, along with the implemented measures, highlight violations of the requirements stipulated by the Law of Georgia "On Personal Data Protection" (hereinafter referred to as "the Law") in the data processing procedures of various public and private organizations. Additionally, to align the data processing procedures scrutinized by the Service with the aforementioned law, the Service issued numerous recommendations and mandatory instructions. Consequently, individuals involved in the data processing process should take heed of the following issues, considering the recommendations issued by the Service and the analysis of instructions:

— It's crucial for data controllers to process personal data in accordance with the legal basis(es) provided by the law. Within the relevant data processing process, considering the legal purposes and the necessity for data retention, it's imperative to establish in advance the storage terms for personal data and ensure that data older than the relevant term is either blocked, deleted, destroyed, or stored in a manner that prevents the identification of individuals. Furthermore, to adhere to the principles outlined by the law, including the timely and secure deletion of unnecessary data after achieving the relevant purpose, it's essential for the data controller to implement automatic deletion mechanisms instead of manually deleting data. This, in turn, helps prevent illegal data processing or unauthorized access;
— Recruiting organizations should assess the duration for which it is essential and justified to retain the data of job seekers in order to fulfill the relevant legal objectives. They should ensure the deletion of this data after the specified period has elapsed and the relevant objectives have been achieved;
— It's crucial for both public and private institutions to adhere to the requirements of the law when processing data for recording the entry and exit of employees from buildings. They should only collect data of a permitted and proportional volume for this purpose;
— Employing organizations should establish a procedure for requesting information on corporate telephone numbers owned by employees, ensuring that this information remains confidential and inaccessible to the employer;
— Before commencing data processing, data controllers must evaluate whether the planned processing procedure guarantees the authenticity and accuracy of the data (for example, whether the data will be obtained from a reliable source, whether it will be updated with reasonable periodicity, etc.);

— When processing a specific type of information solely for the purpose of generating statistics, such information must be processed in a manner that prevents the identification of individuals. Specifically, measures should be taken to ensure that the identity of specific data subjects cannot be discerned;
— Every institution that collects data from a data subject must furnish them with comprehensive information regarding the processing of their data. This includes details such as the name and registered address of the data controller and the data processor, the purpose of data processing, whether the provision of data is mandatory or voluntary, etc;
— To ensure the secure processing of data, it's crucial to utilize electronic means that enable the data controller to implement adequate organizational and technical data protection measures whenever necessary. Additionally, these means should prevent former employees (unauthorized individuals) from accessing the data after the termination of the employment relationship;
— It's essential that each individual with the right to access the data only does so through a user account secured by a complex password. Moreover, devices containing data, such as memory cards, external hard drives, etc., should be safeguarded with a complex password as well;
— Data controllers must ensure comprehensive logging and regular monitoring of actions taken with electronic data, as this serves as an effective measure to prevent illegal data processing. Furthermore, it's important to automatically record actions taken with electronic data because manual recording using human resources poses a high risk of incomplete or incorrect indication of information;
— Access to personal data should be limited to those employees of the data controller who do not require mentioned access in the performance of their duties. Among them, appropriate mechanisms should be implemented to restrict employees' access to data that, under the circumstances, are no longer relevant for the performance of the functions assigned to them. (For instance, some administrative and academic staff may no longer require access to the data of pupils and students who do not have an active status). Additionally, access to data should be revoked for former employees upon termination of their employment;
— Following an analysis of the circumstances and risks associated with data processing, suitable measures should be developed to guarantee the physical security of data. For instance, the area designated for data processing should be designed to prevent access by unauthorized individuals. Data should be stored in secure locations such as locked cabinets or other secure facilities where unauthorized access is not possible;
— In the contract signed with the authorized person, detailed consideration should be given to the obligations of the authorized individual. Similarly, the authorized person must ensure the meticulous fulfillment of the obligations outlined in the contract.
— When transferring data internationally, organizations should evaluate whether the receiving state is listed as approved by the order of the President of the Service. If not listed, organizations should seek permission from the Service to proceed with the transfer.

II

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

Chapter II. Monitoring of the Covert Investigative Actions and the Activities Carried Out at the Central Databank of the Electronic Communication Identification Data

According to Article 40[16] of the Law of Georgia "On Personal Data Protection," the Personal Data Protection Service oversees the execution of covert investigative actions and activities conducted within the Central Databank of Electronic Communication Identification Data.

To oversee covert investigative actions, the Service utilizes electronic monitoring and specialized electronic control systems, which currently has insight into the ongoing covert investigative actions, including covert surveillance, recording of telephone communications, and real-time determination of geolocation. Additionally, the Personal Data Protection Service is provided with physical copies of documents related to the implementation of covert investigative actions, such as court rulings and prosecutor's decrees, 24 hours a day. These physical copies are compared with the electronic documentation submitted by the LEPL "Operative-Technical Agency of Georgia" through electronic control systems.

In addition to covert investigative actions such as secret monitoring and recording of telephone communications and real-time determination of geolocation, other covert investigative actions, depending on their nature, may not be conducted through electronic control systems. Therefore, electronic copies of court rulings and prosecutor's resolutions will not be submitted to the Service in such cases. Instead, the bodies conducting the covert investigative actions are required to provide the Service with physical documentation regarding permission to carry out the action.

Within the scope of controlling covert investigative actions, including secret monitoring and recording of telephone communications, and real-time determination of geolocation, the Personal Data Protection Service is authorized to suspend the initiated covert investigative action if:

- If, upon the initiation of covert investigative action of telephone communication, the electronic copy of the judge's ruling authorizing the commencement of the operation, containing only the requisites of the ruling and the resolution part, was not electronically submitted to the Service by the LEPL "Operative-Technical Agency of Georgia";
- The material copy of the ruling issued by the court was not submitted to the Service within 48 hours of its issuance;
- Within 12 hours after the start of the secret monitoring and recording of telephone communication, the prosecutor's resolution issued due to urgent necessity was not submitted;
- The requisites and/or the resolution part of the prosecutor's resolution submitted through the electronic system or in material (documentary) form contain ambiguity and inaccuracy;
- The data in the requisites and resolution part of the electronic copy of the prosecutor's resolution submitted through the electronic system do not match the data in the requisites and resolution part of the prosecutor's resolution submitted in material (documentary) form;

The suspended covert investigative action resumes only once the error is resolved. LEPL "Operative-Technical Agency of Georgia", the court, and the prosecutor or the authorized representative of the relevant investigative body, within their respective jurisdictions, are required to submit physical and electronic copies of the court ruling or the prosecutor's resolution to provide proof of elimination

of the grounds for suspending covert investigative action to the Service. Upon receiving the necessary documentation, the Service will programmatically acknowledge receipt, and the covert investigative action will resume.

Furthermore, if the reason for its suspension is not rectified within 3 days after the suspension of the covert investigation, the material obtained as a result of the covert investigation is destroyed in accordance with the procedure established by the Criminal Procedure Code of Georgia.

In case of ambiguity or inaccuracy, the Personal Data Protection Service is empowered to suspend the covert investigative action if the flaw is related to the prosecutor's resolution. 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 legislation does not allow for the suspension of the action, Nevertheless, concerning the defect, 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 receiving information about the error, the prosecutor is obligated to submit in a written form to the court that issued the ruling. The court must, within 12 hours of receiving the appeal, rectify the ambiguity or inaccuracy in the judge's ruling and provide the corrected ruling to the Personal Data Protection Service within 24 hours after resolving the ambiguity or inaccuracy.

In addition to the aforementioned, the Service's oversight of covert investigative actions entails the obligation of relevant bodies to furnish the Service with a protocol upon the completion of the covert investigative action. This protocol must clearly delineate the legal basis for conducting the covert investigative action, the time of its initiation and completion, the location for creating the protocol, the type of covert investigative action conducted, the technical means employed during its execution, the location where the covert investigative action took place, the subject of the covert investigative action, and if any covert investigative action specified in subparagraphs "a"-"g" of the first part of Article 143^1 of the Criminal Procedure Code of Georgia was carried out, the technical identifier of the object of the covert investigative action must also be provided.

Criminal Procedure Code of Georgia stipulates the destruction of information/material obtained as a result of covert investigative action. According to the first part of Article 143^8 of the same Code, information obtained as a result of covert investigative action, as determined by the prosecutor, must be immediately destroyed after the termination or completion of the covert investigative action if it holds no value for the investigation. Additionally, in accordance with Article 143^8, Part 5, concerning the destruction of material obtained as a result of covert investigative action, the bodies conducting the covert investigative action are also required to submit the relevant protocol to the Service.

Furthermore, it's important to emphasize that within the framework of the investigation, the relevance of material obtained as a result of covert investigative action to the case is determined by the prosecutor overseeing the case. Additionally, the legality of obtaining the aforementioned material and its relevance to the case are assessed by the court, which renders a decision on its admissibility or inadmissibility as evidence. In the event of the material being deemed inadmissible, it will be destroyed in accordance with the Criminal Procedure Code of Georgia.

1. Information Request

In addition to covert investigative actions, the authority of the Service encompasses the supervision of investigative activities outlined in Articles 136-138 of the Criminal Procedure Code of Georgia. Specifically, these articles pertain to the retrieval of significant information or documentation for criminal cases from computer systems or computer data storage mediums, the continuous collection of internet traffic data, and the acquisition of content data.

It's noteworthy that representatives of law enforcement agencies have the authority to request electronic communication identification data from both electronic communication companies and from the central bank of electronic communication identification of the LEPL "Operative-Technical Agency of Georgia", where in accordance with the law of Georgia "on electronic communications" and the Legal Entity under Public Law – "Operative-Technical Agency of Georgia," are collected databases of electronic communication identification data copied from various electronic communications companies.

To regulate this process, Article 20 of the Law of Georgia "On Personal Data Protection" imposes an obligation to notify the Personal Data Protection Service. Specifically, electronic communication companies are mandated to transfer electronic communication identification data to law enforcement bodies. Within 24 hours after transferring this data, the information should be submitted to the Personal Data Protection Service. Moreover, the Service has real-time access to activities conducted in the central bank of electronic communication identification data, enabling it to identify the data processed by the LEPL "Operative-Technical Agency of Georgia" without the need for additional notification.

It's important to note that prior to the implementation of changes in the Criminal Procedure Code of Georgia in 2022, the obligation to present the rulings issued on requests for information to the Service was also incumbent upon the general courts. This arrangement provided an opportunity to compare the information provided by the courts and electronic communications companies, enabling the identification of potential gaps. However, in the present scenario, only process inspection serves as an effective mechanism for controlling this issue.

The Personal Data Protection Service conducts inspections of investigative bodies, as well as the LEPL "Operative-Technical Agency of Georgia", within the framework of controlling covert investigative actions, both based on citizens' appeals and on its own initiative, to examine the lawfulness of data processing. If a violation is uncovered during the examination of data processing lawfulness, the Service imposes administrative penalties on the violator. Moreover, to rectify identified violations, the Service is authorized to issue mandatory instructions and recommendations to address shortcomings. Furthermore, if indications of a crime are discovered during the inspection, the Personal Data Protection Service is obligated to notify the appropriate investigative body for further action.

2. Important Directions and Trends

Considering the sensitivity and public interest surrounding the issue, the Service annually plans and conducts comprehensive inspections to safeguard the rights of data subjects within the scope of covert investigative actions. These inspections also ensure proper enforcement of legal obligations by relevant individuals. In 2023, the Service conducted 8 inspections across various agencies, addressing diverse issues. These inspections involved oversight of covert investigative actions as well as the study of the issue of compliance with the obligation by law enforcement agencies and electronic communication companies.

During the conducted inspections, the Service identified 7 instances of law violation and issued 9 mandatory instructions for execution, of which 3 have been completed, while the deadline for the remaining 6 has not yet elapsed.

In 2023, the Personal Data Protection Service received complaints from 4 citizens concerning covert investigative actions taken towards them.

In 2022, the Personal Data Protection Service conducted a study at the LEPL "Operative-Technical Agency of Georgia" regarding the utilization of real-time stationary technical capabilities for obtaining communication data during the implementation of covert investigative actions, specifically focusing on "secret monitoring and recording of telephone communication" as delineated in subparagraph "a" of the first part of Article 143[1] of the Criminal Procedure Code of Georgia. The study aimed to address data security concerns related to this matter.

Within the framework of planned inspections in 2023, the Service incorporated materials obtained by the agency as a result of implementing covert investigative action- specifically, "covert video recording and/or audio recording, photography" as defined by subparagraph "e" of the first part of Article 143[1] of the Criminal Procedure Code of Georgia. During the process of transferring materials to the initiator through a special electronic control system for data processing and real-time determination of geolocation, the initiator of the notification, conducted in the Public Safety Command Center "112", a legal entity of public law operating under the Ministry of Internal Affairs of Georgia, mobile communication equipment was utilized. Issues regarding the fulfillment of obligations to provide real-time logging data for determining geolocation in automatic mode to the Personal Data Protection Service were addressed[1].

Additionally, during the reporting period, the planned inspection initiated in 2022 was concluded. This inspection focused on examining the duration of data retention in the central bank of electronic communication identification data by the agency, as well as assessing the proportionality of data provided after receiving relevant requests.

Furthermore, a planned inspection was identified within the Special Investigation Service to investigate the obligation to submit protocols on the completion of covert investigative actions to the Personal Data Protection Service.

Furthermore, to comprehensively address the scope of the mandate and ensure effective control, a systematic examination was conducted regarding the compliance of the electronic communication company, "Magticom" LLC, with the obligation to notify the Service on the transfer of electronic communication identification data to law enforcement bodies, as stipulated by the procedure outlined in Article 136 of the Criminal Procedure Code of Georgia.

1 Checking on progress.

3. Instructions and Recommendations

While conducting covert investigative actions, law enforcement authorities must adhere to the obligations outlined in Criminal Code of Georgia and uphold the principles of data minimization and proportionality. Together with that, considering the outcomes of the conducted inspections, it is crucial to only process data for which there exists a legitimate purpose. Furthermore, electronic communications companies should only provide the specific type of data to the agency as mandated by law.

To effectively oversee covert investigative actions, it is imperative to adhere to the obligations outlined in the Criminal Procedure Code of Georgia. Law enforcement agencies must take appropriate measures to ensure they can promptly submit reports of completed covert investigations to the Service.

The conducted inspections have once again highlighted that the absence of proactive provision of information on court rulings, or incomplete provision thereof to the Service, creates a significant obstacle in terms of timely identification of possible violations of the law. It should be emphasized that information on court rulings offers an opportunity to verify the legality and proportionality of information provided by electronic communications companies and activities conducted within the Central Bank of Electronic Communication Identification Data.

The Personal Data Protection Service pays special attention to the control of covert investigative actions. Consequently, in 2024, planned inspections in this process will be actively continued.

4. Statistical Data

THE COURT RULINGS REGARDING COVERT WIRETAPPING AND RECORDING OF THE TELEPHONE COMMUNICATIONS

TOTAL NUMBER	859
APPROVED	744
NOT APPROVED	80
PARTIALLY APPROVED	35

In 2023, the court reviewed 859 motions for wiretapping and recording of telephone communications. Among these, 87% (744) were fully approved, 9% (80) were not approved, and 4% (35) were partially approved.

In 2022, from March 1 to December, inclusive, the court deliberated on 1,077 motions concerning secret monitoring and recording of telephone communications. Of these, 75% (808) were fully approved, 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

TOTAL NUMBER	228
APPROVED	198
NOT APPROVED	8
PARTIALLY APPROVED	22

In 2023, the court reviewed 228 motions for extending the period of secret monitoring and recording of telephone communications. Among these, 87% (198) were approved, 4% (8) were not approved, and 9% (22) were partially approved.

In 2022, the court deliberated on 288 motions for extending the period of secret surveillance and recording of telephone communications. Of these, 71% (204) were approved, 8% (23) were not approved, and 21% (61) were partially approved.

THE COURT RULINGS REGARDING THE COVERT VIDEO AND/OR AUDIO RECORDING, PHOTOGRAPHING

TOTAL NUMBER	1022
APPROVED	952
NOT APPROVED	66
PARTIALLY APPROVED	4

In 2023, the court reviewed 1,022 motions concerning covert video recording and/or audio recording, photography. Among these, 93% (952) were fully approved, 6.5% (66) were not approved, and 0.4% (4) were partially approved.

In 2022, the court considered 888 motions regarding covert video recording and/or audio recording, photography. Of these, 91% (811) were fully approved, 8% (68) were not approved, and 1% (9) were partially approved.

THE COURT RULINGS REGARDING EXTENSION OF TERM OF COVERT VIDEO AND/OR AUDIO RECORDING, PHOTOGRAPHING

TOTAL NUMBER	122
APPROVED	105
NOT APPROVED	15
PARTIALLY APPROVED	2

In 2023, the court reviewed 122 motions for extending the period of covert video recording and/or audio recording, photography. Among these, 86% (105) were approved, 12% (15) were not approved, and 2% (2) were partially approved.

In 2022, the court considered 186 motions for extending the period of covert video recording and/or audio recording, photographing. Of these, 77% (144) were approved, and 23% (42) were not approved.

PROSECUTOR'S DECREES SUBMITTED TO THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

TOTAL NUMBER	126
COVERT VIDEO RECORDING AND/OR AUDIO RECORDING, PHOTOGRAPHY	76
COVERT MONITORING AND RECORDING OF TELEPHONE COMMUNICATIONS	16
REQUESTS FOR DOCUMENTS OR INFORMATION	34

In 2023, 126 prosecutor's decrees were submitted to the Service authorizing covert investigative actions deemed urgently necessary. Among these, 60% (76) pertained to covert video recording and/or audio recording, photography, 13% (16) involved covert monitoring and recording of telephone communications, and 27% (34) related to requests for investigative actions, documents, or information as provided for in Article 136 of the Criminal Procedure Code of Georgia.

In 2022, out of the 150 resolutions entered, 66% (99) were associated with covert video recording and/or audio recording, photography, while 34% (51) were related to covert monitoring and recording of telephone communications.

COURT RULINGS SUBMITTED TO THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

TOTAL NUMBER	1519
APPROVED	1518
NOT APPROVED	1

Court rulings and prosecutor's orders, with the latter being based on urgent necessity, are submitted to the Personal Data Protection Service regarding requests for investigative actions, documents, or information as provided for in Article 136 of the Criminal Procedure Code. Throughout the reporting period, 1519 court rulings were submitted to the Service regarding Article 136 of the Code, with 99% of the prosecutor's petitions being approved.

In 2022, a total of 3575 court decisions were submitted to the Service in connection with Article 136 of the Code, with 99% of the prosecutor's petitions being approved.

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

34

In 2023, 34 decrees under urgent necessity issued by the prosecutor were submitted to the Personal Data Protection Service concerning investigative actions, document, or information requests as specified in Article 136 of the Criminal Procedure Code. In 2022, the Service received 45 decrees from the prosecutor under similar urgent circumstances.

USING THE SUSPENSION MECHANISM

TOTAL NUMBER	76
FAILURE TO SUBMIT THE COURT JUDGMENT ON TIME	74
RECOGNITION OF COVERT INVESTIGATIVE ACTIONS AS UNLAWFUL	1
TERMINATION OF COVERT INVESTIGATIVE ACTIONS	1

During the reporting period, the Service utilized the mechanism of halting covert monitoring-recording of telephone communications (via the electronic control system) in 76 instances. Primarily due failure to submit the court judgment on time (74 cases), one case involved the court recognizing the secret investigative action initiated based on the prosecutor's resolution due to urgent necessity as unlawful, while another case stemmed from termination of the covert investigative action itself [2].

In 2022, the Personal Data Protection Service employed the suspension mechanism in 176 cases.

2 The resolution of the prosecutor on the termination of the covert investigative actions was provided to the Service before submission to the LEPL "Operative-Technical Agency of Georgia". Consequently, until the agency received the information and terminated the investigative action, the Service halted the secret monitoring and recording of telephone communication.

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

6

In 2023, LEPL "Operative-Technical Agency of Georgia" was informed by the court regarding ambiguity and inaccuracy in permits issued for covert monitoring and recording of telephone communication (via the electronic control system) on 6 occasions. In 2022, the Service utilized the ambiguity-inaccuracy reporting mechanism 14 times.

ACTIVITIES IDENTIFIED IN THE CENTRAL DATABANK FOR ELECTRONIC COMMUNICATIONS IDENTIFICATION DATA

69

In 2023, based on the information provided to the service through the Central Bank's electronic control system of identification data of electronic communication, the data from the Central Bank of Electronic Communication Identification Data was issued by LEPL "Operative-Technical Agency of Georgia" 69 times based on relevant court decisions.

In 2022, the LEPL "Operative-Technical Agency of Georgia" issued data from the Central Bank of Electronic Communication Identification Data 79 times based on relevant court decisions.

NOTIFICATIONS SUBMITTED BY ELECTRONIC COMMUNICATIONS COMPANIES

1756

- ***In 2023, 11 electronic communication companies submitted notifications to the Service, indicating that they provided information to law enforcement authorities based on 1756 court rulings during the reporting period.***

- ***In 2022, 15 electronic communication companies submitted information, stating that they provided information to law enforcement officials based on 2405 court orders during the reporting period.***

CITIZENS' APPLICATIONS REGARDING COVERT INVESTIGATIVE ACTIONS CARRIED OUT TOWARDS THEM

4

- ***In 2023, a total of 4 individuals contacted the Personal Data Protection Service to inquire whether secret investigative actions were being conducted towards them.***

- ***In 2022, the Personal Data Protection Service received applications from 93 individuals.***

THE NUMBER OF COURT RULINGS REGARDING COVERT INVESTIGATIVE ACTION FOR THE REMOVAL AND FIXING OF INFORMATION FROM COMMUNICATION CHANNELS, COMPUTER SYSTEM

TOTAL NUMBER	3
APPROVED	1
NOT APPROVED	2

During the reporting period, the court considered 3 motions regarding the secret investigative action of communication channels, concerning the removal and fixation of information from the computer system. One of these motions was granted, while two were denied.

COURT RULINGS ON THE ONGOING COLLECTION OF INTERNET TRAFFIC DATA

1

During the reporting period, the court reviewed 1 motion concerning the ongoing collection of Internet traffic data, which was approved.

III

ACTIVITIES RELATED TO THE IMPLEMENTATION OF THE NEW LAW "ON PERSONAL DATA PROTECTION"

CHAPTER III. ACTIVITIES RELATED TO THE IMPLEMENTATION OF THE NEW LAW "ON PERSONAL DATA PROTECTION"

Harmonizing the legal framework for personal data protection with European legislation is an obligation Georgia has assumed under the Association Agreement with the European Union and the Association Agenda. In 2016, the European Parliament and the Council adopted the "General Data Protection Regulation" (GDPR), which took effect in 2018. The GDPR set forth novel standards for personal data protection, introducing crucial concepts and institutions to align with modern technological advancements. For Georgia, a country progressing towards European legal culture and integration, harmonizing its legislation on personal data protection with EU laws is paramount and accordingly, the implementation of new democratic standards at the national level will ensure the effective protection of human rights and freedoms, including privacy, in the processing of personal data. Additionally, the independent data protection supervisory body will be equipped with appropriate mechanisms and powers to uphold these standards.

In recent years, the standard of personal data protection, both in legislation and in practice, has notably improved. Nonetheless, challenges persist in both private and public sectors. To address these challenges and rectify deficiencies at the legislative level, while reinforcing standards and guarantees for personal data protection and privacy, a new law on personal data protection was developed. This law was adopted by the Parliament on June 14, 2023, with its main provisions coming into effect on March 1, 2024.

To achieve the stated objectives, the law placed significant emphasis on empowering the independent data protection supervisory body with suitable mechanisms and powers concerning both the public and private sectors. Consequently, transparency and accountability within the personal data supervisory authority have heightened, rendering legislation in the domain of personal data protection more foreseeable and robust. Moreover, sustainable and effective mechanisms for personal data protection, centered on safeguarding human rights, have been devised. Crucially, the legislation has drawn significantly nearer to European standards and facilitated Georgia's fulfillment of international obligations, thereby fostering the establishment of internationally recognized principles and best practices.

Strategic Action Plan for the Implementation of the New Law

To proficiently oversee the implementation processes of the new law, the Service has devised a strategy and action plan for executing the new law of Georgia "On Personal Data Protection." This comprehensive plan encompasses the Service's tasks, activities, performance indicators, responsible or supporting structural units for the activities, and deadlines for task completion or individual activities.

During the implementation of the new law, the Personal Data Protection Service organized and executed several significant external and local events aimed at enhancing public awareness of personal data protection issues. These initiatives included sectoral meetings with various major data controllers in both the public and private sectors.

As part of the action plan for implementing the new law, the following activities and events focused on raising public awareness were conducted:

Awareness Campaign for the New Law "On Personal Data Protection"

In the second half of 2023, the Service actively started an information campaign in order to inform the public, representatives of the public and private sector, and various target groups of the obligations and legislative news provided by the new law. The information campaign included both face-to-face meetings and various activities in social networks and media.

"Conversations on the New Law"

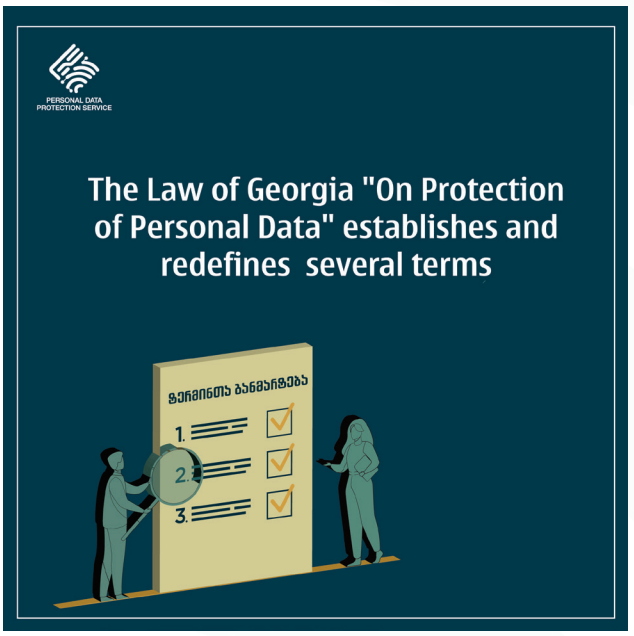
To inform the public and target groups about the new law, a series of meetings titled "Conversations on the new law" was initiated. As part of this campaign, 20 meetings were scheduled and conducted with the target audience to discuss the changes introduced by the new law "On Personal Data Protection."

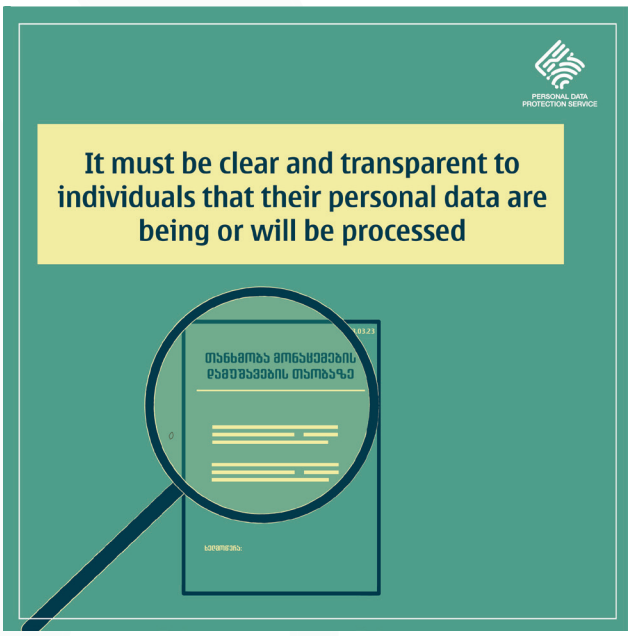
Consultations on the New Law

The Service introduced a new format of individual consultations every Friday at its office for those interested in the changes outlined in the new law. Anyone who wishes has the opportunity to receive consultations from the Service's representatives regarding the new law "On Personal Data Protection" within the framework of face-to-face meetings. This project will be actively sustained in 2024. To facilitate free participation in these events, the Service's social media platforms actively disseminate registration links. Any citizen can access information about the planned events and attend them if they wish.

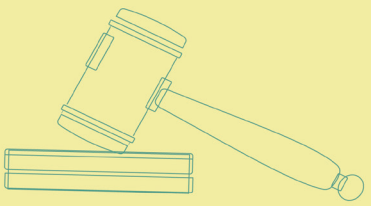
Online Campaign "#newlaw"

To inform the public about the changes introduced by the new law, the Service initiated an active campaign on social networks. Specifically, information cards were created to offer interested individuals information about the law changes in a language they could easily comprehend. These informational illustrated cards with relevant explanations were progressively shared on the Facebook and LinkedIn pages of the Service. In total, they reached approximately 56,000 users.





Under the new law, the grounds for processing personal data has been expanded and redefined



Data processing for direct marketing purposes will only be allowed with the consent of the data subject

The new law envisages the obligation to carry out a data protection impact assessment

Data subjects have a right to data portability under the new law

New principles for the processing of personal data:

Transparency, erasure/destruction, technical and organisational measures

IV

INTERNATIONAL COOPERATION

CHAPTER IV. INTERNATIONAL COOPERATION

On the path of European integration, the Service has played an active role in fulfilling the instructions necessary to secure EU membership candidate status for Georgia. This involves aligning national personal data protection legislation with international legal instruments and implementing best practices from Europe. Since its inception, one of the Service's strategic development priorities has been fostering deeper international relations and participating in sectoral international platforms. The Service maintains cooperation with relevant institutions of the European Union involved in personal data protection, foreign counterparts' supervisory bodies for personal data protection, and international organizations.

During the reporting period, the Service undertook several initiatives to enhance international cooperation. Additionally, it actively researched international industry trends and issued advisory publications in line with international standards of personal data protection.

1. Obtaining the Observer Status of the Activities of the "European Data Protection Board" ("EDPB") and Cooperation with the "European Data Protection Supervisor" ("EDPS") Institution

In 2023, the Personal Data Protection Service attained observer status of the "European Data Protection Board" ("EDPB"). The "European Data Protection Board", an EU entity, was established under Article 68 of the EU General Data Protection Regulation ("GDPR"). Since May 25, 2018, it has served as the legal successor to the Article 29 Working Group of Directive No. 95/46/EC of the European Parliament and the Council of October 24, 1995, "Concerning the Protection of the Rights of Natural Persons in Connection with the Processing of Personal Data and the Free Movement of Said Data". It consists of representatives of the data protection supervisory authority of each EU member state, the European Commission and the "European Data Protection Supervisor" ("EDPS"). Additionally, the European Commission retains the right to participate in its activities. The Council plays a crucial role in ensuring the efficacy of personal data protection regulations throughout the EU and in establishing consistent, uniform, and best practices for data protection supervisory authorities. Specifically, it makes decisions with binding legal force, publishes opinions, consults the European Commission on any issue of personal data protection in the European Union, and develops guidelines and recommendations.

The Council decided to confer observer status upon the Personal Data Protection Service, considering several criteria outlined in its Regulation ("RoP") 8.1, which was adopted based on the relevant article. According to this article, the Council may, upon receiving a corresponding request, grant observer status to a data protection supervisory authority of a non-member state of the European Union if it is deemed to be in the Council's interest and if two cumulative conditions are met: the data

protection supervisory authority of the non-member state of the European Union operates with complete independence. The data protection supervisory authority is based in a non-member state that, in its pursuit to join the European Union, has committed to fully aligning its national data protection legislation with the regulatory rules applicable in the European Union. Consequently, starting from June 2023, the President of the Personal Data Protection Service participates in the plenary sessions of the "European Data Protection Council" and represents the Service as a data protection supervisory body with observer status in the activities of the Council.

The Service has further strengthened its collaboration with the European Data Protection Supervisor ("EDPS"), exploring the potential for a long-term secondment of an Employee of the Personal Data Protection Service to the supervisory authority in the Kingdom of Belgium. This represents an unprecedented form of cooperation and underscores the robust backing of European counterparts for the Georgian Personal Data Protection Supervisory Authority. The "European Data Protection Supervisor" oversees the implementation of the provisions of the "General Data Protection Regulation" ("GDPR") in the member states of the European Union. Its primary function is to supervise the processing of personal data by the institutions and bodies of the European Union. Starting from 2024, the Personal Data Protection Service will appoint a representative to the "European Data Protection Supervisor" institution. During the visit, the representative of the Personal Data Protection Service of Georgia, Nikoloz Popiashvili, who serves as the Head of the Office of the President, will have the opportunity to familiarize themselves with the best practices of the European Data Protection Supervisor in the realm of data protection and privacy. Additionally, he will participate in the plenary meetings of the "European Data Protection Board" ("EDPB") and various activities organized by the Secretary General, including events commemorating the 20th anniversary of the European Data Protection Supervisor. The outlined cooperation format entails the support of the Personal Data Protection Service in implementing the new law "On Personal Data Protection," participation in research activities related to EU regulations on artificial intelligence, and engagement in various initiatives aimed at sharing experience in the field of personal data protection. Regarding the substance of this cooperation and the support provided to the Personal Data Protection Service of the "European Data Protection Supervisor" ("EDPS") on the path to European integration, the President of the Service convened a working meeting with the Secretary-General of the European Data Protection Supervisor, Leonardo Cervera Navas, in Brussels in December 2023.

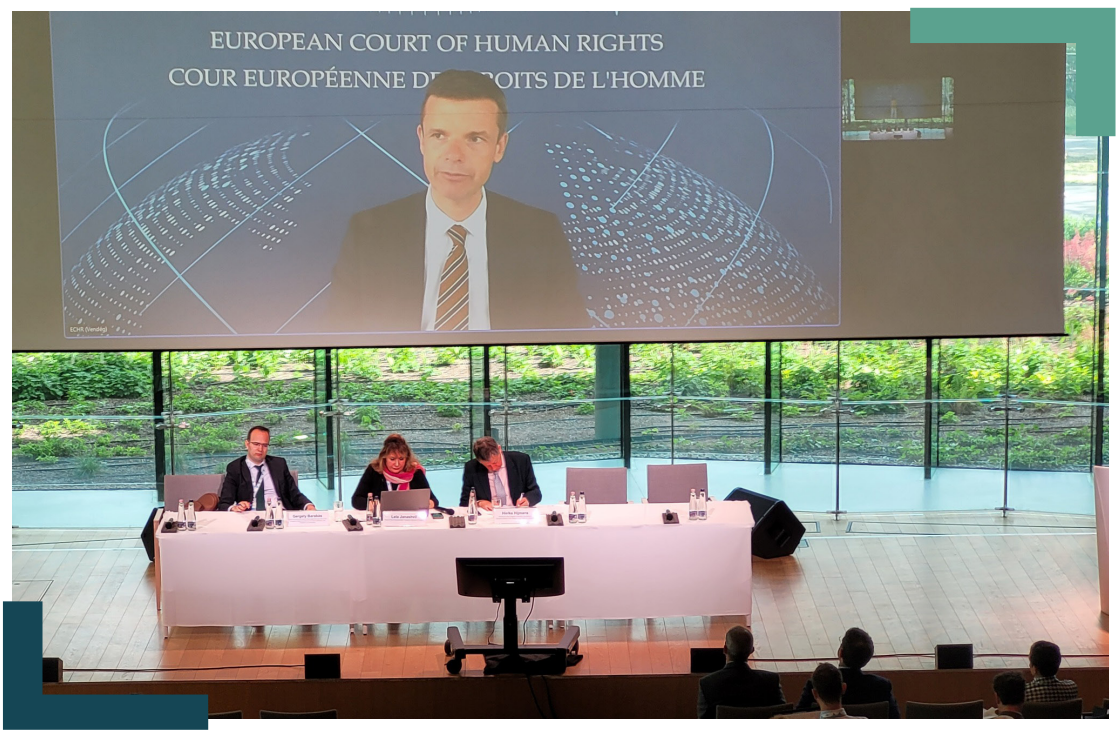
2. Representation of the Service in International Sectoral Institutions and Networks

During the reporting period, the Service took an active part in various international forums focused on personal data protection and privacy. Specifically, the President of the Service and their first deputy attended the 44th and 45th plenary sessions of the Consultative Committee ("T-PD") of the Council of Europe Convention (108th Convention) on the "Protection of Individuals with regard to Automatic Processing of Personal Data". The Service actively engages in the committee's activities and, upon request, periodically submits reports on national legislation and the activities conducted by the Data Protection Supervisory Authority of Georgia.

President of the Personal Data Protection Service of Georgia, Lela Janashvili, participated in and presented a report at the annual international conference, "Privacy Symposium," hosted by Ca'Foscari University of Venice, Italy, in 2023. One of the conference panels focused on promoting cooperation among non-member personal data protection supervisory bodies of the European Data Protection Board ("EDPB"). During this panel, President of the Service discussed the mandate of the Georgian personal data protection supervisory body, national legislation, and the Law of Georgia "On Personal Data Protection." They also highlighted the Service's international relations and emphasized the significance of a bilingual, scientific periodical publication with an international editorial board established by the Service- the "Journal of Personal Data Protection Law."

As a member of the "European Conference of Data Protection Authorities," the Service is an accredited member of the "Spring Conference". It participated in the 31st conference of 2023 hosted by the Hungarian Personal Data Protection Supervisory Authority. Notably, the President of the Service moderated a panel during the closed session of the conference focusing on the practices of the European Court of Human Rights ("ECHR") and the Court of Justice of the European Union ("CJEU") regarding personal data protection.

During one of the panels of the “Spring Conference,” the focus was on summarizing the activities of the conference working group from the previous term, providing an overview of the 2022 European Proceedings Workshop, and announcing the next host agency of the conference. Within this panel, the head of the Department of International Relations, Analytics, and Strategic Development of the Service delivered a report. They introduced the contents of the European Proceedings Workshop held in Tbilisi and shared the results of the satisfaction survey conducted among the participants of the event. As part of the report, both the Georgian and English editions of the “Journal of Personal Data Protection Law” were presented to underscore the Service’s role in the development of personal data protection law.



In 2023, the new composition of the “Steering Group” of the “European Conference of Data Protection Authorities” was selected. Following the conference regulations and considering the election results for the selection of regular members of the working group, the new composition includes the Personal Data Protection Service, along with data protection supervisory authorities of Bulgaria, the United Kingdom, and Cyprus. Additionally, based on the consensus of the newly recruited working group members, the Personal Data Protection Service of Georgia will serve as the coordinator of the working group.

Employees of the Personal Data Protection Service took part in the “European Case Handling Workshop (ECHW)” hosted by the Swiss Data Protection Supervisory Authority in 2023. During the event, the Service’s employees provided participants with insights into the new law “On Personal Data Protection” and shared the practices of the Georgian Personal Data Protection Supervisory Authority on various thematic issues.

During the reporting period, the agency actively participated in the activities of the “Global Privacy Assembly” (“GPA”). The President of the Service moderated a closed session panel on Privacy Trends: Steps Forward at the 45th Assembly Meeting in Hamilton, Bermuda. This panel provided an

overview of the latest news, challenges, and main trends in the field of personal data protection and privacy. Additionally, at the 45th meeting of the Assembly, the Personal Data Protection Service, serving as the co-chair of the "Working Group on Data Protection Metrics," submitted an annual report on the activities of the working group. It's noteworthy that in 2023, the Service became a member of another working group within the Assembly, titled "The Role of Personal Data Protection in International Development Aid, International Humanitarian Aid, and Crisis Management"[3] which encompassed topics related to the new law "On Personal Data Protection," the issue of obtaining the status of an observer of the activities of the "European Data Protection Board" ("EDPB") by the Service, and various activities of the Personal Data Protection Service.

In 2023, the Service took part in the International Working Group on Data Protection in Technology in the 71st meeting of the so called "Berlin Working Group," hosted by the Italian Data Protection Authority ("Garante Per La Protezione Dei Dati Personali"). During this meeting, the head of the Service briefed the members of the working group on significant developments in the field of personal data protection law in Georgia, legislative changes, and the Service's international activities.

3 See The Global Privacy Assembly ("GPA") Official Website.

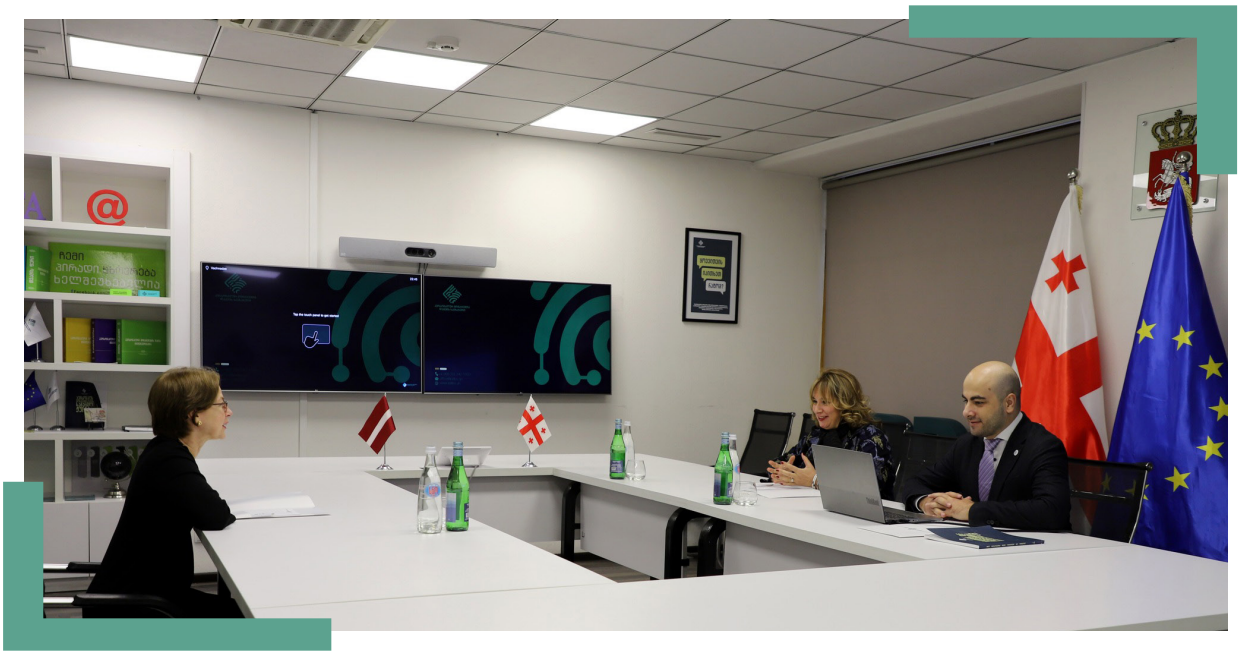
In 2023, The first deputy President of the Personal Data Protection Service, Otar Chakhunashvili, represented the Personal Data Protection Service at an international symposium organized by the German Federal Commissioner for Data Protection and Freedom of Information, titled “Portals, Registers, Platforms - Digital and Transparent?”. During the symposium, representatives from European data protection supervisory authorities and international experts deliberated on the dissemination of personal information in the online sphere, open data platforms, registers, and portals. Concurrently, to bolster future cooperation between the agencies, the first deputy head of the Service held a meeting with Dagmar Hartge, Brandenburg’s State Commissioner for data protection and access to information.

In collaboration with the “Institute of Transparency, Public Information and Protection of Personal Data” (“ITEI”) of the State of Jalisco, Mexico, alongside The “National Institute for Transparency, Access to Information and Personal Data Protection” (“INAI”) of Mexico, as well as upon the invitation of the Personal Data Protection and the “National Transparency System” (“SNT’) “Personal Data Protection Commission” (“CPDP”), the head of the Department of International Relations, Analytics, and Strategic Development of the Personal Data Protection Service participated in the hybrid-format conference titled “The route of Inviolability of Private Life” (“Ruta de la Privatidad”). During the event, conference attendees discussed pressing issues related to personal data protection and presented a report to the conference attendees on the mandate of the Georgian Personal Data Protection Supervisory Body, along with the Service’s experience in safeguarding the personal data of minors.

In 2023, as part of its strategic development priorities aimed at expanding international cooperation, the Personal Data Protection Service became a member of the “Francophone Association of the Personal Data Protection Authorities”. The decision to accept the Service as a member was unanimously supported by all nineteen participating members of the association’s assembly, recognizing the Service as a data protection supervisory body. Established in 2007 with the support of French-speaking personal data protection authorities and representatives of the International Organization of Francophonie, the “Francophone Association of the Personal Data Protection Authorities” aims to enhance the effectiveness of its members’ activities, establish a French-language expert platform in the field of data protection, share best practices, inform members about relevant activities, and foster cooperation with other international organizations.

3. Cooperation with the Diplomatic Corps and International Organizations

In 2023, the President of the Personal Data Protection Service conducted an introductory meeting with the Latvian Ambassador to Georgia, Edīte Medne. During the meeting, the Ambassador was briefed on the functions, structure, activities, and future plans of the Personal Data Protection Service, including its action strategy. The discussion centered around legislative updates, international relations, and collaboration with European counterpart supervisory bodies.



An introductory meeting took place with the Ambassador of Romania to Georgia, Razvan Rotundu, and Consul, Marius Pandelea. During the meeting, the President of the Service outlined the main directions of the agency's activities, as well as the planned initiatives for institutional development. Discussions revolved around the prospects for future cooperation and the potential for collaboration between the personal data supervisory authorities of Georgia and Romania.

It's worth mentioning that to support the implementation of legislative changes regarding personal data protection, enhance public awareness, and foster institutional development of the Personal Data Protection Service, the Service actively collaborates with international organizations. With their assistance, a number of activities were conducted during the reporting period.

In 2023, within the framework of the EU project "Support to External Security Sector Oversight in Georgia," which aims, among other things, to strengthen personal data protection in law enforcement agencies, the head of the personal data protection supervisory body of Latvia, Jekaterina Macuka, visited the Personal Data Protection Service on an expert mission. During the workshop, the President of the Service shared insights into the Service's activities with the visiting expert, the head of the project team, and representatives, emphasizing the implementation of the new law "On Personal Data Protection" and the importance of exchanging best practices among European data protection supervisory bodies in this endeavor. During the reporting period, supported by the project and with the participation of an invited expert, a number of activities were conducted. These included a working meeting with representatives of law enforcement agencies to acquaint them with the changes outlined in the new legislative regulation of personal data. Additionally, a two-day training session was organized for employees of the Personal Data Protection Service and representatives of law enforcement agencies. It's worth noting that the project's objective is to develop training programs and informational materials to facilitate the establishment of a mechanism for sharing the experiences of personal data protection supervisory authorities of EU member states.

It's noteworthy that as part of the Council of Europe project "Strengthening Media Freedom, Internet Governance, and Personal Data Protection in Georgia," a hybrid working meeting was conducted on the topic: "Privacy by design and by default" for employees of the Personal Data Protection Service, led by invited expert of the Council of Europe, Nana Bochorishvili. Additionally, with the Council of Europe's support, an invited expert evaluated the draft normative act of the President of the Personal Data Protection Service titled "On the criteria for determining the circumstances that trigger the obligation to assess the impact on data protection and the assessment procedure" Recommendations issued were shared and incorporated into the final version of the draft normative act.

In 2023, with the backing of the European Union ("EU") and the United Nations Development Programme ("UNDP")- "Human Rights for All," the Service executed several initiatives aimed at institutional advancement and enhancing public awareness. Informational gatherings and events were organized for diverse target demographics, encompassing minors, representatives of ethnic minorities, and non-governmental organizations. Furthermore, informational booklets and illustrated posters were devised for the target audiences, available in the languages of ethnic minorities (Armenian and Azerbaijani), as well as tailored for minors. With program support and collaboration with Professor Konstantin Korkelia of Ivane Javakhishvili Tbilisi State University, a compilation of rulings from the European Court of Human Rights was assembled. This compilation encapsulates the most recent and precedent-setting practices concerning the safeguarding of the right to privacy. Additionally, as part of the program, guidelines on inspection techniques and methods were formulated with the participation of invited expert Nevena Ruzic. These guidelines were crafted based on the exemplary practices of European personal data protection supervisory authorities.

The year 2023 is also remarkable for hosting the inaugural meeting of the network comprising representatives from personal data protection supervisory bodies of Eastern Partnership countries in

Tbilisi. This event was co-organized by the Personal Data Protection Service and conducted within the framework of the project "Improving Public Services in the Eastern Partnership Countries" of the Eastern Partnership Regional Fund for Public Administration Reform. The opening day of the event commenced with welcoming addresses from the first deputy head of the Personal Data Protection Service, Otar Chakhunashvili, and the regional manager of the "PAR" project implemented by "GIZ", Dr. Hrachik Yarmaloyan. During the first day of the regional meeting, the staff of the Personal Data Protection Service delved into legal institutions and ongoing trends provided by the new law "On Personal Data Protection". Notably, they actively participated in a seminar aimed at enhancing the quality of state Services across Eastern Partnership countries, which received support from The German Agency for International Cooperation ("GIZ") and the Eastern Partnership Regional Fund. As part of this project, a workshop titled "Data-Protection in the Western Balkans and Eastern Partnership Region" was held in Brussels in September 2023. This workshop was organized by the "Regional School of Public Administration" (ReSPA) and the "Support for Improvement in Governance and Management" a joint initiative of the OECD and the European Union ("SIGMA"/"OECD"), the "Regional Cooperation Council" ("RCC"), and the German Agency for International Cooperation ("GIZ"). During these meetings, the Personal Data Protection Service was represented by the Head of the Office of the President and the Head of the Department of International Relations, Analytics, and Strategic Development. The personal data protection supervisory bodies of the participating countries have reviewed their legal arrangements and existing practices. Additionally, meetings were convened with prominent figures such as the Chairman of the "European Data Protection Board" ("EDPB"), the Secretary General of the "European Data Protection Supervisor" ("EDPS") institution, with the head of the Belgian Personal Data Protection Supervisory Authority, the Italian and Spanish Personal Data Protection Supervisory Authorities, and representatives of various EU institutions. The participants of the event also made presentations during the regular 84th plenary session of the "European Data Protection Board" ("EDPB"), where they discussed the legislative framework for personal data protection in Georgia, the mandate of the agency, and its activities. It's worth mentioning that since June 2022, a project initiated by the German Ministry for Economic Cooperation and Development ("BMZ") has been underway in five Eastern Partnership ("EaP") countries, namely Azerbaijan, Georgia, Armenia, Moldova, and Ukraine.

Participation in the EU project, "Supporting Public Administration Reform in Georgia," involved training sessions for Service employees on integrity matters. During these workshops, Hendrikus van Boxmeer, a senior expert in accountability, transparency, and integrity, along with trainer Nino Tsukhishvili, discussed integrity concepts, management tools, and policy enforcement mechanisms.

It's notable that the Service receives donor support from the "Public Governance Programme" of the U.S. Agency for International Development (DAI/USAID) to raise public awareness. Planned activities include developing a communication strategy and action plan for engaging with the public. Additionally, a training program will be prepared by a foreign expert to retrain a personal data protection officer.

Continuing to cooperate with various donor organizations, the Service aims for effective implementation and institutional development of the new law "On Personal Data Protection."

4. Study of Sectoral Trends and Research Activities

Development of thematic manuals, preparation of studies, research of international and European standards of personal data protection, and exploration of best practices of other states are among the directions of the service's activities.

In order to provide a comparative legal review of industry trends and create a discussion platform, on March 1, the Service held an international scientific conference entitled: "The Status of Personal Data Protection and Its Legal Aspects in Georgia". The conference featured four panel sessions where during the conference, representatives of the Service, as well as the judicial corps, the academic field, and expert circles presented reports to the participants of the event. These reports covered various topics, including the legal status of the Personal Data Protection Service, issues related to the protection of personal data of minors, corporate management, and judicial practice. Notably, Leonardo Cervera Navas, Secretary General of the "European Data Protection Supervisor" ("EDPS") institution, participated remotely as a special guest and presented a report.

In 2023, the Personal Data Protection Service hosted Prof. Norbert Bernsdorff, a former judge of the German Federal Social Court, a member of the editorial board of the Service's bilingual scientific periodical "Journal of Personal Data Protection Law," and a professor at Philipps University of Marburg. This event aimed to implement the new law "On Personal Data Protection" and to share internationally recognized best practices in the field of personal data protection. Employees of the Personal Data Protection Service and representatives of the academic circle of Ivane Javakhishvili Tbilisi State University attended the event. In his report, Prof. Norbert Bernsdorf expressed a positive view regarding the adoption of the new law, "On Personal Data Protection," emphasizing its alignment with the EU's "General Data Protection Regulation" and internationally recognized standards in the field of data protection law. The Professor also conveyed his readiness to collaborate with the Service in providing scientific and expert support for the implementation process of the new law and to participate in the Service's scientific-discussion platforms concerning legislative innovations.

Under the current memorandum of cooperation with the Croatian Personal Data Protection Agency, "Agencija za zaštitu osobnih podataka," Service employees, along with representatives from the German and North Macedonian Data Protection Supervisory Authorities, engaged in online workshops hosted by the Croatian Personal Data Protection Agency. The workshops covered topics such as "Inspection of Data Protection Using a Standard Model" and "Data Protection Impact Assessment." These sessions were dedicated to exchanging experiences among the supervisory bodies of the involved nations, conducted through discussions and question-and-answer sessions.

Each month, the Service releases an information digest titled “World Practice,” highlighting the latest developments in personal data protection. This digest includes insights into notable practices of leading data protection supervisory bodies worldwide, as well as recommendations and significant rulings from the European Court of Human Rights and the Court of Justice of the European Union.

The Service has crafted and published a study titled “Personal Data Protection of Minors: Theory and Practice” [4] focusing on the subject of safeguarding minors’ personal data. The aim of the paper is to study the best international standards regarding the rights of minors in the digital environment, and beyond, and to adapt them to national legislation.

The second edition of the Service’s bilingual, periodic, scientific publication, the “Journal of Personal Data Protection Law,” [5] for the year 2023 has been released, commemorating the 10th anniversary of the Personal Data Protection Supervisory Body of Georgia. This edition features contributions from the editor-in-chief, the Public Defender of Georgia, the Secretary General of the “European Data Protection Supervisor” (“EDPS”), as well as scholarly articles authored by representatives from foreign personal data protection supervisory bodies, international experts, and practitioners from Georgia. Notably, to qualify for indexing in the scholarly database of “HeinOnline,” the journal underwent rigorous evaluation based on criteria such as its publishing policy, mission, and academic standards. It was subsequently integrated into the database following the decision of the database’s leadership.

4 See Electronic version of the paper: <https://personaldata.ge/ka/press/post/9629>.
5 See “Journal of Personal Data Protection Law” Second edition of 2023, <www.journal.pdps.ge>.

V

ENHANCING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES

CHAPTER V. ENHANCING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES

Raising public awareness remained one of the main tasks for the Personal Data Protection Service in 2023. To foster a culture of personal data protection within society, promoting privacy, and safeguarding both individual and collective rights, the Data Protection Supervisory Authority of Georgia engaged in an array of initiatives, campaigns, and educational endeavors throughout the year. These activities aimed to educate diverse segments of society and various age demographics about the significance of personal data protection, thereby raising awareness and understanding of data privacy issues.

1. Various Awareness-Raising Activities

- **28 January – International Day of Personal Data Protection**

The International Data Protection Day was celebrated with a large-scale event, which included various activities and was open to people of all age-groups.

- The Tbilisi TV broadcasting tower and the Ferris Wheel were lit up in the colours of the logo of the Personal Data Protection Service of Georgia;
- Lela Janashvili, the President of the Service, delivered a presentation covering two main topics: The Legal Clinic for Personal Data Protection and the first scientific journal focused on Personal Data Protection Law. Additionally, she shared video clips with the audience to enhance public awareness.
- Psychologist Zurab Mkheidze gave a public lecture on the culture of habitual behaviour;
  An engaging open lesson and enjoyable activities were organized for students and young children to emphasize the significance of safeguarding personal data;
- Guests attending the event had access to the consultation room throughout the day;

The media actively covered the event.

28 JANUARY

CAMPAIGN – "#PRIVACY IS YOUR RIGHT!"

Personal Data Protection Service of Georgia started the year of 2023 by launching a campaign called "Privacy is Your Right". As part of the campaign, informational videos were prepared with the participation of representatives from various fields.

In any environment or space- "#privacy is your right"- distinguished representatives of the field talk about the importance of protecting personal data in education, medicine, the digital world, the labour market and photography.

As part of the campaign, the teacher and scientist Gia Murgulia, the endocrinologist and Doctor Ketevan Asatiani, the President of the Association of Farmers Nino Zambakhidze, the cybersecurity specialist Giorgi Gurgenidze and the photographer Goga Chanadiri shared insights from their respective domains, highlighting the importance and risks associated with personal data protection. They offered concrete examples, advice, and stressed the significance of privacy.

The campaign videos garnered a total of 255,000 views on social media platforms during the reporting period. Additionally, various media outlets covered the presentation of these video clips in their broadcasts.

CAMPAIGN - “#DETECT VIOLATION”

In order to raise public awareness in 2023, a social networking campaign- “#detect the violation” was carried out. As part of the campaign, illustrated cards were created to help people check how aware they are, how much information they have about the basics of data protection and whether they can detect a violation in a given situation.

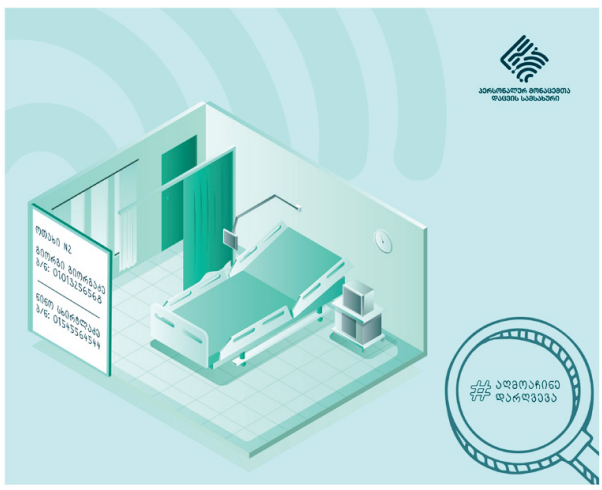
A total of 204,388 users of the social network accessed the illustrated cards as part of the campaign.


პერსონალურ მონაცემთა დაცვის სამსახური
#ადამიანი დარღვევა


თუ პირადი ინფორმაციის შემცველ დოკუმენტებს გადაყრას უპირებთ, დაანგრევდეთ! ან დაანჯიანით იმგვარად, რომ მასზე დატანილი ინფორმაცია გარჩევადი არ იყოს!
პერსონალურ მონაცემთა დაცვის სამსახური
#ადამიანი დარღვევა


პერსონალურ მონაცემთა დაცვის სამსახური
შეიქმნეთ პაროლი ციფრებით
#ადამიანი დარღვევა


დარღვევაა, თუ მარკეტინგულ შეტყობინებას მასზე უარის თქმის მექანიზმის გარეშე გაგზავნით ან მიიღებთ!
პერსონალურ მონაცემთა დაცვის სამსახური
შეიქმნეთ პაროლი ციფრებით
SMS OFF: 0000
#ადამიანი დარღვევა


პერსონალურ მონაცემთა დაცვის სამსახური
ოთახი №2
პირადი ინფორმაცია
პირადი ინფორმაციის მიმღები
#ადამიანის უფლებები

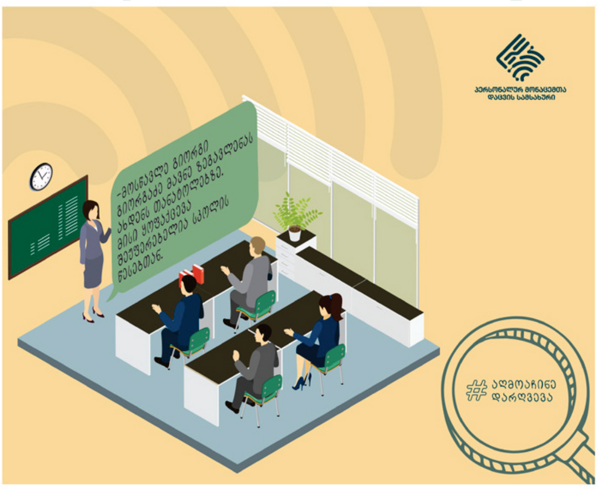

ნებისმიერი დაწესებულება ვალდებულია დაიცვას მოხმარებლის პირადი ინფორმაცია, მათ შორის, ინფორმაციის მისი ვიზიტის შესახებ.
პერსონალურ მონაცემთა დაცვის სამსახური
ოთახი №2
პაციენტი №1
პაციენტი №2
#ადამიანის უფლებები

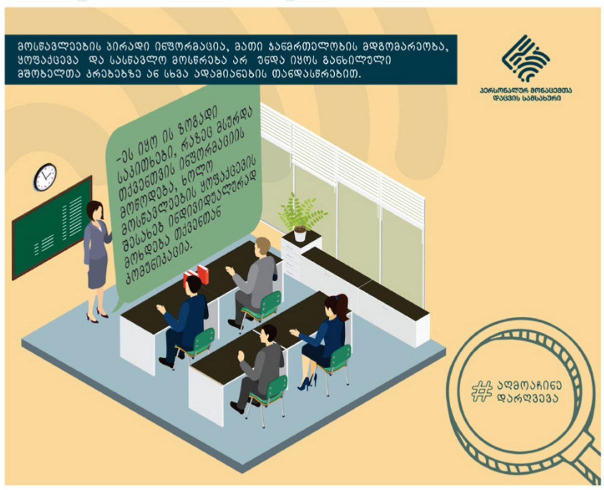

პერსონალურ მონაცემთა დაცვის სამსახური
#ადამიანის უფლებები


„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს, რომ ჯანმრთელობის მდგომარეობასა და ჯანმრთელობის მიმართ გაწეული ადრინდელი მიზნებისთვის თითის ანაბეჭდის გამოუვლენლად წარმოადგენს კანონის მოთხოვნების დარღვევას.
პერსონალურ მონაცემთა დაცვის სამსახური
#ადამიანის უფლებები


-გამარჯობა, ინებეთ.
-გამარჯობა, ჩემი მეუღლის ანალიზების პასუხი მსურს გავიტანო. გიორგი გიორგაძე, 01012545875
-მადლობა.
პერსონალურ მონაცემთა დაცვის სამსახური
აღმოაჩინე დარღვევა


დაუშვებელია, სხვისი პერსონალური ინფორმაცია გადაეცეს სხვა პირს შესაბამისი ნებართვის ან დამამტკიცებელი საბუთის გარეშე.
-გამარჯობა, სხვა პირის ანალიზების პასუხს ვერ გაგატანთ, გარდა იმ შემთხვევისა თუ მისი წერილობითი თანხმობა არ გაქვთ.
-გამარჯობა, ჩემი მეუღლის ანალიზების პასუხი მსურს გავიტანო. გიორგი გიორგაძე, 01012545875
-მადლობა, გასაგებია
პერსონალურ მონაცემთა დაცვის სამსახური
აღმოაჩინე დარღვევა


-მოსწავლე გიორგი გიორგაძე მავნე ზეგავლენას ახდენს თანატოლებზე. მისი ყოფაქცევა შეუფერებელია სკოლის წესებთან.
პერსონალურ მონაცემთა დაცვის სამსახური
აღმოაჩინე დარღვევა

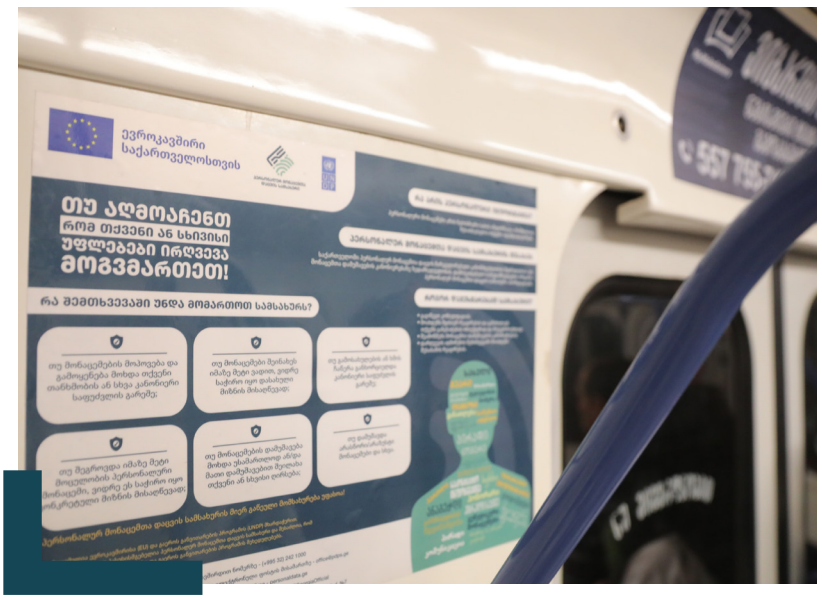

მოსწავლეების პირადი ინფორმაცია, მათი ჯანმრთელობის მდგომარეობა, ყოფაქცევა და სასწავლო მოსწრება არ უნდა იყოს განხილული მშობელთა კრებებზე ან სხვა ადამიანების თანდასწრებით.
-ეს იყო ის ზოგადი საკითხები, რაზეც მსურდა თქვენთვის ინფორმაციის მოწოდება, ხოლო მოსწავლეების ყოფაქცევის შესახებ ინდივიდუალურად მოხდება თქვენთან კომუნიკაცია.
პერსონალურ მონაცემთა დაცვის სამსახური
აღმოაჩინე დარღვევა

Informational Posters in Public Transport

The Personal Data Protection Service has placed informational posters in municipal transport in Tbilisi, Batumi, Gori, Rustavi and Telavi.

What is personal data, what are the risks of disclosing personal data, in what cases are human rights violated and how to contact the Service- citizens can get answers to these questions while travelling by municipal transport.

The project was implemented with the support of the European Union (EU) and the United Nations Development Programme (UNDP), Tbilisi City Hall and Tbilisi Transport Company LLC.



Printed Information Brochures

Printed informational brochures titled 'Be informed, protect your personal data!' have been created to educate individuals about personal information and its protection. These materials include details on when and how to reach out to the Service for assistance. Additionally, brochures translated into Armenian and Azerbaijani were distributed to ethnic minority groups during various meetings, events, and activities.

The brochures were printed with support from the European Union (EU) and the United Nations Development Programme (UNDP).

Information Brochures for Persons with Disabilities

In order to raise the awareness of persons with disabilities on the issue of personal data protection, the Personal Data Protection Service produced the existing brochures in Braille. These materials were handed over to the Tbilisi and Batumi Unions of the Blind.

It should be noted that the Georgian Blind Union has 15 branches in Tbilisi and the regions, with about 3000 members. Personal Data Protection Service will gradually hand over brochures in Braille to all branches of the Union of the Blind in Georgia.

Informative Newspapers Enrich the Tbilisi-Batumi Train Experience

On the occasion of the opening of the Service's new representative office in the city of Batumi, informational leaflets and entertaining newspapers were distributed on several routes of the Tbilisi-Batumi train.

These brochures informed the passengers about the activities of the Service and issues related to the protection of personal data, and they had the opportunity to familiarise themselves with articles, quizzes, scans, crosswords and campaigns of the Service in the cognitive and entertaining newspaper prepared on issues related to the protection of personal data. This initiative was implemented with the support of Georgian Railways.

Image Video Clip

In 2023, the Service introduced a new image video aimed at informing the audience about the importance of safeguarding personal data and how to reach out to the Service when needed. This video was created with support from the Eastern Partnership Fund project of the German Society for International Cooperation (GIZ).

Throughout the reporting period, the video garnered 86,000 views on social media platforms. Additionally, a condensed version of the video was aired on various television programs, including the advertising networks of the Public Broadcaster, Adjara Television, "Imedi," and "Rustavi 2" television companies, as well as on the programs of the Public Broadcaster and Adjara Radio.

Article Contest for Students

For the students of the higher education institution of the Autonomous Republic of Adjara, the Service organised an article competition on the topic “Protection of personal data as a universally recognised human right”. The aim of the competition was to raise students’ awareness of the importance of personal data protection. The winners received commemorative gifts.

Informational Activities on The Protection of Minors’ Personal Data

During the reporting period, special attention was paid to the issue of protection of personal data of minors. During the year, information trainings were actively conducted and printed materials were prepared - posters, notebooks, stickers, bookmarks, erasers and school boards. Entertaining and educational materials tailored to young people help them learn about personal data protection issues in simple and understandable language. Among them, The training held in the village near the occupation line holds particular importance. The President of the Service - Lela Janashvili, the first deputy - Otar Chakhunashvili, the deputy - Gela Gelashvili, as well as other representatives of the Service visited the public school of the village of Kveshi and held a meeting with students and teachers.

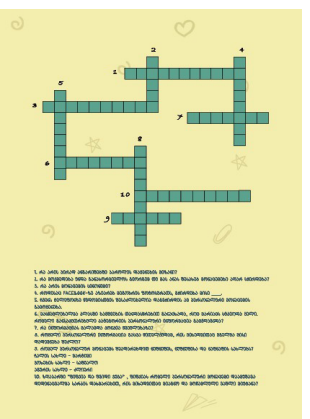
nformative Posters in Public Schools

What is personal data, how should children protect personal data when communicating with unknown or known persons at school or on the Internet, and how should they contact the Service in case of violation - to get answers to these questions, the Personal Data Protection Service has placed informative/illustrated posters in all public schools in Georgia, including for representatives of ethnic minorities in Armenian and Azerbaijani languages.

Informative posters have been placed in more than 2200 schools. This project was implemented with the support of the European Union (EU), the United Nations Development Programme (UNDP) and the Ministry of Education and Science.

Informative Activities in Social Networks and Media

A variety of entertaining and educational posts emphasizing the significance of safeguarding minors' personal data were shared across social media platforms. These included quizzes, puzzles, and crosswords aimed at raising awareness. Additionally, programs and media reports were developed specifically for June 1st- the International Day of Child Protection.



Establishing an Information Stand at the University

A dedicated information corner on personal data protection has been inaugurated at Ivane Javakhishvili Tbilisi State University. Located in the second building of the Tbilisi State University, the corner serves as an educational hub where students can explore the importance of protecting personal data, understand the risks associated with its disclosure, and learn about the services offered by the institution. Within the designated student area, an interactive personal data protection alphabet has been installed, providing both informative content and practical functionality. In addition, the lockers are equipped with mobile phone chargers to ensure that students can safely charge their devices while accessing the resources provided.

ESTABLISHING AN INFORMATION STAND AT THE UNIVERSITY

Website and Social Media

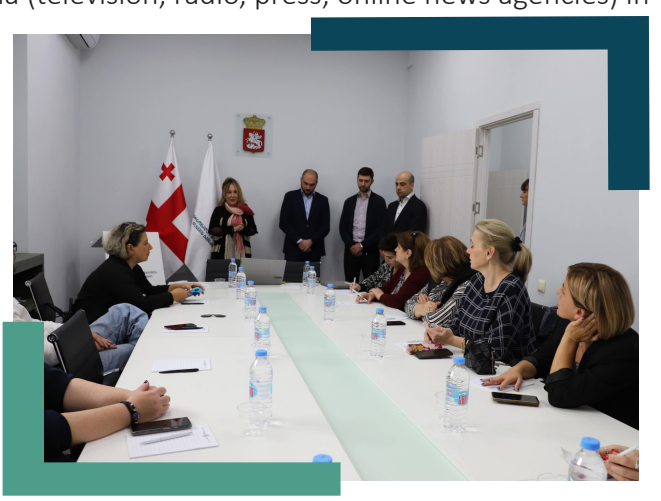
Social Media ("Facebook", "linkedin", "X", "Youtube")

In addition to the meetings and other activities of the Service, the decisions, "world practices", announcements and publications of the Service were systematically published on the social networks of the Service throughout the year. Reports and statistical data on the activities of the Service were published on a quarterly basis.

208 posts were placed by the Service in the social network "Facebook", the number of users accessing these posts was 1,033,986, and the number of page visitors was 161,863. The number of subscribers to the official page of the Service is growing and in December 2023 it will be 14,400. As for the Service's website (www.personaldata.ge; www.pdps.ge), the number of visitors is 106,000, which is also an increase compared to the previous year.

Media Engagement

The Service actively cooperates with the media (television, radio, press, online news agencies) in order to raise public awareness about the activities of the Service and issues related to the protection of personal data.



It should be noted that public information, transparency and accountability are among the main priorities of the Service. To this end, representatives of the media were invited to all important events organised by the Service. Information on cases of high public interest, the activities of the Service, various activities and precedent decisions is published proactively. 44 press releases were sent to the media and news agencies.

Representatives of the Service participated in more than 20 programmes on television news, morning and afternoon programmes, radio and thematic programmes (business, economy, medicine, etc.). Interviews were published in online media. A number of comments were made on issues of interest to journalists.

2 briefing sessions were held for media representatives (in Adjara and Tbilisi) to provide detailed information on personal data protection issues. The meetings were attended by more than 30 representatives of different media.

2. Conducted Trainings and Public Lectures

In 2023, 62 public lectures and training sessions were held for public and private organisations, including across regions, with 3158 interested participants.

Regional meetings were held with representatives of the Autonomous Republic of Adjara, the public and private sectors, students, the media, private organisations and representatives of municipalities in the Imereti and Kakheti regions. Representatives of the Ministries of the Autonomous Republic of Abkhazia also participated in the meetings. Briefings were held with the Administration of the Government of Georgia, the Ministry of Economy and Sustainable Development of Georgia, the Ministry of Finance of Georgia, the Ministry of Environmental Protection and Agriculture of Georgia, the Ministry of Foreign Affairs of Georgia, the Ministry of Culture, Sports and Youth of Georgia, and the Office of the State Minister for Reconciliation and Civil Equality, for representatives of the Ministry of Justice, the Ministry of Regional Development and Infrastructure of Georgia, the IDPs from the Occupied Territories of Georgia, the Ministry of Labour, Health and Social Protection, the Ministry of Education and Science of Georgia, as well as public legal entities and sub-departmental institutions in the system/subordination of the ministries. Meetings were also held with representatives of Tbilisi City Hall, Tbilisi Sakrebulo, district administrations and public legal entities/non-entrepreneurial legal entities in the system/subordination of the City Hall and other organisations exercising public authority.

Sectoral meetings were held for representatives of private sector companies and associations, including the Union of Industrialists and Employers, as well as representatives of the health care, education, media, insurance, banking and finance sectors.

CONDUCTED TRAININGS AND PUBLIC LECTURES

VI

ADMINISTRATIVE MANAGEMENT OF THE SERVICE

CHAPTER VI. ADMINISTRATIVE MANAGEMENT OF THE SERVICE

1. Issues of Organisational Management of the Service

1.1. Institutional Strengthening and Internal Organization of the Service

In 2023, notable alterations were made to the organizational framework of the Service. These adjustments involved integrating the Department of Planned Inspection and the Office of the President of the Service into the Service itself. Additionally, within the Department of Information Technology and Monitoring, a monitoring department was established.

Furthermore, in September 2023, the Service expanded its operations by representative office in Batumi.

Moreover, during the same year, the Service initiated an internship program designed to enhance the qualifications and professional growth of students and graduates from relevant higher educational institutions. This program offers participants invaluable opportunities to acquire practical experience and develop essential skills.

1.2. Career Management and Number of Employees

At the end of 2022, in accordance with the legislation, on the basis of the evaluation of the performance of the employees in the Service in 2023, 17 employees of the Service were promoted/increased to the rank of civil servant. In addition, starting from January 1, 2023, employees of the Personal Data Protection Service who previously held a state special rank or military rank in state service were granted the corresponding state special rank of the Personal Data Protection Service according to amendments to the law. Furthermore, some employees who did not previously have a state special or military rank were awarded a state special rank for their conscientious performance of official duties by the decision of the President of the Personal Data Protection Service.

It's noteworthy that in 2023, the number of employees of the Service increased to 67, consisting of 64 civil servants and 3 officials. At the beginning of the year, on 1 January 2023, the Service employed 47 individuals, leaving 20 posts vacant. By the end of the year, on 31 December 2023, the number of full-time staff had increased to 64, comprising 61 civil servants and 3 officials. In addition, the number of employed contract staff increased from 9 at the beginning of the year to 17 at the end of the year.

As of December 31, 2023, the number of individuals employed in the Personal Data Protection Service by category and gender is as follows:

№	INFORMATION ABOUT EMPLOYEES	NUMBER	NUMBER OF WOMAN	NUMBER OF MAN	WOMAN - %	MAN - %
1	TOTAL AMOUNT OF ACTING EMPLOYEES	81	38	43	47%	53%
2	STATE OFFICIALS	3	1	2	33%	67%
3	PROFESSIONAL CIVIL SERVANTS APPOINTED TO A MANAGERIAL POSITION	16	10	6	63%	37%
4	PROFESSIONAL CIVIL SERVANTS APPOINTED TO NON-MANAGERIAL POSITION	45	22	23	49%	51%
5	CONTRACT EMPLOYEES	17	5	12	29%	71%

In 2023, the Service organized 37 open competitions and 5 internal competitions to recruit new staff. The Service received applications from 1,634 candidates, resulting in the recruitment of 32 new employees. Additionally, within the framework of the 5 internal competitions, 5 existing employees were appointed to senior positions, including 4 heads and 1 first-category senior specialist.

1.3. Enhancing Employee Qualifications and Organizational Ethics

The reporting period was significant for the professional development and skill enhancement of staff. The staff of the Personal Data Protection Service participated in 36 training events. It should be noted that several lectures/trainings were held within the framework of cooperation with international organisations, and the representatives of the Service had the opportunity to receive important information from local and international experts. In addition to professional training, the staff of the Service actively participated in training courses for civil servants.

The 'Employees for Employees' internal training campaign continued during the reporting period, with employees of the Service holding lectures and training sessions for other interested employees. As part of this campaign, informational training for new employees was actively conducted to facilitate their integration into the organization. It is also important to note that employees of the Service actively participated in training on the rights of persons with disabilities and standards of communication with them, prevention of sexual harassment and response mechanisms, emergency procedures, practical aspects of applying decisions of the European Court of Human Rights, basics of information security, and other important issues.

The rules of disciplinary proceedings and the Code of Ethics for employees of the Personal Data Protection Service were adopted.

It should be noted that during the reporting period the Code of Ethics was fully respected and no disciplinary misconduct was observed in the workplace.

Also in 2023, the Service has approval of policy documents, namely:

— Gender Equality Policy of the Personal Data Protection Service;

— Standard of communication with citizens in the Personal Data Protection Service;

— Labor Security Policy of the Personal Data Protection Service.

Working and favorable conditions, adapted to the interests of employees, were considered as much as possible.

According to the changes in the legislation during the reporting period, the employees of the Personal Data Protection Service are subject to mandatory state insurance, which has contributed to the creation of solid social protection guarantees for the employees of the Service and has had a positive effect on the motivation of the employees and the strengthening of the work culture.

2. Budget and Performance of the Personal Data Protection Service of Georgia

2.1. Budget and Performance of the Personal Data Protection Service of Georgia

According to Article 46 of the Law of Georgia "On Personal Data Protection", the activities of the Service are financed from the State budget of Georgia and the necessary allocations are determined by a separate code. The approved budget for 2023 is GEL 5,500,000. As of 1 January 2023, 67 staff units have been defined for the Service and 66 civil servants have been appointed to equivalent positions. According to the structure and staff list of the Service, the organisational structure of the Service includes 9 departments and the Office of the President of the Service. During the reporting period, the cash flow of the budget amounted to GEL 5,214,594. It should be noted that the percentage of cash flow in relation to the annual plan is 94.81%.

№	ARTICLE OF BUDGET CLASSIFICATION	DETAILED PLAN	CASH FLOW PERFORMANCE
1	REMUNERATION	3 460 000	3 409 025
2	GOODS AND SERVICES	1 400 000	1 227 035
3	SOCIAL SECURITY	60 000	40 322
4	OTHER EXPENSES	65 000	50 983
5	NON-FINANCIAL ASSETS	515 000	487 229
	TOTAL	5 500 000	5 214 594

2.2. Salary, Bonus and Monetary Reward

During the reporting period, the employees of the Personal Data Protection Service (including the President of the Service and the Deputy Presidents of the Service) received official bonuses amounting to GEL 2,808,747.03 and rank bonuses amounting to GEL 6,657.12.

During the reporting period, 396,451.34 GEL was given as bonuses to the employees of the Service, of which 106,530.14 GEL was given to an employee with a special rank within the framework of the mandatory bonus stipulated by the Law of Georgia "On Personal Data Protection"; 23,850.93 GEL- within the framework of the mandatory bonus stipulated by the fourth paragraph of Article 26 of the Law of Georgia "On Public Service"; and 266,070.27 GEL- for additional functions and overtime work. In 2023, a bonus of GEL 197,169.50 was given to the employees of the Service.

The total remuneration of the employed persons under the labour contract (18 employees) during the reporting period amounted to GEL 316,704.23.

2.3. Means of Transport

According to the status as of January 1, 2023, six vehicles were registered on the balance of the Personal Data Protection Service. The vehicles were not sufficient to meet the needs of all departments, depending on the workload. It is worth mentioning that in 2023, a new office of the Service was opened in Batumi. In addition, Service employees often travel to regions throughout the country, which increases the demand for the use of vehicles.

Based on the above, during the year, four units of vehicles were purchased within the framework of the 2022 budget through a consolidated tender.

During the reporting period, the actual expenses for the technical service of 10 vehicles amounted to GEL 10,680.17 and fuel expenses amounted to GEL 36,023.44

2.4. Real Estate Included In The Balance Sheet Of The Service

In order to develop the organisation of the Service, strengthen its institutions and carry out strategic tasks, new structural units were created in 2023 and 17 staff units were added to the existing staff. In order to facilitate the establishment of the regional representation office in Adjara and the creation of new structural units, as well as the full and smooth exercise by the Service of the powers vested in it by law, and to provide staff with adequate working space, 2 structural units of the Service were accommodated in leased private premises (the cost of the 9-month lease was 50,682.21 GEL).

At the end of 2022, for the purpose of regional enlargement of the Service, GEL 148 192.80 was spent on the improvement of the building on Bako Street in Batumi on necessary repairs and renovations.

At the end of 2023, the Service had 2 properties on its balance sheet.

№	REAL ESTATE, ADDRESS	TYPE OF RIGHT	PURPOSE
1	TBILISI, N. VACHNADZE STR. N7	STATE-OWNED PROPERTY (WITH RIGHT TO USE)	ADMINISTRATIVE BUILDING, WHERE 7 DEPARTMENTS OF THE SERVICE (STRUCTURAL UNIT) ARE LOCATED
2	BATUMI, BAKO STR. N48	PROPERTY OF A/R OF ADJARA; RIGHT TO USE BEFORE THE DEMAND	THE ADMINISTRATIVE BUILDING WHERE THE WESTERN REPRESENTATIVE OFFICE IS LOCATED

2.5. Secondments and Other Expenses

In the reporting period, the expenses for secondments within the country amounted to GEL 25,525.29 and outside the country to GEL 131,596.36.

In the reporting period, the telecommunications expenses of the Personal Data Protection Service amounted to GEL 15,019.29.

In addition, the cost of advertising by the Service amounted to GEL 70,138.83. It should be noted that only events aimed at raising public awareness were the subject of advertising.

2.6. Financial Support From Donor Organisations

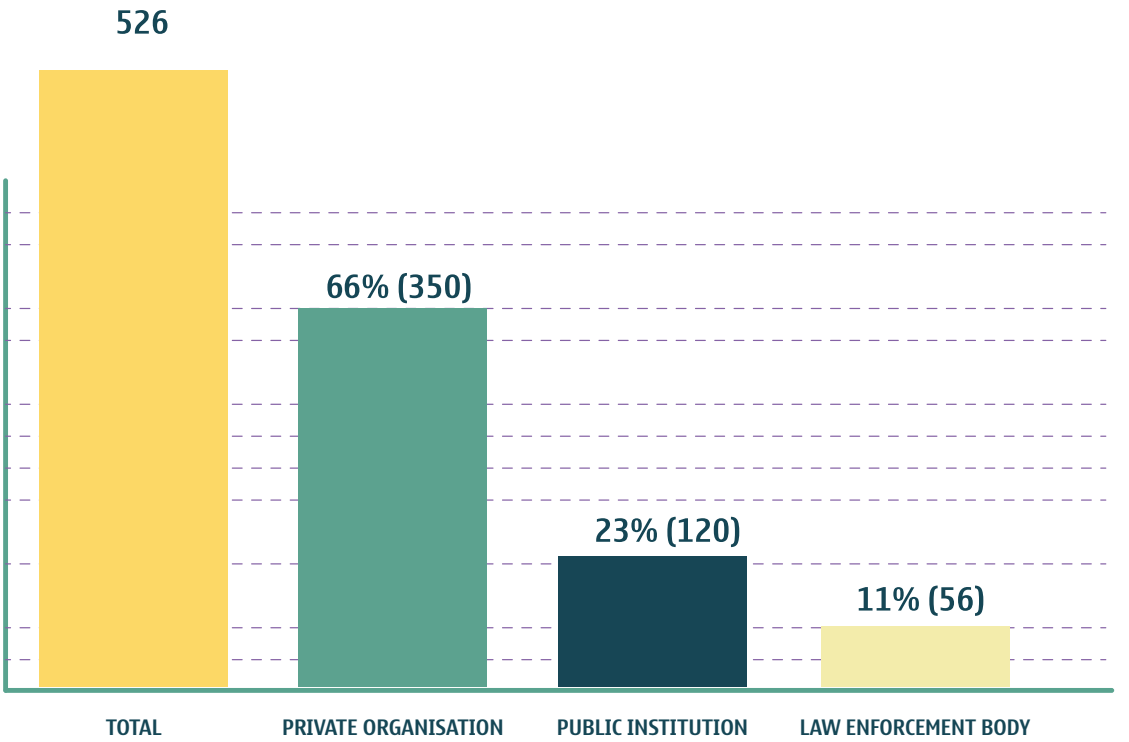
During the reporting period, the Personal Data Protection Service, with the support of the Eastern Partnership Regional Fund of the German Society for International Cooperation ("GIZ") and within the framework of the joint project "Human Rights for All" of the European Union ("EU") and the United Nations Development Programme ("UNDP"), carried out various activities on personal data protection issues to raise public awareness. With donor support, informational posters were printed and placed in public transport throughout the country, and informational brochures and booklets were published in Georgian, Armenian and Azerbaijani for representatives of ethnic minorities. In addition, a graphic video clip was produced to create an active promotional campaign on the importance of personal data protection, which was subsequently broadcast on social networks and television.

ANNEX №1: STATISTICAL DATA

1. Statistics on the Monitoring of the Lawfulness of Data Processing

DONOR ORGANIZATION	FORM OF ASSISTANCE	CONTENTS OF ASSISTANCE	COST (GEL)	STATUS
UNDP - the joint project of the European Union and the United Nations Development Programme "Human Rights for All"	Marketing Materials	Triplets, brochures in 3 languages (Georgian, Armenian, Azerbaijani)	16 989 34	Completed
GIZ Eastern Partnership Regional Fund of the German Society for International Cooperation	Fixed Asset	Graphic video clip	6 449	Completed

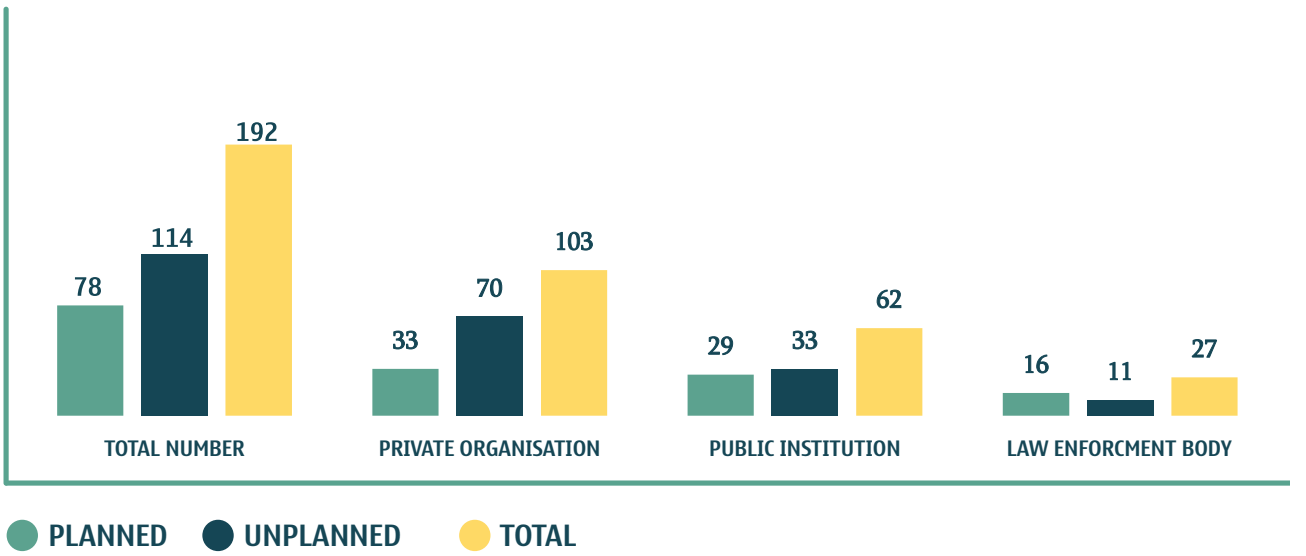
NUMBER OF APPLICATIONS / NOTIFICATIONS RECEIVED



During the reporting period, the Service received 526 applications/notifications, of which 83% (436) were applications and 17% (90) were notifications. 66% (350) of the applications/notifications concerned data processing by private bodies/individuals, 23% (120) concerned data processing by public bodies, and 11% (56) concerned law enforcement authorities.

It should be emphasised that the number of applications/notification has increased compared to 2022. In particular, in 2022, the Service received 447 applications/notifications, of which 64% (287) were applications and 36% (160) were notifications. 62% (277) of the applications/notifications concerned data processing by private bodies, 21% (93) concerned data processing by public bodies and 17% (77) concerned law enforcement authorities.

EXAMINATION/INSPECTION

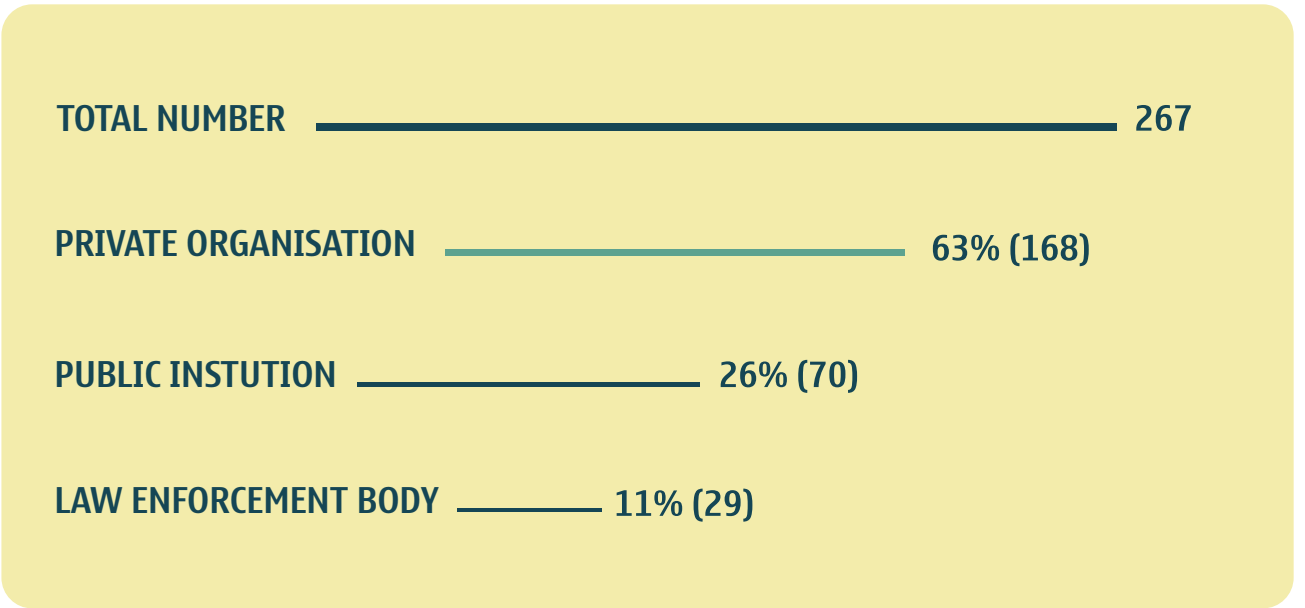


During the reporting period, the Service conducted 192 inspections of the lawfulness of personal data processing, of which 59% (114 inspections) were unplanned and 41% (78 inspections) were planned.

Of the 192 inspections, 54% (103 inspections) were related to the examination of the lawfulness of data processing by the private sector, 32% (62 inspections) by public bodies, and 14% (27 inspections) by law enforcement agencies.

The number of inspections/inspections carried out in 2022 was 149, so in 2023 the mentioned indicator has increased, namely 68% (101 inspections) were unplanned and 32% (48 inspections) were planned. Out of 149 inspections, 54% (81) were related to the verification of the lawfulness of data processing by the private sector, 28% (42) by public authorities and 18% (26) by law enforcement bodies.

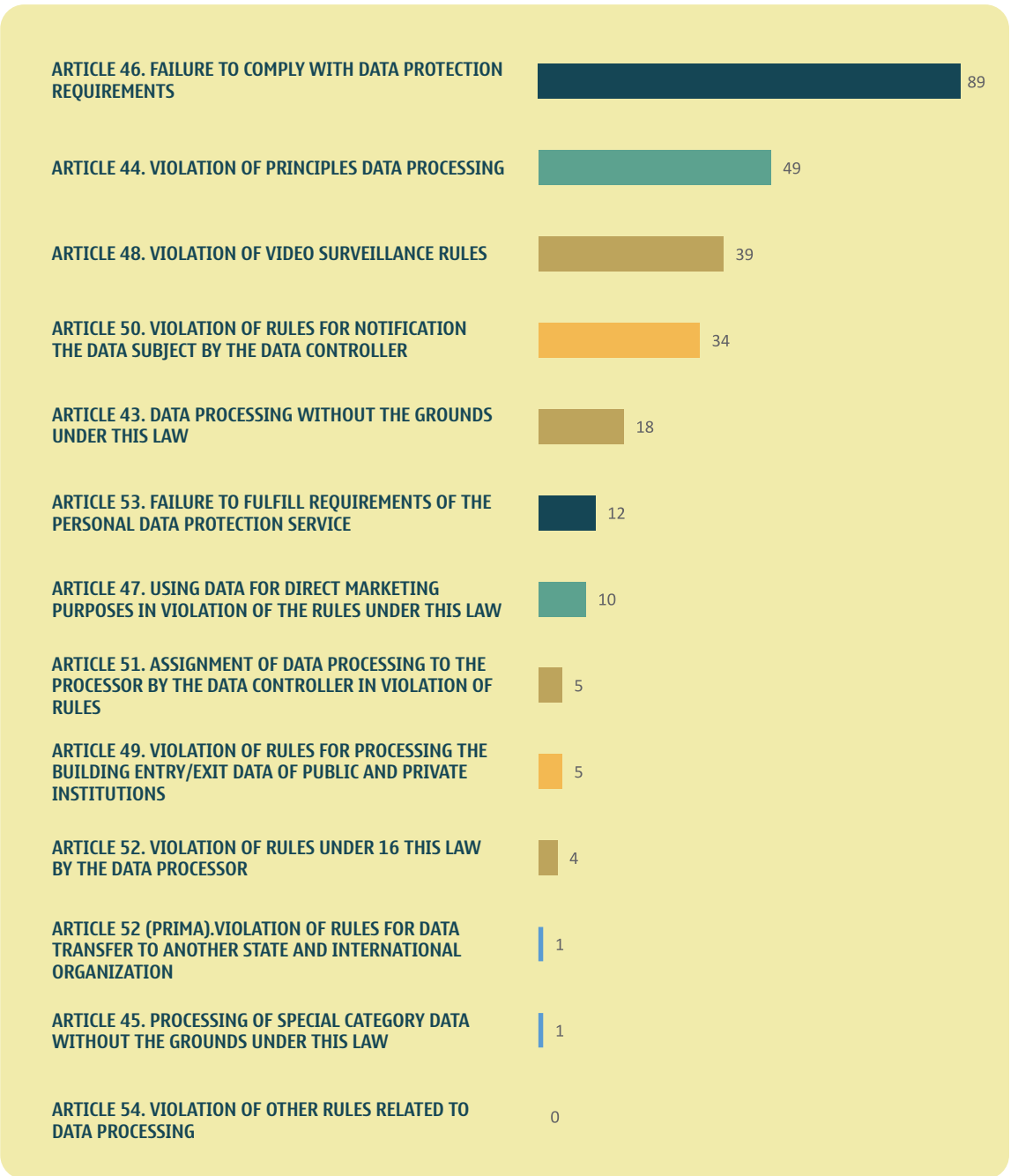
ADMINISTRATIVE OFFENCES



During the reporting period, the Service identified 267 cases of unlawful processing of personal data, of which 39 cases were detected from 2022 to the reporting period and 228 cases - from 2022 to the reporting period - were detected as a result of inspections. 63% (168) of the cases concerned unlawful processing in the private sector, 26% (70) in the public sector and 11% (29) in law enforcement bodies.

It should be noted that the number of offences detected has increased compared to 2022. In 2022, the Service detected 157 cases of unlawful processing of personal data and 64% (101) of the administrative offences concerned unlawful processing in the private sector, 27% (42) in the public sector and 9% (14) in law enforcement agencies.

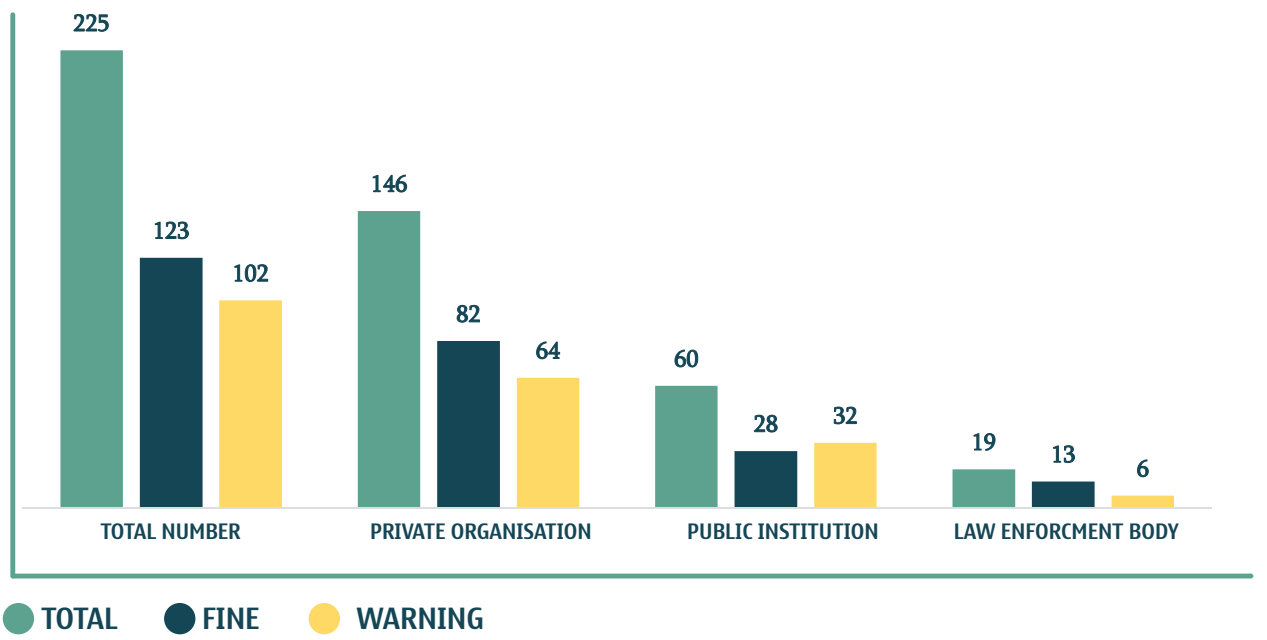
ADMINISTRATIVE OFFENCES



In the reporting period, 33% (89) of the 267 offences detected by the Personal Data Protection Service were related to non-compliance with data security requirements, 18% (49) to non-compliance with data processing principles and 15% (39) to non-compliance with video-surveillance rules.

In 2022, 27% (43) of the 157 offences detected by the Service concerned non-compliance with data security requirements, 24% (37) with data processing principles and 15% (23) - failure to inform the data subject by the controller.

ADMINISTRATIVE SANCTIONS



As a result of the examinations (inspections) carried out during the reporting period, 225 subjects were fined. Of those found to have committed an administrative offence, 123 subjects (55%) received an administrative fine and 102 (45%) received a warning. Of the 123 fines imposed, 19 were related to inspections started and completed during the reporting period in 2022 and 104 were related to inspections started and completed during the reporting period. Of the 102 warnings issued, 15 were for inspections started in 2022 and completed in the reporting period and 87 were for inspections started and completed in the reporting period. One of the controller was exempted from the administrative fine by the Service and received a verbal warning.

Of the administrative fines imposed, 65% (146) were imposed on private institutions, 27% (60) on public institutions and 8% (19) on law enforcement bodies.

Compared to 2022, the number of administrative fines imposed has increased. In particular, administrative fines were imposed on 123 subjects in 2022. Of the identified administrative offenders, 86 (70%) received an administrative fine and 37 (30%) received a warning.

INSTRUCTIONS AND RECOMMENDATIONS

TOTAL NUMBER	472
INSTRUCTION	459
RECOMMENDATION	13

In addition to the imposition of administrative sanctions, the Service issued mandatory instructions and recommendations to remedy the identified non-compliances. The Service issued 472 instructions and recommendations to public institutions and private organisations and law enforcement bodies. Out of 459 instructions, 63 were related to inspections started in 2022 and completed in the reporting period, and 396 were related to inspections started and completed in the reporting period. Of the 13 recommendations issued, 1 related to inspections started in 2022 and completed during the reporting period and 12 related to inspections started and completed in 2023. Of the 472 instructions and recommendations issued, 48% (226) were addressed to a private entity, 41% (196) to a public entity and 11% (50) to a law enforcement body.

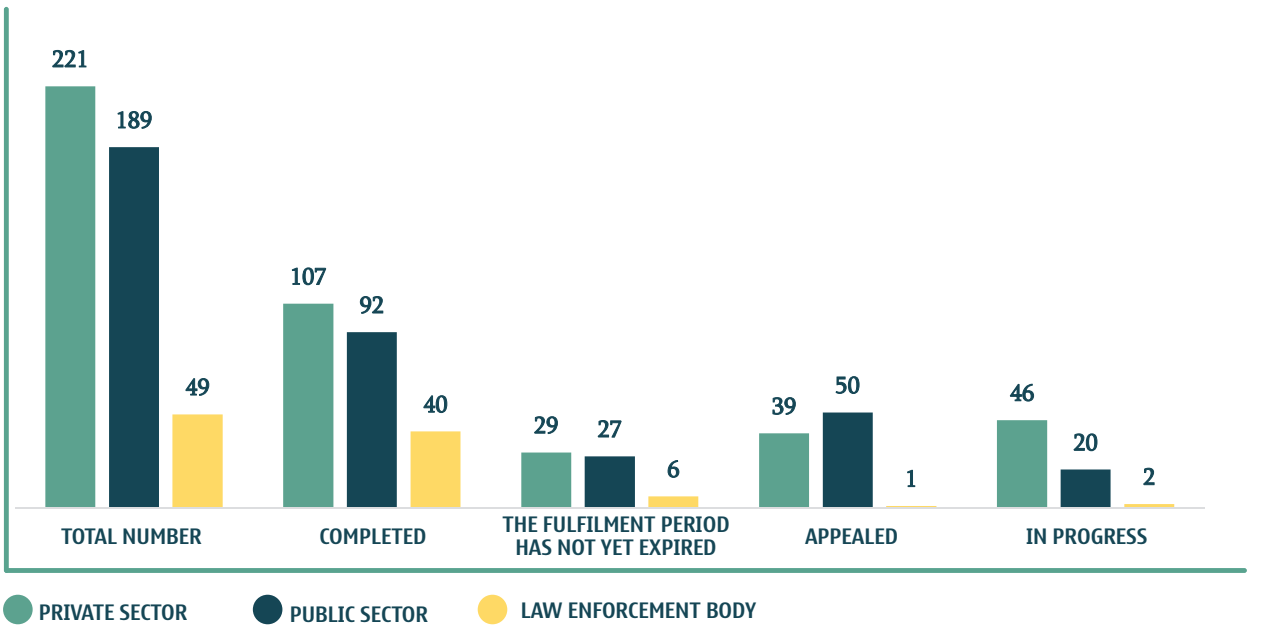
It should be noted that, compared to 2022, the rate of instructions and recommendations has increased. In particular, in 2022 the Service issued 217 instructions and 5 recommendations.

FULFILMENT RATE OF INSTRUCTIONS ISSUED BY THE SERVICE

It should be noted that 52% (239) of the 459 Instructions have been fully completed, 13% (62) have not yet expired, 20% (90) have been appealed and 15% (68) are in progress.

It should be emphasised that, compared to 2022, the fulfilment rate of the instructions issued by the Service has increased. In particular, in 2022, 40% (87) of the instructions issued were completed .

FULFILMENT RATE OF INSTRUCTIONS ISSUED BY THE SERVICE BY SECTOR



It should be noted that during the reporting period, 48% (107) of the 221 instructions issued by the Service to private bodies have been completed, the deadline for completion has not yet expired for 13% (29), 18% (39) of the instructions issued have been appealed and 21% (46) are in the process of being implemented.

49% (92) of the 189 instructions issued to public bodies have been completed, the deadline for completion has not yet expired for 14% (27) of the instructions issued, 26% (50) of the instructions issued have been appealed and 11% (20) are in progress.

82% (40) of the 49 instructions issued to law enforcement bodies have been completed, 12% (6) of the instructions issued have not yet expired, 2% (1) have been appealed and 4% (2) are in progress.

2. Statistical Data by Field of Study

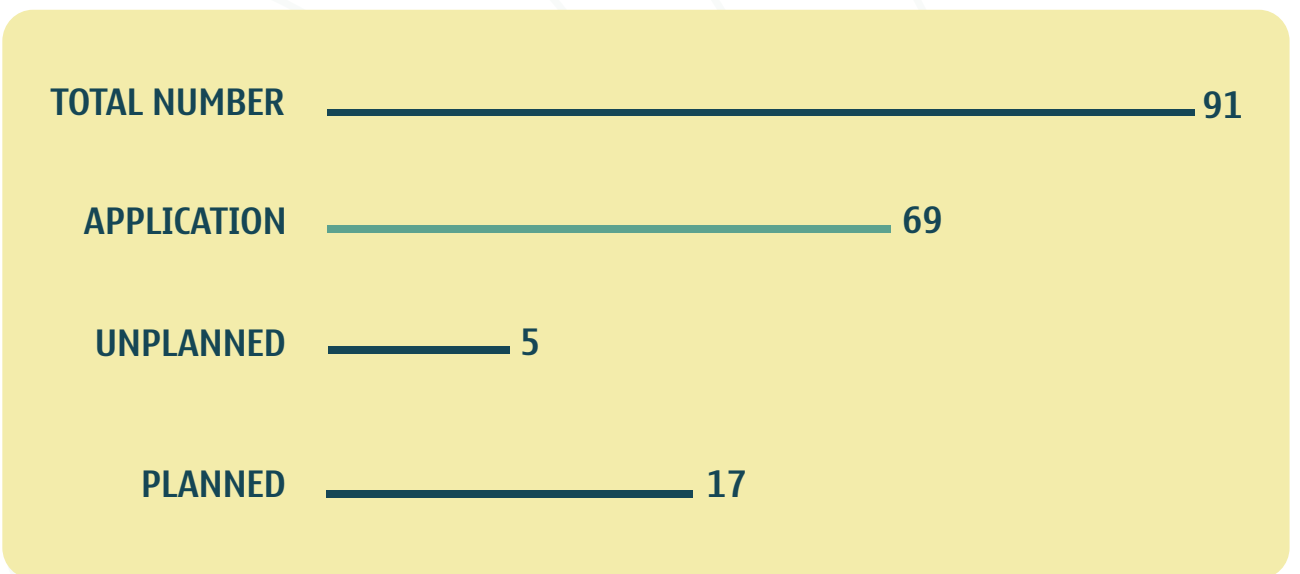
Individuals Accessing Their Own Data

In 2023, the Personal Data Protection Service examined 91 (ninety-one) cases concerning the lawfulness of the information given to individuals by various authorities, of which 17 (seventeen) were initiated by the Personal Data Protection Service, 5 (five) unplanned and 69 (sixty-nine) based on a application.

On the basis of the cases examined by the Personal Data Protection Service, 36 (thirty-six) cases of administrative responsibility were imposed. As a sanction, 17 (seventeen) subjects received a warning and 19 (nineteen) received a fine. In addition to administrative fines, the Service issued 73 (seventy-three) mandatory instructions and 1 (one) recommendation in order to improve data processing processes in public and private organisations and to ensure their compliance with the Law of Georgia "On Personal Data Protection".

In 2022, the Personal Data Protection Service examined 41 (forty-one) cases concerning the lawfulness of the information provided to an individual by various authorities. On the basis of the cases examined by the Personal Data Protection Service, administrative responsibility was imposed on 21 (twenty-one) subjects. The Service issued 24 (twenty-four) mandatory instructions.

EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS

TOTAL NUMBER	74
INSTRUCTION	73
RECOMMENDATION	1

ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	36
FINE	19
WARNING	17

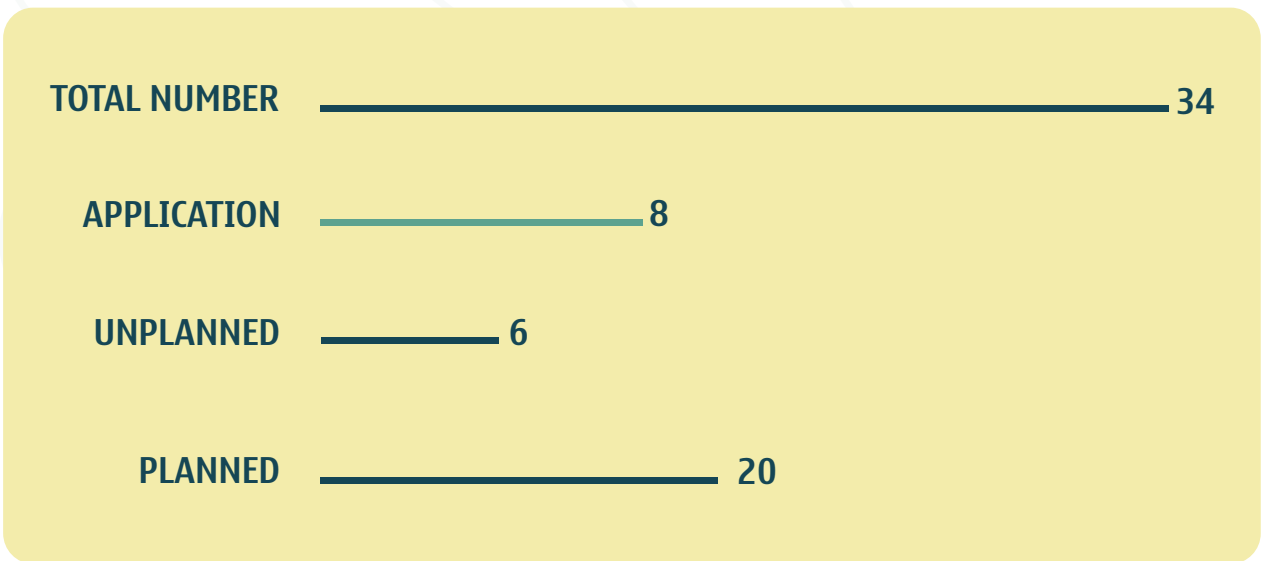
Protection of Minors' Personal Data

In 2023, the Personal Data Protection Service investigated 34 (thirty-four) cases of processing of personal data of minors, of which 20 (twenty) were carried out on the initiative of the Personal Data Protection Service, 6 (six)- unplanned and 8 (eight)- based on applications received.

On the basis of the cases examined by the Personal Data Protection Service, administrative liability was imposed on 24 (twenty-four) subjects. As a sanction, 10 (ten) subjects received a warning and 14 (fourteen) subjects received a fine. In parallel with the administrative fines, the Service issued 3 (three) recommendations and 77 (seventy-seven) mandatory instructions to improve the data processing processes in public and private institutions and to ensure their compliance with the Law of Georgia "On Personal Data Protection".

In 2022, the Personal Data Protection Service examined 39 (thirty-nine) cases of processing of personal data of minors. On the basis of the cases examined by the Personal Data Protection Service, administrative liability was attributed to 19 (nineteen) subjects. The Service issued 2 (two) recommendations and 44 (forty-four) mandatory instructions.

EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS

TOTAL NUMBER	80
INSTRUCTION	77
RECOMMENDATION	3

ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	24
FINE	14
WARNING	10

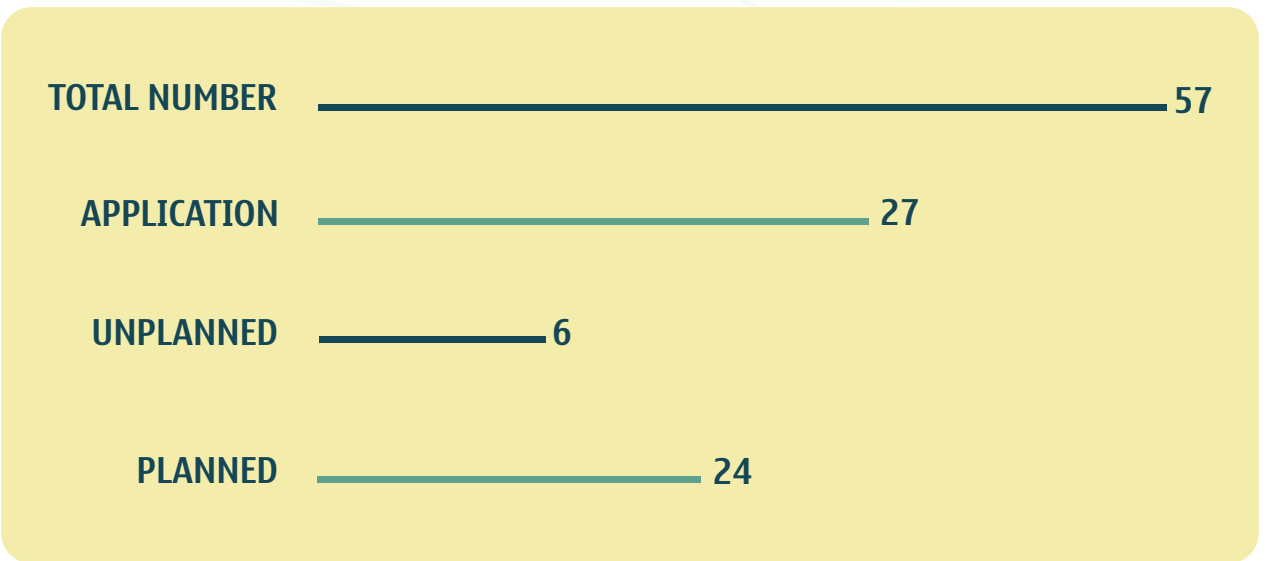
Protection of Personal Data in the Field of Labour Relations/Employment

In 2023, the Personal Data Protection Service examined 57 (fifty-seven) cases of processing of personal data in the context of the employment context, of which 24 (twenty-four) were at the initiative of the Service, 6 (six)- unplanned and 27 (twenty-seven)- at the request of citizens.

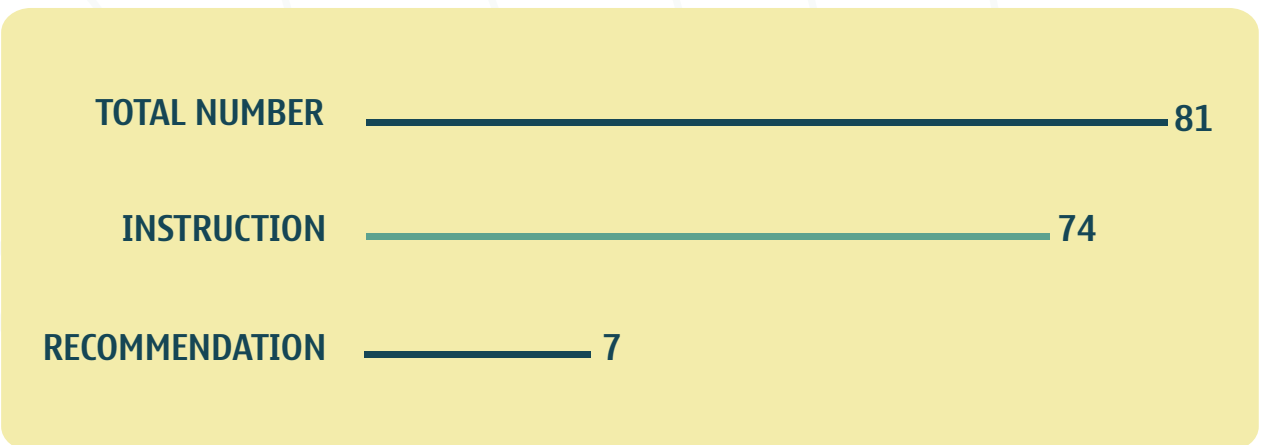
On the basis of the cases examined by the Personal Data Protection Service, 26 (twenty-six) subjects were referred to administrative responsibility. As a sanction, 6 (six) subjects received a warning and 20 (twenty) subjects received a fine. In addition to the administrative sanctions, the Service issued 7 (seven) recommendations and 74 (seventy-four) mandatory instructions in order to improve the data processing processes in public and private institutions and to ensure their compliance with the Law of Georgia "On Personal Data Protection".

In comparison with 2022, there has been an increase in the number of investigations into the processing of personal data in the context of employment relationships. In particular, in 2022, the Service examined a total of 18 cases. Administrative responsibility was applied to 14 (fourteen) cases. In addition, the Service issued 27 (twenty-seven) mandatory instructions.

EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	26
FINE	20
WARNING	6

Video Surveillance

In 2023, the Service examined 65 (sixty-five) cases of video monitoring in public and private institutions. 18 (eighteen) of them were carried out on the initiative of the Personal Data Protection Service, 21- unplanned and 26- on the basis of applications.

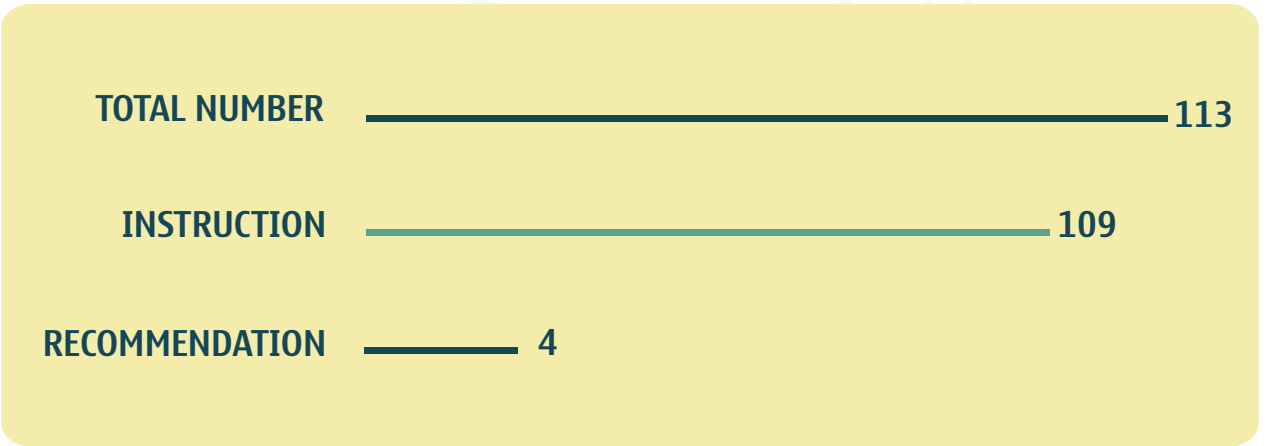
On the basis of the cases examined by the Personal Data Protection Service, 42 subjects were imposed with administrative liability. As a sanction, 25 (twenty-five) subjects received a warning and 17 (seventeen) subjects received a fine. In parallel with administrative sanctions, the Service issued 4 (four) recommendations and 109 (one hundred and nine) mandatory instructions in order to improve data processing processes in public and private institutions and to ensure their compliance with the Law of Georgia "On Personal Data Protection".

In 2022, the Personal Data Protection Service examined 46 (forty-six) cases of video surveillance, and administrative responsibility was imposed on 28 (twenty-eight) subjects. The number of mandatory instructions issued was 61 (sixty-one) and the number of recommendations was 4 (four).

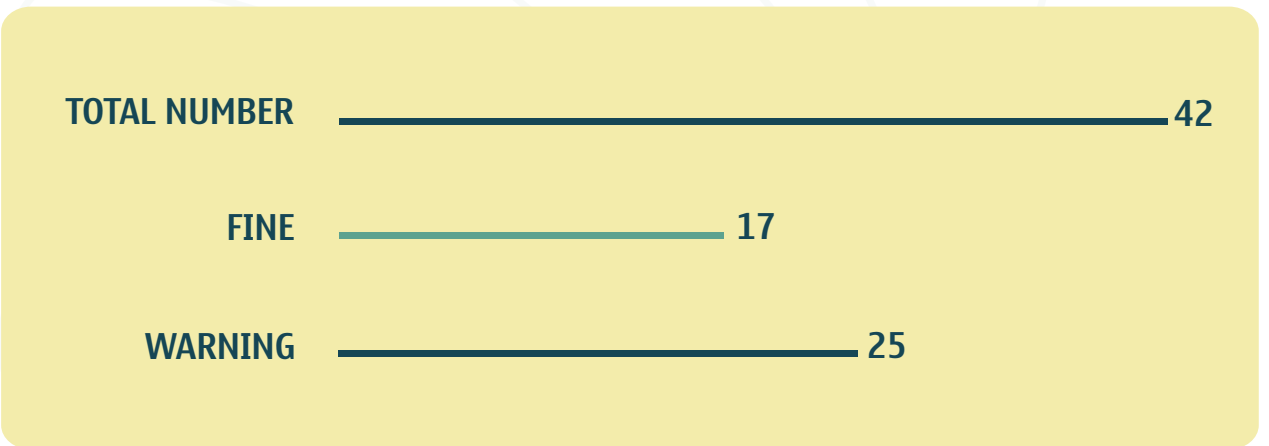
EXAMINATION/INSPECTION

TOTAL NUMBER	65
APPLICATION	26
UNPLANNED	21
PLANNED	18

INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS



Processing of Personal Data in the Health Sector

In 2023, the Personal Data Protection Service examined 15 (fifteen) cases of data processing in the health care sector, of which 7 (seven) were carried out on the initiative of the Personal Data Protection Service, 4- unplanned and 4- based on applications from citizens.

On the basis of the cases examined by the Personal Data Protection Service, 18 (eighteen) subjects were found to be administratively responsible. As a sanction, 4 (four) subjects received a warning and 14 (fourteen)- received a fine. In addition to administrative fines, the Service issued 35 (thirty-five) compulsory instructions and 1 (one) recommendation in order to improve data processing processes in public and private organizations and to ensure their compliance with the Law of Georgia "On Personal Data Protection".

In 2022, the Personal Data Protection Service examined 12 (twelve) cases of data processing in the healthcare sector. On the basis of the cases examined by the Personal Data Protection Service, administrative responsibility was imposed on 9 (nine) subjects. The service issued 22 (twenty-two) mandatory instructions.

EXAMINATION/INSPECTION

TOTAL NUMBER	15
APPLICATION	4
UNPLANNED	4
PLANNED	7

INSTRUCTIONS AND RECOMMENDATIONS

TOTAL NUMBER	36
INSTRUCTION	35
RECOMMENDATION	1

ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	18
FINE	14
WARNING	4

Processing of Personal Data in the Financial Sector

In 2023, the Personal Data Protection Service examined 41 (forty-one) cases of processing of personal data in the financial sector, of which 5 (five) were carried out on the initiative of the Service, 9- unplanned, and 32- on the basis of citizens' applications.

On the basis of the cases examined by the Personal Data Protection Service, 18 (eighteen) cases of administrative responsibility were issued. As a sanction, 2 (two) subjects received a warning and 16 (sixteen) subjects received a fine. In addition to administrative fines, the Service issued 24 (twenty-four) mandatory instructions to improve the data processing processes in private organizations and ensure their compliance with the Law of Georgia "On Personal Data Protection".

Compared to 2022, the rate of examining the lawfulness of the processing of personal data in the financial sector has increased. In particular, in 2022, the Service examined 17 (seventeen) cases. On the basis of the cases investigated by the Personal Data Protection Service, administrative responsibility was imposed on 9 (nine) subjects. The authority issued 11 (eleven) mandatory instructions.

EXAMINATION/INSPECTION

TOTAL NUMBER	41
APPLICATION	32
UNPLANNED	9
PLANNED	5

INSTRUCTIONS

INSTRUCTION	24

ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	18
FINE	16
WARNING	2

Data Security

In 2023, the Personal Data Protection Service examined 90 (ninety) cases related to data security, of which 44 (forty-four) were carried out on the initiative of the Personal Data Protection Service, 19 - unplanned and 27- based on applications from citizens.

On the basis of the cases investigated by the Personal Data Protection Service, 84 (eighty-four) subjects were imposed with administrative liability. As a sanction, 30 (thirty) subjects received a warning and 54 (fifty-four) subjects received a fine. In parallel with the administrative fines, in order to improve the data processing processes in public and private institutions and to ensure their compliance with the Law of Georgia "On Personal Data Protection", the Service issued 4 (four) recommendations and 155 (one hundred and fifty-five) mandatory instructions.

Compared to the previous year, the number of cases examined on data security issues almost doubled. In particular, the Personal Data Protection Service investigated 47 (fifty-seven) cases related to data security in 2022. On the basis of the cases examined by the Personal Data Protection Service, administrative responsibility was imposed on 39 (thirty-nine) subjects. The Service issued 6 (six) recommendations and 105 (one hundred and five) mandatory instructions.

EXAMINATION/INSPECTION

TOTAL NUMBER	90
APPLICATION	27
UNPLANNED	19
PLANNED	44

INSTRUCTIONS AND RECOMMENDATIONS

TOTAL NUMBER	159
INSTRUCTION	155
RECOMMENDATION	4

ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	84
FINE	54
WARNING	30

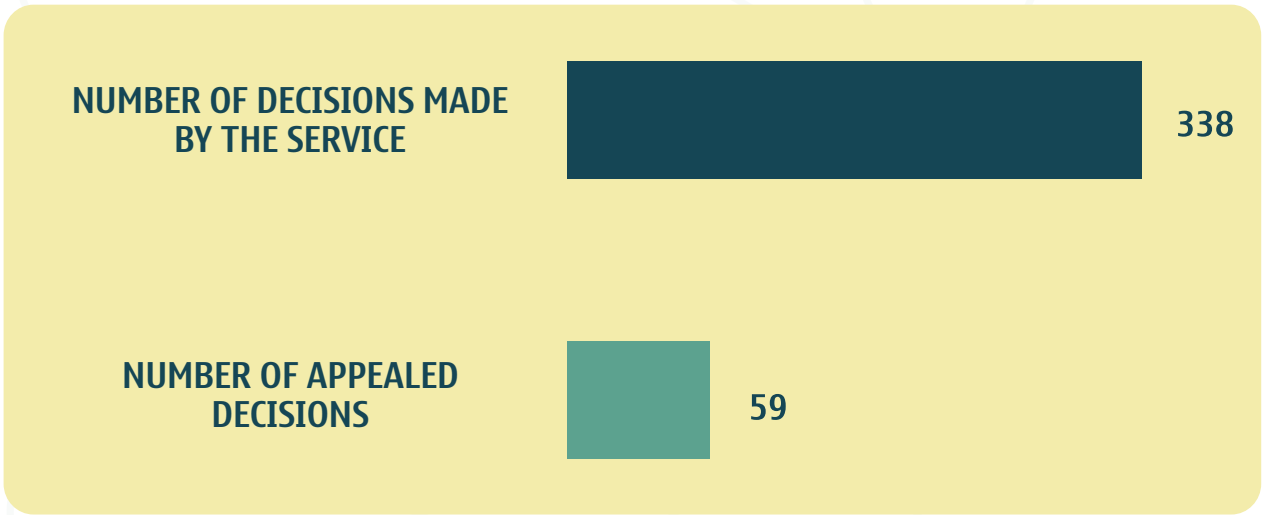
ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

TOTAL NUMBER	19
FINE	13
WARNING	6

3. OTHER STATISTICAL DATA

The Service provided a total of 5106 consultations on monitoring the lawfulness of the protection of personal data and other legal issues. It should be noted that in 2022 the Personal Data Protection Service gave a total of 3292 consultations.

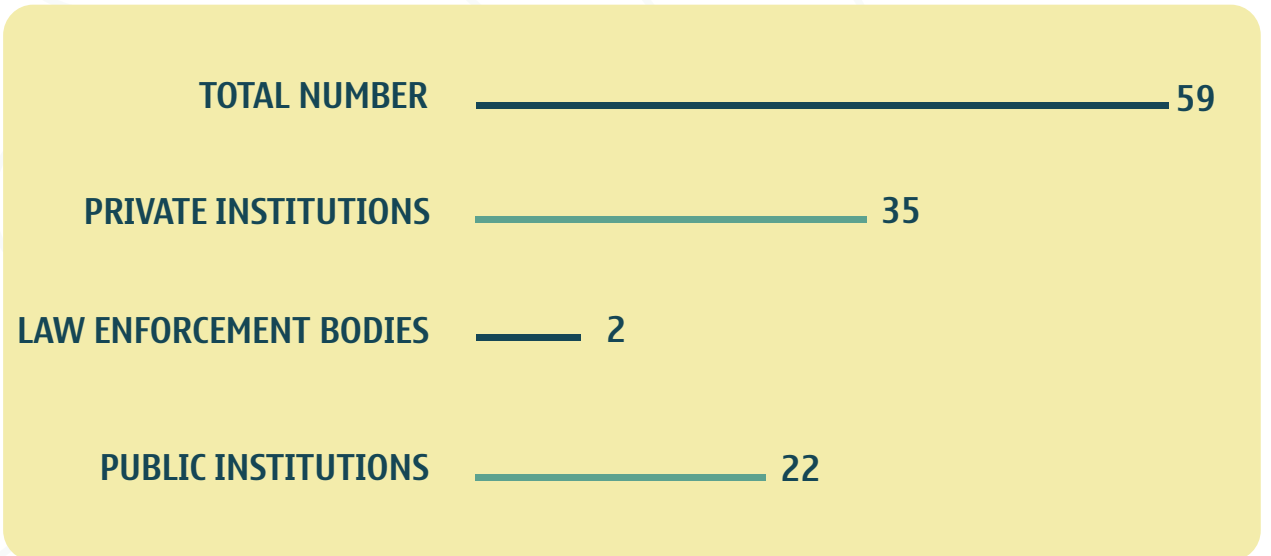
THE RATE OF COURT APPEALS AGAINST DECISIONS OF THE SERVICE



It should be noted that 17% (59) of the 338 decisions issued during the reporting period were appealed.

In 2022, 17% (41) of the 242 decisions issued during the reporting period were appealed.

RATE OF DECISIONS OF THE SERVICE APPEALED BY SECTORS



Of the 59 decisions appealed during the reporting period, 59% (35) were related to private institutions, 4% (2) to law enforcement agencies, and 37% (22) to public institutions.

In 2022, 41% (17) out of the 41 decisions appealed concerned the private entities, 34% (14) - law enforcement bodies and 25% (10) of appeals were to the decisions taken towards the public entities.

PUBLIC AWARENESS-RAISING, INFORMATION MEETINGS AND TRAININGS

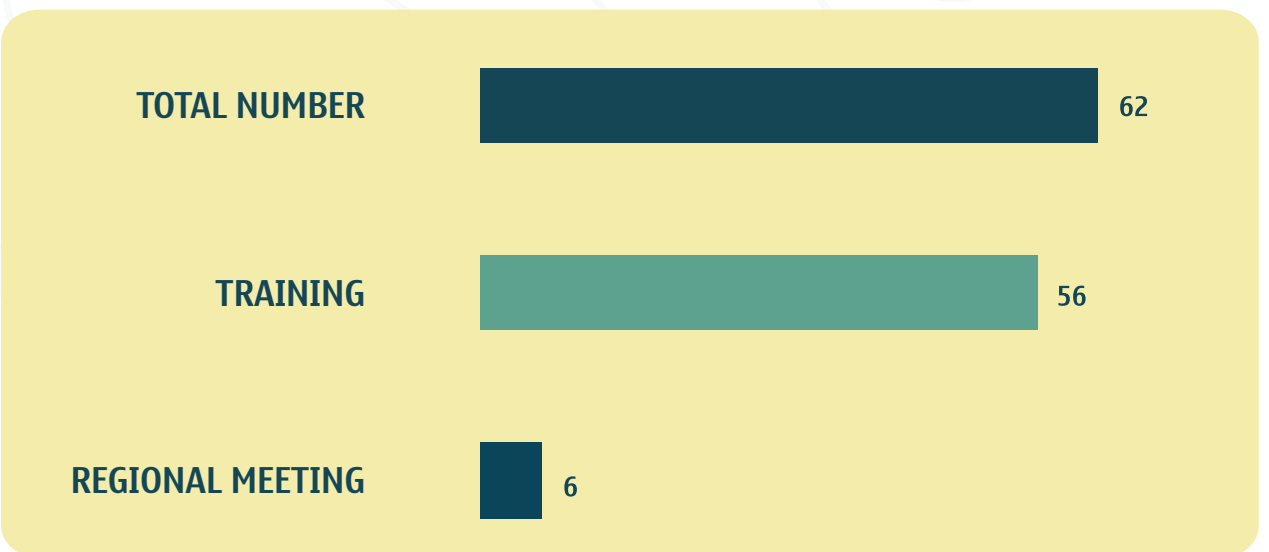
3158

The Service actively carries out educational activities on issues related to data processing and protection. In order to raise awareness of data protection, the Service systematically organises public lectures, information meetings and training sessions for representatives of the private and public sectors and law enforcement agencies.

During the reporting period, the Service held 62 meetings with 3158 participants, part of them represented both data subjects and data controllers.

It should be noted that there has been an increase in the number of training sessions in comparison with 2022. In particular, in 2022, the Service organised 36 meetings with 1007 participants.

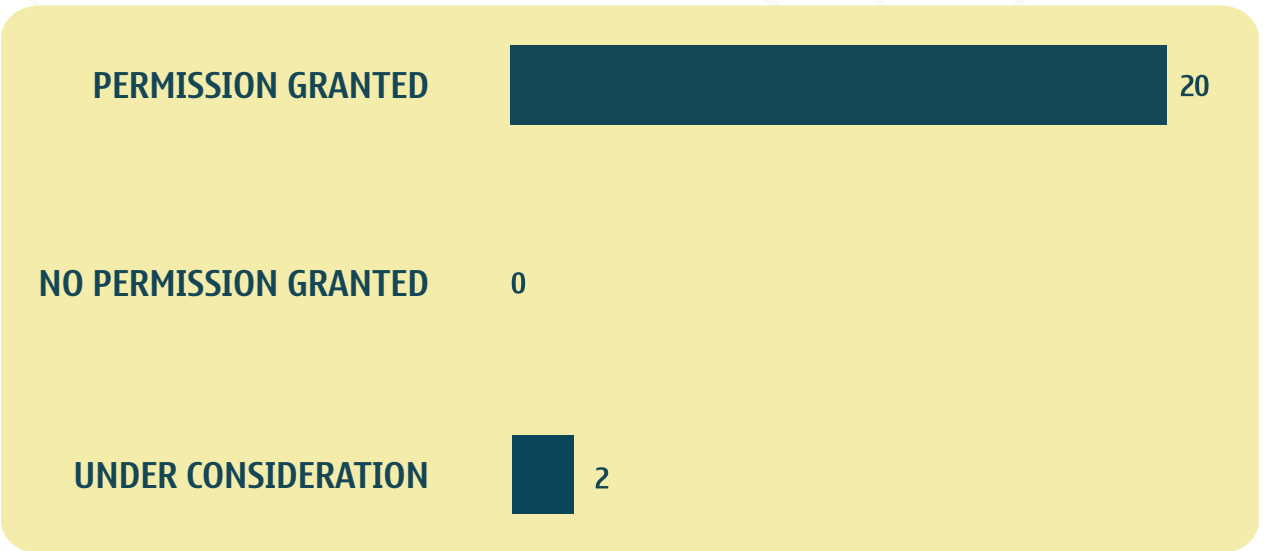
NUMBER OF INFORMATIONAL MEETINGS AND TRAININGS



In 2023, out of 62 meetings, 90% (56) were training meetings and 10% (6) were regional meetings.

In 2022, out of 36 meetings, 78% (28) were trainings and 22% (8) were regional meetings.

INTERNATIONAL TRANSFER OF DATA



As of 31 December 2023, the proceedings was completed for 20 applications and permission to transfer data had been granted for all of them, while the Service has not completed the review of 2 applications.

In 2022, the proceedings was completed for 3 applications all of which were authorized for data transmission, while the Service has not completed the review of the 1 application.

LEGAL EXPERTISE OF DRAFT INTERNATIONAL TREATIES AND AGREEMENTS

12

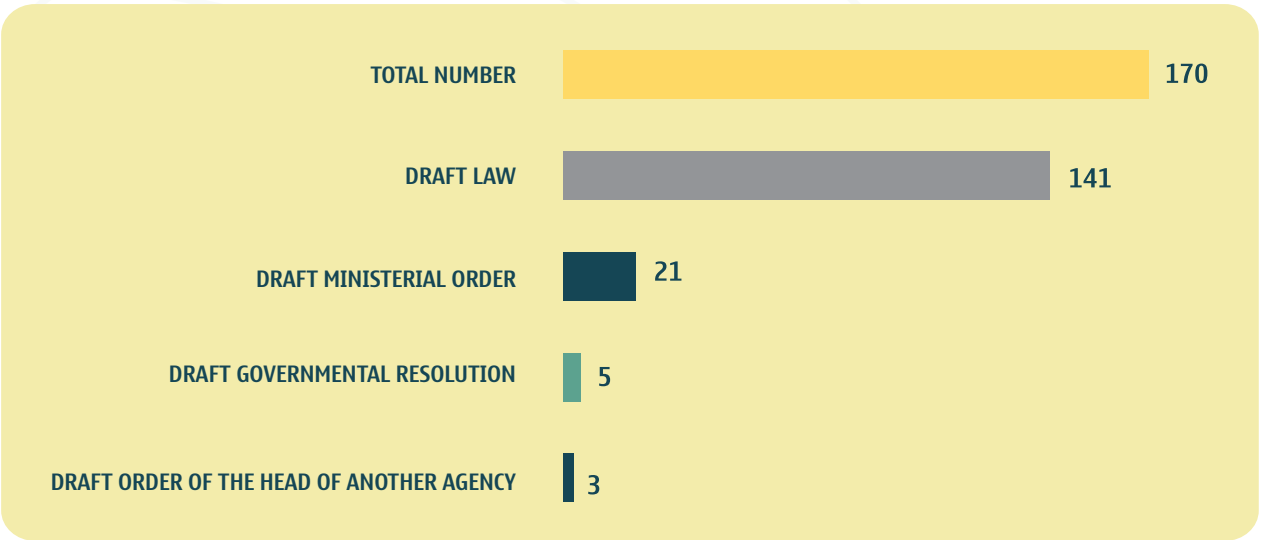
During the reporting period, the Service conducted a legal expertise of 12 draft international treaties and agreements signed on behalf of Georgia, within which no recommendations were issued by the Service.

As part of the legal examination, the Service will study the draft of the presented international agreement, the legal arrangement, and the institutional mechanisms of personal data protection in the contracting state. Based on this study, a recommendation to make changes to the

draft will be issued. It should be noted that, during the reporting period, no recommendations were issued on the drafts of international agreements and treaties examined by the Service.

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 six cases.

TYPES OF ACTS ON WHICH THE SERVICE CONDUCTED LEGAL EXPERTISE

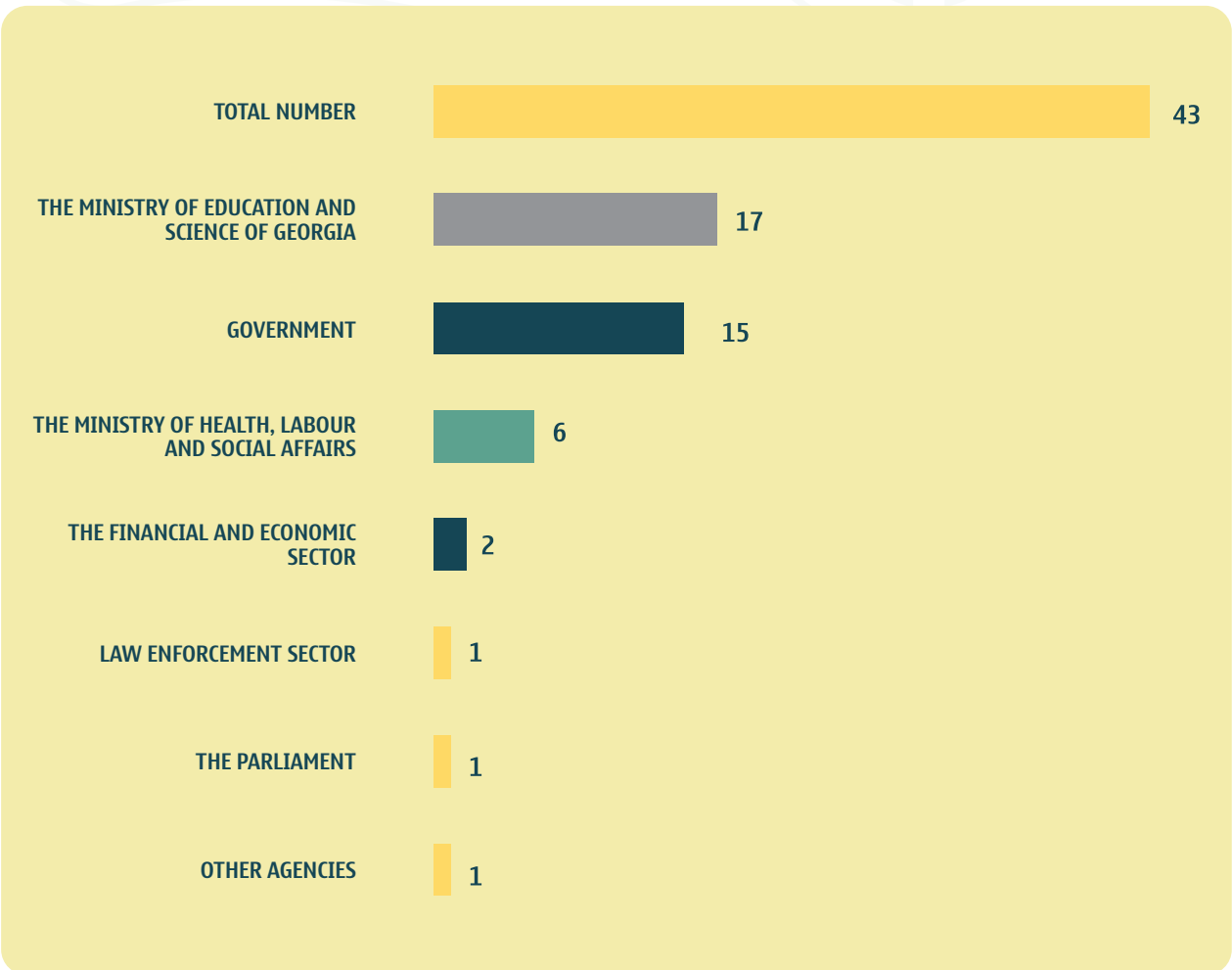


In order to ensure a high standard of personal data protection, based on the request of other agencies, the Personal Data Protection Service conducts a legal examination of draft legislative and bylaw acts.

During the reporting period the Service assessed the compliance of 141 draft laws, 21 draft ministerial orders, 5 draft governmental resolutions and 3 draft order of the Head of another authority with the Law of Georgia "On Personal Data Protection".

In 2022, 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".

AGENCIES THAT HAVE APPLIED TO THE SERVICE FOR CARRYING OUT LEGAL EXPERTISE



NUMBER OF REQUESTS RECEIVED RELATED TO THE ACCESS TO PUBLIC INFORMATION

TOTAL NUMBER	116
COMPLETELY SATISFIED	86
UNSATISFIED	30

From 11 December 2022 to 10 December 2023, the Personal Data Protection Service received 116 requests related to the access to public information, and in 86 of the cases the requests were fully satisfied and 30 were not, because:

- ***In 16 cases, the requested information was not recorded by the Personal Data Protection Service;***
- ***In 14 cases, the requested information was not stored at Personal Data Protection Service.***[6]

6 [6] 2023 Report on ensuring access to public information by the Personal Data Protection Service, <www.matsne.gov.ge>.

COMPLAINTS RECEIVED BY THE SERVICE REGARDING THE DECISIONS OF THE SERVICE

20

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, 20 decisions of the Head of the structural unit were appealed to the Service. In all 20 cases, the Service upheld the decision taken by the Head of the structural unit of the Service.

In 2022, 10 decisions of the Head of the structural unit were appealed to the Service.

LAW-MAKING ACTIVITY

11

In order to ensure the high quality of the work of the Personal Data Protection Service and its institutional development, the Service developed 11 bylaws.

In 2022, the Service developed 11 bylaws.

Annex №2: Publicly Available Information on Funding and Financial Estimate of the Personal Data Protection Service of Georgia

The List of Vehicles on the Balance Sheet of the Service, Indicating the Model and the Year of Manufacturing:

№	NAME OF VEHICLE	THE YEAR OF MANUFACTURE
1	KIAOPTIMA; LG917GL	2014
2	HONDACRV;OO781GG	2013
3	TOYOTACAMRY; PP643FF	2019
4	HYUNDAIACCENT WW825UW	2021
5	HYUNDAIACCENT WW816UW	2021
6	HYUNDAIACCENT WW817UW	2021
7	FIAT TIPO BB846YY	2022
8	HYUNDAI ELANTRA GG293GR	2023
9	HYUNDAI ELANTRA; GG291GR;	2023
10	MITSUBISHI L200; MI554MM	2023

The total public procurement in 2023 amounts to GEL 1 102 500, including the public procurement of GEL 1 042 182 for the full operation of the Service and that of GEL 60 318 for representation expenses.

It should be noted that public procurement in 2022 amounted to GEL 657 500, including public procurement of GEL 607 450 for the full operation of the Service and that of GEL 50 050 for representation expenses.

ADDRESS: 7, N. VACHNADZE STR., 0105, TBILISI, GEORGIA
48 BAKO STR. 6010, BATUMI, GEORGIA

TEL.: (+995 32) 242 1000
E-mail: office@pdps.ge
www.pdps.ge