PERSONAL DATA
PROTECTION SERVICE

2024 ACTIVITY REPORT OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

On the State of Data Protection in Georgia, the Conduct of Covert Investigative Actions, and the Control of Activities Related to the Central Bank of Electronic Communications Identification Data

2024

WWW.PDPS.GE

PERSONAL DATA
PROTECTION SERVICE

2024 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.

Also, in accordance with Article 169, Paragraph 2 of the Rules of Procedure of the Parliament of Georgia, the President of the Service shall submit to the Parliament of Georgia, once a year, a report on the results of the oversight of the investigative actions provided for in Articles 136–138 of the Criminal Procedure Code of Georgia, as well as the covert investigative actions stipulated in subparagraphs "a" and "b" of Part 1 of Article 143[1] of the same Code. The Bureau of the Parliament shall forward this report to the relevant committee and the Trust Group of the Parliament.

The following report contains details of the Service's activities conducted from January 1, 2024, to December 31, inclusive, in compliance with the prevailing legislation during the reporting period.

Table of Contents

Foreword of the President of the Personal Data Protection Service of Georgia 5

Chapter I. The State of Personal Data Protection in Georgia 8

1. Data Processing Within the Public Sector 8
    1.1. Important Directions and Trends 9
    1.2. Case Law 19
    1.3. Instructions and Recommendations 25
2. Data Processing in the Private Sector 27
    2.1. Key Directions and Trends 27
    2.2. Case Law 42
    2.3. Instructions and Recommendations 44
3. Data Processing by Law Enforcement Bodies 47
    3.1. Key Directions and Trends 47
    3.2. Case Law 51
    3.3. Instructions and Recommendations 56
4. Planned Inspection on the Lawfulness of Data Processing 58
    4.1. Key Directions and Trends 58
    4.2. Case Law 65
    4.3. Instructions and Recommendations 73

Chapter II. Monitoring of the Covert Investigative Actions and the Activities Carried Out at the Central Databank of the Electronic Communication Identification Data 76

1. Key Directions and Trends 76
2. Decisions 79
3. Instructions and Recommendations 80
4. Statistical Data 81

Chapter III. Enhancing Public Awareness and Educational Activities 88

1. Awareness-raising Activities 88
2. Conducted Trainings and Public Lectures 94

Chapter IV. Administrative Management of the Service 96

1. Issues of Organisational Management of the Service 96
    1.1. Institutional Strengthening and Internal Organization of the Service 96
    1.2. Enhancing Employee Qualifications and Organizational Ethics 98
2. Budget and Performance of the Personal Data Protection Service of Georgia 99
    2.1. Budget and Performance of the Personal Data Protection Service of Georgia 99
    2.2. Salary, Bonus and Monetary Reward 100
    2.3. Vehicles 100
    2.4. Real Estate Included In the Balance Sheet of the Service 100
    2.5. Business Trips and Other Expenses 101

Annex №1: Compliance of the Law of Georgia "On Personal Data Protection" with the European Union's Data Protection Legal Framework 104

Annex №2: Statistical Data 138

Annex №3: Publicly Available Information on Funding and Financial Estimate of the Personal Data Protection Service of Georgia 165

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

On behalf of the Personal Data Protection Service of Georgia, I am pleased to present the Annual Report on the activities of the Service for 2024. The past year marked a significant milestone in aligning national data protection legislation with European standards. Since March 2024, the Law of Georgia "On Personal Data Protection" has entered into force, establishing essential safeguards for the effective protection of data subjects' rights and freedoms. This legislation also strengthens the mandate of the independent supervisory authority by equipping it with the necessary powers and mechanisms to carry out its functions effectively. In the context of Georgia's European integration, the harmonization of national legislation with EU data protection standards—and the resulting development of Georgian law through the adoption of a new legislative framework—is particularly noteworthy.

Globally, the protection of personal data and the right to privacy remain high on the international agenda. The rapid pace of digital development and technological innovation continues to pose new and complex challenges, emphasizing the importance of international cooperation and the adoption of best practices to safeguard fundamental human rights in the digital era.

Nowadays, the legal regulation of artificial intelligence (AI) and its implications for privacy and data protection have become especially relevant. The increasing use of AI in decision-making processes presents a range of challenges related to ensuring fairness, transparency, and compliance with personal data protection principles. Key issues include profiling, risks of discrimination, the principle of data minimization, and the responsible use of algorithms. These developments call for the continuous assessment of the impact of emerging technologies on the rights and freedoms of data subjects, and the mitigation of associated risks. The Service remains actively engaged in monitoring global trends in the field of personal data protection to incorporate international best practices into our work. We are committed to continuing efforts to harmonize national standards with international norms and to ensuring the ethical and secure use of artificial intelligence in the digital age.

Accordingly, this report addresses key topical issues related to the lawfulness of data processing, including major trends and developments in data processing within both the public and private sectors. It outlines precedent-setting decisions, issued instructions, and recommendations aimed at enhancing the effectiveness of personal data protection. The report also provides information on oversight of data processing activities and covert investigative actions carried out by law enforcement bodies, as well as the activities conducted within the Central Bank of Electronic Communications Identification Data.

One of the core areas of activity for the Personal Data Protection Service of Georgia is raising public awareness. Reflecting this, the report details a range of informational initiatives undertaken to increase public understanding of personal data protection. Additionally, the report includes statistical data on the Service's activities, which—among other indicators—demonstrate growing public engagement with the Service, the extent of data processing oversight, and the results achieved.

It is noteworthy that the Personal Data Protection Service has published two significant special reports. The first, titled "Personal Data Protection Service of Georgia Special Report International Activities carried out by the Service in 2022-2024 to Implement the Best European Practices and Standards of Personal Data Protection Law," outlines the Service's participation in international forums and cooperation with counterpart supervisory authorities. The second, the "Special Report on the Activities of the Personal Data Protection Service on the Implementation of the Law of Georgia 'On Personal Data Protection,'" highlights the activities carried out and the emerging practices following the enactment of the new legislation.

The report is accompanied by an annex analyzing the compliance of the Law of Georgia "On Personal Data Protection" with EU legislation. It includes a comparative analysis of individual legal provisions in relation to the standards established by EU law. In addition, the Service has developed the "Strategy of the Personal Data Protection Service for 2025–2028," which sets forth the strategic vision and key priorities of the Service. These include fostering a culture of data protection in society, raising public awareness of the means and importance of personal data protection, enhancing the visibility and impact of the Service, strengthening both supervisory and preventive mechanisms, supporting institutional development, and expanding cooperation with personal data protection authorities of EU Member States and beyond, as well as with EU sectoral institutions and international organizations.

In conclusion, I would like to emphasize that the Personal Data Protection Service of Georgia remains committed to promoting and advancing modern European standards of personal data protection. To this end, we actively collaborate with our European counterpart authorities and international partners. The unwavering objective of the Service is to strengthen the culture of privacy and personal data protection in Georgia, in line with European values. In this context, 2024 represented a landmark year for the de lege ferenda development of national data protection legislation and the effective execution of the supervisory function by the Personal Data Protection Service. This progress lays a firm foundation for mitigating the risks associated with digital development and for further advancing data protection standards in the country.

DR. DR. LELA JANASHVILI

President of the Personal Data Protection Service of Georgia

Associate Professor at Ivane Javakhishvili Tbilisi State University

Associate Professor at the Autonomous University of Barcelona

I

The State of Personal Data Protection in Georgia

CHAPTER I: THE STATE OF PERSONAL DATA PROTECTION IN GEORGIA

1. DATA PROCESSING WITHIN THE PUBLIC SECTOR

Considering the implementation process of the Law of Georgia "On Personal Data Protection", the 2024 reporting period was marked by numerous challenges. The number of applications and notifications has increased significantly compared to previous years, and the data processing cases investigated by the Personal Data Protection Service have encompassed a range of issues covered by the Law. Public agencies have actively utilized the mechanism for notifying the Service of instances of unlawful data processing. It is noteworthy that certain innovations introduced by the Law are specifically directed at the public sector. For example, as of June 1, 2024, it has become mandatory for every public institution to appoint a personal data protection officer. Furthermore, the scale of data processing activities within each institution has necessitated the preparation of various written documents required by the Law (such as the rule on the implementation of video monitoring, the document for recording information related to data processing as stipulated in Article 28 of the Law, etc.). In addition, multiple institutions are frequently involved in a single data processing operation within the public sector, and the Law imposes an obligation on data controllers to justify the lawfulness of data processing. Moreover, public institutions are often supported by other organizations in terms of organizational and technical matters. In this context, data security has been established by the Law as one of the fundamental principles of processing, thereby significantly elevating its importance. At the same time, liability for breaches of data security has also been extended to data processors, which has contributed to the identification of violations committed by public agencies authorized to process data.

The data processing activities assessed on the basis of applications and notifications, as well as those examined on the initiative of the Service during the reporting period, encompassed the following areas: detection and management of incidents (data security breaches) and fulfillment of related notification obligations; data collection in the course of identifying and administering administrative offenses; use of video monitoring systems for such purposes; ensuring data confidentiality in labor relations and the healthcare system; data processing related to the provision of services; processing of children's data within childcare and educational institutions; appointment of personal data protection officers and related conflict of interest issues; various aspects concerning the exercise of data subjects' rights; compatibility of data processing with the principle of transparency; lawfulness of processing data of deceased persons; and other related matters.

During the reporting period, the legality of processing the personal data of various data subjects—including patients, kindergarten students, parties to disciplinary proceedings, current and former employees of agencies, socially vulnerable family members, persons with tax obligations, debtors, persons in state care, children with disabilities, and individuals subject to administrative penalties—was examined. As a result of inspections and the review of applications, various measures provided for by the Law (including instructions, recommendations, and violation protocols) were applied to the bodies of the Ministry of Education, Science and Youth of Georgia, the Ministry of Justice of Georgia, Ministry of Internally Displaced Persons from the Occupied Territories, Health, Labour and Social Affairs of Georgia, entities of the system of Ministries of Finance of Georgia, as well as judicial institutions, municipalities, and other entities.

1.1. Important Directions and Trends

a. Incident — Data Breach

During the reporting period, particular attention was given to the fulfillment of obligations related to data security breaches (incidents). The Law establishes the duties to record an incident, notify the Service, and inform the data subject. Every incident, irrespective of its nature and consequences, must be documented; however, the obligation to notify the Service and inform the data subject arises only when the incident is likely to cause significant damage and/or poses a significant threat to fundamental human rights and freedoms, with a medium or high probability.

Based on the cases reviewed, it was determined that, in instances where a non-standard volume of information is requested from databases, individual institutions do not proactively assess the impact of such suspicious actions on personal data. While they undertake certain measures to safeguard security, they simultaneously acknowledge that they cannot definitively confirm whether an incident has occurred.

In such cases, the agencies submit information regarding the alleged offense to the investigative authorities, and if the Service expresses interest in the matter, they indicate that they will respond upon the completion of the investigation and clarification of the circumstances. It is noteworthy that the improper fulfillment of the obligations imposed by the Law on data controllers and data processors cannot be justified by the initiation of an investigation. Ensuring data security requires the prompt detection of incidents and the timely implementation of necessary measures to minimize harm to the rights of data subjects, whenever possible, through reasonable and risk-appropriate organizational and technical safeguards.

A cyberattack and an incident are distinct concepts. An incident is defined as a data security breach that results in the unlawful or accidental damage, loss, unauthorized disclosure, destruction, alteration, access, collection, retrieval, or any other unauthorized processing of data. Accordingly, it is crucial for responsible public agencies to clearly differentiate between these concepts and to submit an incident report to the Service not in the case of a cyberattack per se, but specifically in instances of a data security breach. For the Service to be involved in the incident-related process, certain information must be provided, as specified by the normative act issued by the President of the Service. Additionally, the option to complete the relevant form on the Service's website is made available. During the reporting period, instances were identified where the Service was notified of an incident not by the data controller, but by another institution informed of the event. In such cases, the obligation to notify the incident cannot be considered fulfilled, since these third parties, do not possess comprehensive information regarding the data security breach, including details such as the volume of data involved, data categories, the outcomes of the incident, its status (e.g., resolved or ongoing), or whether the incident affected vulnerable groups such as minors or persons with disabilities.

The Service responds promptly to incident reports. There have been instances where the Service was notified of facts constituting unlawful data processing through incident reports, which, however, do not qualify as data security breaches (for example, a teacher who, on their own initiative and to seek advice or opinions from the public, publishes a student's personal data on a social network). Accordingly, both public awareness and the practices of public institutions face significant challenges concerning the understanding and handling of incidents.

b. Personal Data Protection Officer

The appointment or designation of a personal data protection officer and the proper fulfillment of other obligations set forth in Article 33 of the Law remains one of the key problematic issues. In 2024, based on both inspections and applications, dozens of data controllers and data processors were examined, including general educational institutions and municipal bodies (such as Tbilisi City Assembly and City Hall). The decisions issued by the President of the Service concerned executive authorities, legal entities of public law, and others. In most cases, the assessment focused on the following: compliance with the obligation to appoint or designate a personal data protection officer; issues related to conflict of interest; the officer's appropriate knowledge of the field of data protection; provision of the officer's identification and contact information to the Service; and the proactive publication of such information through various channels.

During the reporting period, more than ten cases of non-fulfillment of the obligation to appoint a personal data protection officer were identified. Additionally, despite the legislative requirement,[1] in some instances the Service was not informed about the appointment of a personal data protection officer. The majority of institutions did not indicate the identity of the officer on their official websites, or the information was published in a manner that was difficult for the public to access; meanwhile, institutions without websites failed to publish information about the officer through any alternative means.

Among the institutions inspected by the Service that chose to appoint a personal data protection officer by assigning the role to an existing employee, one of the most significant issues identified was the conflict of interest. In most cases, the designated officer assumed the role in addition to their existing duties. The Service examined several cases in which it was revealed that the responsibilities of the personal data protection officer were combined with those of the head of a decision-making structural unit and/or with employees responsible for managing human resources, carrying out pedagogical activities, organizing administrative proceedings, overseeing organizational matters, managing state procurement, handling inventory procedures, representing the employer in court, and similar functions. These activities are inherently linked to making or influencing decisions regarding the purposes and means of personal data processing, thereby creating a conflict of interest with the responsibilities of the officer.

The personal data protection officer is responsible for ensuring the lawful conduct of data processing activities and, therefore, must possess appropriate knowledge in the field of data protection. In light of the challenges associated with finding qualified personnel, it is important to note that a range of guidelines, recommendations, rules, and instructions are available on the Service's official website, enabling interested parties to acquire the necessary knowledge in the field of data protection. In addition, the Service conducts consultations in various formats, and a number of normative acts are also publicly accessible.

In addition, although the personal data protection officer represents the institution in its interactions with the Service, the examination of the legality of specific data processing activities has shown that, in order to accurately and effectively present technical, organizational, or legal

[1] Law of Georgia "On Personal Data Protection," Article 33, Paragraph 8.

information related to the processes under assessment, it is important for institutions to ensure the participation of employees with relevant competence and experience alongside the officer and/or their involvement in the proceedings as witnesses during discussions and inspections conducted by the Service.

c. Data Security

"To ensure the security of data, technical and organisational measures shall be taken during the processing of data to ensure appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction and/or damage"[2]. In addition, it is important to anticipate the risks of accidental data disclosure in advance and to select measures that are proportionate to those risks. In this context, one of the challenges lies in the organizational and technical setup of citizen service areas. Frequently, in such spaces, under conditions of so-called live queues, communication involves the use of sensitive data, thereby increasing the risk of accidental information disclosure. However, with appropriate effort and proper planning of the service process, such disclosures can be prevented—for example, by modifying or reorganizing the physical space, introducing an effective queue management system, and providing employees with clear and specific instructions.

Data processing operations are rarely fully automated. It is essential that they are carried out with the involvement of personnel employed within institutions. As in previous years, during the reporting period, institutions frequently attributed cases of unlawful data processing to the actions of their employees. However, providing only general instructions to employees, without informing them about appropriate organizational and technical safeguards or data protection obligations, often results in violations of the Law. Moreover, the imposition of disciplinary measures on an employee cannot serve as a basis for exempting institutions from liability. It is the responsibility of data controllers and data processors to consider potential risks and threats and to implement appropriate measures to ensure the lawful conduct of data processing, particularly in the context of personnel changes and process planning.

Within the framework of inspections conducted by the Service, instances were identified where employees used their access to data stored in electronic systems for non-official purposes, as well as cases where an employee who had not been assigned a specific user account within the electronic system accessed data. According to the Law of Georgia "On Personal Data Protection", for the purpose of ensuring data security, every employee is obligated not to exceed the scope of authority granted to them and to maintain the secrecy and confidentiality of data. The existence of such challenges is primarily linked to the absence of an effective monitoring and control mechanism. Accordingly, beyond ensuring that employees are thoroughly informed about data protection and the measures required upholding it, it is essential for public institutions to implement appropriate monitoring mechanisms for data processing activities that are effective in detecting and preventing incidents of unlawful data processing.

[2] **Law of Georgia "On Personal Data Protection," Article 4, Paragraph 1, Subparagraph "f".**

One of the inspections revealed that the use of personal email addresses by employees of a public institution for official purposes resulted in the accidental disclosure of a substantial volume of health data to an unauthorized individual. The use of personal email accounts (such as Google email addresses) increases the risk of unlawful data processing, with the scale and severity of potential negative consequences depending on factors including the type of data involved and the frequency of information exchange. Personal email, from the perspective of data security, differs significantly from work email. For instance, an employer cannot exercise control over personal email accounts, which limits the institution's ability to take effective measures regarding the further storage or potential use of personal information obtained through such means—even in the event of the employee's dismissal. Accordingly, explanations provided by public agencies citing challenges related to work email, such as technical malfunctions and/or insufficient storage capacity, cannot be regarded as objective circumstances that justify non-compliance with the obligations imposed by the Law.

In most cases, data processing is conducted through electronic systems, reflecting modern technological advancements. Similar to the previous year, during the current reporting period, a recurring issue was identified in several case studies concerning the method of recording actions performed on data within electronic systems managed and administered by various agencies (commonly referred to as "logging"). Pursuant to the Law of Georgia "On Personal Data Protection", both the data controller and the data processor are obligated to ensure comprehensive logging. This enables the timely and effective detection of unauthorized access, accurate identification of the content, timing, and identity of the individual performing the action, and the appropriate response to such incidents.

Public institutions utilize official websites to provide certain information to their target audiences. During the reporting period, the Service identified data processing through public publication as a significant challenge. Publication represents a particularly sensitive form of data processing, where unlawful processing often results in irreversible harm. Accordingly, the timing of data disclosure must be carefully considered, which is frequently problematic in cases of proactively published personal data. The existence of a legal basis for initiating data processing does not guarantee the continued legitimacy of that basis throughout the entire processing lifecycle. Institutions often attribute the presence of outdated data on websites to technical malfunctions of electronic resources, the need for system updates, and/or personnel changes. To prevent unlawful data processing, it is essential that responsible persons periodically review the content published on websites, evaluate the legitimate interests in publicly disclosing each document containing personal data, and, despite organizational and technical challenges, remove unlawfully disseminated information.

d. Data Processing in Compliance with the Principle of Transparency

The principle of transparency is achieved through the effective provision of information to data subjects, which is often not perceived as a proactive obligation by data controllers. It must be clear to data subjects that data concerning them is being processed. They must be informed of the purposes, scope, means, and methods of processing in order to understand the associated risks and, where necessary, to exercise their rights.

Information on data processing should be presented clearly and be easily accessible to the widest possible range of individuals, placed in a specific and easily visible location. Where appropriate, visual materials, the official website, and other channels may be used to facilitate access to this information. Compliance with this principle is particularly important when the number of data subjects or potential data subjects is large and the data processing activities are diverse in nature. In such cases, the issue of inadequate implementation of the principle of transparency was identified in a number of inspections.

Although the legal basis for data processing in public institutions is most often established by legislation, the information contained in legal acts is frequently insufficient to fully uphold the principle of transparency. Accordingly, a key challenge in implementing the new principle introduced by the Law lies in identifying mechanisms through which data subjects can be properly and proactively informed. This often involves amending existing legal acts, drafting additional documents, and/or delivering information to the public through appropriate means.

In response to the measures taken by the Service, public institutions have developed relevant documentation to support the principle of transparency, and information about these efforts has been communicated to the public through various means.

Numerous special visual warning signs have been installed throughout the Tbilisi Municipality to inform the public about the implementation of video monitoring by the Municipality. As a result, it will no longer come as a surprise to the public that video camera recordings may be used as evidence in cases of certain administrative violations.

One of the issues that drew attention during the reporting period was the confusion between two distinct concepts in data processing: informing the data subject and obtaining the data subject's consent. Informing serves to uphold the principle of transparency and can be carried out through various procedures. For example, when data is collected directly from the data subject, data controllers have specific obligations, and when data is not collected directly from the subject, the information must still be provided to them—subject to certain exceptions. The data subject is not required to sign the documents shared for the purpose of informing, and the absence of a signature does not mean that the obligation to inform has not been fulfilled. Consent, on the other hand, constitutes a legal basis for data processing. It reflects a unilateral expression of will and must be given either by signing a document or through another form of clear expression. For consent to be valid, the content to which the individual agrees is of primary importance. Moreover, when consent is included as part of lengthy legal documents—such as multi-point terms of service, loan agreements, or other contracts—the voluntary nature of consent must not be overshadowed or absorbed by the complexity of the legal text. During the reporting period, it became evident that many data controllers were not fully familiar with the

mandatory elements of data subject consent as defined by the current version of the Law, and in many cases, consent was incorrectly treated as the legal basis for data processing.

e. Exercise of Data Subject Rights

Given the broad scope of the concept of personal data, correctly identifying certain types of information as personal data remains a challenge for both data subjects and data controllers. The concept of personal data encompasses not only identifying, contact, banking, or other information about an individual, but also includes the behavior of the data subject, related opinions and assessments, as well as the person's psychosocial or physical characteristics. Proper identification of what constitutes personal data is essential for ensuring the lawful conduct of data processing activities and for the effective realization of data subjects' rights

There are frequent instances in which individuals, by contacting the Service, seek to obtain information about third parties under the pretext of exercising their right to access personal data. However, responding to such requests falls outside the scope of the Service's competence when the information in question does not constitute the personal data of the requesting data subject.

During the reporting period, data subjects frequently exercised their rights to receive information, access data, and request copies, as provided for in Articles 13 and 14 of the Law. However, an assessment of the legitimacy of responses revealed that issues related to incomplete retrieval or delivery of information and documentation by public institutions were primarily attributable to inadequacies in the search functions of electronic systems. In some cases, a low level of organizational culture regarding the proper protection of data subject rights was also observed, which further impeded the effective exercise of these rights.

In the context of developing effective mechanisms for the realization of data subject rights, it is important to highlight the obligation established by Article 26 of the Law[3], which requires the integration of data protection standards into service processes as a means of ensuring the effective exercise of these rights.

The right to information of a data subject is not absolute; however, it often serves as a prerequisite for the exercise of other rights and acts as a means to realize the constitutional right to informational self-determination. Accordingly, the current data protection legislation places significant emphasis on the scope and modalities for restricting this right, as well as on the obligation to provide information to individuals in a prompt, clear, and effective manner. The proper realization of this right is primarily achievable within the framework of well-organized data processing systems, employees possessing adequate knowledge, and an established organizational culture committed to personal data protection—areas which, despite progress, continue to present challenges.

[3] **Privacy by design and by default.**

In some cases, public institutions, citing sector-specific legal acts (such as tax legislation), argue that while the publication of certain data is regulated, the processing related to its deletion is not, and therefore they lack the authority to delete such data. However, the Law of Georgia "On Personal Data Protection", as well as the EU General Data Protection Regulation (GDPR), recognize the right to erasure (commonly known as the "right to be forgotten"), which may only be restricted in cases explicitly provided for by law. The absence of a provision regarding data deletion in the legislation governing a particular sector cannot be considered a valid basis for refusing a request to delete data. It is imperative that public institutions evaluate each data processing activity in accordance with the Law of Georgia "On Personal Data Protection".

f. Processing of Minors' Data

The best interests of the child constitute a fundamental principle applicable to any decision-making process involving the child. Accordingly, when processing data, data controllers and data processors should adopt individualized and appropriate approaches to determine the best interests of the minor. Such approaches include, where possible, involving the minor in the decision-making process; communicating with the child using language and methods suited to their vocabulary and socio-cultural characteristics, with the assistance of suitably qualified professionals; and assessing the child's expressed wishes while considering factors such as age and any disabilities. These measures both promote the proper realization of the rights of the child as a data subject and help prevent unlawful data processing. It is frequently observed during inspections related to the processing of children's data that organizations are less likely to justify their actions with reference to the best interests of the child. It is noteworthy that, when processing the data of a minor, the Service assesses not only the legal grounds for processing but also considers the best interests of the child.

Considering the number of educational institutions, the diversity of their activities, and the large number of employees and students, several challenges related to data processing in this sector have been identified. Employees in schools and kindergartens, through their daily professional and personal interactions, acquire and share a variety of professional data in both formal and informal settings. Data processing conducted during professional activities falls within the scope of the Law of Georgia "On Personal Data Protection". Accordingly, institutions, administrative staff, and teachers must assess the legal grounds for data processing before publishing information related to colleagues, students, or other individuals on social networks or in specialized communication channels, such as designated "chat rooms."

At the initial stage of the implementation of the Law, public schools improperly sought to obtain the data subject's consent. Typically, the consent forms were developed by the schools themselves and signed by the legal representatives of the children. However, standard data processing activities in public schools are regulated by legislation. Moreover, the provision of education is a public service offered by the state, and parents submit applications for their children's enrollment in specific schools. Therefore, consent as a legal basis for data processing is applicable only in limited, individual cases. In addition, it is essential that consent be obtained correctly. The data subject must consent to the processing of their data for a specific, clear, and

lawful purpose. When schools attempted to obtain such consent, the standard language of the consent forms often failed to include this information and created uncertainty regarding the necessity of collecting certain types of data—such as biometric or special category data—mentioned in the documents. It is important that the wording of consent forms be drafted in a manner that avoids ambiguity and prevents the possibility of an unreasonably broad interpretation.

It should also be taken into account that children, as individuals who have not yet reached physical and psychological maturity, may have a limited understanding of the risks, consequences, safeguards, and scope of their rights related to the processing of personal data. Therefore, taking proactive measures to ensure the lawful processing of children's data, as well as maintaining the accuracy and timely updating of such data, is critically important. This is especially relevant when children participate in various programs and/or processes alongside adult family members, where the awareness of the legal representative alone may not be sufficient.

During the reporting period, a case was identified in which a child's data was processed for several years under the status of a member of a socially vulnerable household, despite the fact that the child's parents were divorced, the child's grandmother and father were registered as members of the socially vulnerable household, and the child had been living with his mother in another region for an extended period. According to applicable legislation, a socially vulnerable household is defined as a group of individuals residing at the same address and sharing a common household. In the case under review, it was established that the child initially resided with his father at the registered address but subsequently lived with his mother in a different region for many years. Nevertheless, the composition of the socially vulnerable household was neither verified nor updated, resulting in the prolonged processing of inaccurate data concerning the child's social status. The use of various social work interventions may prove effective and preventive in identifying and addressing such cases.

g. Processing of Data related to Employment Relationships

Labor relations involve a wide range of data processing activities, often due to the duration and scope of the relationship and the large volume of data involved. The Service identified a case in which a public institution uploaded materials related to disciplinary proceedings involving a former employee to an electronic case management system in a manner that resulted in unauthorized access to the document. Disciplinary proceeding materials are sensitive by nature, as they carry a negative context and burden for the employee, regardless of the legal severity of the outcome. Accordingly, individuals involved in the processing of such data must carefully select appropriate organizational and technical measures to safeguard the security of materials related to disciplinary proceedings and ensure the effective protection of their confidentiality.

Cases of unlawful data processing are frequently the result of employee errors. In the context of inspections, employers typically initiate disciplinary proceedings and respond to employee misconduct by imposing sanctions or fines. However, this does not preclude the Service from assessing such incidents; and within the framework of inspections conducted by the supervisory authority, particular attention is given to the organizational and technical measures implemented by the employer. These measures should be designed to minimize the risk of erroneous or unlawful data processing by employees.

There is also significant interest in disciplinary proceeding materials—particularly in the identities of witnesses and their testimonies—as reflected in the applications submitted to the Service. Data subjects often object to the redaction of information relating to other individuals in the materials provided to them. In such cases, the competence of the Service is limited to overseeing the realization of the data subject's rights, including access to their own data and the right to be informed about the materials. An effective method for transferring documents, video recordings, or audio recordings containing the personal data of third parties is the concealment of such data—commonly referred to as "redaction." Accordingly, raising data subjects' awareness regarding the scope of the Service's competence and their own rights remains an ongoing priority.

According to the cases reviewed during the reporting period, data subjects often believe that they, as individuals, have the right to publicly disclose details and nuances of their labor relationships, while employers do not enjoy the same right. At the same time, the openness of information contributes to enhancing the accountability of public institutions and increasing the effectiveness of their activities. Public institutions that provide various services to a large number of citizens must exercise particular care in this regard, as fulfilling their duties effectively, maintaining public trust, and preserving their business reputation require a careful balance. In some cases, these institutions respond publicly to information concerning former or current employees that the employees themselves have disseminated to an indefinite audience and which may pose a risk to the institution's reputation. In such instances, it is critically important to ensure that only a minimal and proportionate volume of data is made public.

h. Audio and Video Monitoring

Audio monitoring by public institutions represents a common form of data processing. According to the cases examined during the reporting period, the purposes of audio monitoring are generally linked to ensuring the quality of service, as well as enhancing the efficiency and transparency of administrative proceedings.

It is noteworthy that a number of cases involving inadequate provision of information about audio monitoring were identified. A data controller cannot properly fulfill the obligation to inform data subjects about ongoing audio monitoring if its employees lack adequate knowledge of the data processing activities (for example, whether data is being collected through audio monitoring, and if so, for what purpose, on what legal basis, etc.). The importance of properly informing individuals becomes even more critical when applicants have objective expectations about audio monitoring, which may arise from explanations provided via institutional hotlines or from information published on official websites.

According to the identified cases, regulating the issue of informing data subjects—such as determining the content of the information to be provided—solely through practice often results in inconsistent and inadequate realization of the right. Some public institutions have not developed the specific written rule required by law, or have done so only partially. In such instances, the rule fails to comprehensively reflect key aspects of audio monitoring, including its purpose and scope, duration, rules and conditions for accessing the audio recordings, their storage and destruction, and the mechanisms in place to safeguard the rights of data subjects.

Video monitoring, as one of the most widespread forms of data processing, must be conducted in strict compliance with legal requirements. The Service has identified several cases in which public institutions placed warning signs regarding video monitoring in inappropriate or poorly visible locations. Consequently, in multiple instances, the requirements for the proper placement of warning signs in clearly visible areas have been clarified. Specifically, a warning sign must be positioned so that both its inscription and image are easily perceptible to any individual present within the video monitoring area. Additionally, information about the institution responsible for implementing the video monitoring must be clearly communicated to data subjects to facilitate the prompt and effective exercise of their rights.

During the reporting period, in the context of administrative violations related to traffic regulations, the use of video cameras installed on traffic light poles in Tbilisi—owned by the Tbilisi Municipality—was observed. Data subjects frequently raised concerns regarding the legality of personal data (photographs, video recordings) collected through these means. In some cases reviewed, the absence of warning signs in clearly visible locations was identified, and the instructions issued to address this deficiency were promptly implemented.

1.2. Case Law

a. Failure to fulfill obligations related to the incident

- **Unauthorized access to the database and data extraction through the electronic system of the Tbilisi Municipality City Hall and the N(N)LE Municipal Services Development Agency were also identified during the reporting period**

Based on an anonymous report, the Service identified a case of non-fulfillment of obligations related to an incident. The report included a link containing English-language terms that indicated an offer to sell data obtained from the N(N)LE Municipal Services Development Agency. In addition, certain Georgian-language sources also contained information regarding the disclosure of data from the institution.

Based on the evidence obtained within the framework of the case study and the normative acts regulating the detection and assessment of incidents, the Service identified the characteristics of the incident and concluded that there was a high probability of causing harm and/or posing a significant threat to human rights and freedoms. In assessing this issue, various factors were taken into account, including: the type of incident, the number of data subjects affected, the specific nature of the activities carried out by the data controller, and the degree of identifiability of the data subjects. As a result of the study, the N(N)LE Municipal Services Development Agency was found to have violated Articles 27 and 28 of the Law of Georgia "On Personal Data Protection", while the Tbilisi Municipality City Hall violated Articles 28, 29, and 30 of the same Law. Accordingly, the data processor was found guilty of the offense provided for in Articles 76 and 77 of the Law, and the data controller was found guilty of the offense provided for in Articles 77, 78, and 79.

- **A medical institution accidentally disclosed the data of dozens of individuals diagnosed with cancer on a government procurement website during the reporting period**

Based on the information submitted to the Personal Data Protection Service, the supervisory authority examined the legality of the data disclosure and the fulfillment of the obligation to notify the Service of the alleged incident, which involved the publication of genetic mutation analysis results on the public state procurement website.

In accordance with Article 29 of the Law of Georgia "On Personal Data Protection," the company, acting as the data controller, failed to fulfill its obligation to notify the Service about an incident posing a medium-level threat to human rights. Consequently, in accordance with Article 78 of the Law, the company was declared in violation.

b. Challenges Related to the Appointment of a Personal Data Protection Officer

The Personal Data Protection Service conducted an unscheduled examination of the proper fulfillment of the obligation to appoint or designate a personal data protection officer by more than twenty municipal bodies, several schools, universities and various legal entities of public law and non-entrepreneurial (non-commercial) legal entities operating under the Ministry of Labor, Health and Social Defense of Georgia, the Ministry of Justice of Georgia, and other agencies.

The Service established instances of non-compliance with paragraph 5 of Article 33 of the Law. Furthermore, cases were identified in which, despite an assignment issued by decision of the Personal Data Protection Service, certain institutions failed to appoint a personal data protection officer. This was assessed by the Service as a violation of Article 87 of the Law (failure to comply with the lawful request of the Service).

c. Processing of a Financial Declaration Containing a Person's Name and Surname by Publishing It in the Register of Organisations Pursuing the Interests of a Foreign Power

The Law of Georgia "On Transparency of Foreign Powers" and the "Rules for Maintaining the Register of Organizations pursuing the Interests of Foreign Powers, Submission of Financial Declarations and Monitoring" are newly adopted normative acts that define data processing procedures. Based on a notification, the Personal Data Protection Service examined the legality of the processing of the applicant's personal data as reflected in one of the financial declarations published in the "Register of Organizations pursuing the Interests of Foreign Powers."

During the inspection, it was revealed that the organization employing the author of the notification did not give due consideration to the guidance provided in the financial declaration, which stated that the purpose of the expenses should be formulated in a way that avoids including the personal data of a special category relating to the individual receiving the funds. Additionally, it was established that the author of the notification had previously disclosed information about their disability status and the specific grounds for granting that status through publicly accessible sources. Nevertheless, the organization's submission of information to the agency regarding income benefits related to the individual's disability status was assessed as a violation of the principle of data minimization (subparagraph "c" of paragraph 1 of Article 4 of the Law of Georgia "On Personal Data Protection"). As a result, the organization was found to be in violation of the law under subparagraph "a" of paragraph 1 of Article 66.

d. Processing of Data by LEPL "National Agency of Public Registry" within the Framework of Disciplinary Proceedings against an Employee

The data of an employee who has committed misconduct must be processed with particular care within the framework of disciplinary proceedings, with data security being of paramount importance in such cases. The Personal Data Protection Service, based on an application submitted by a former employee of the National Agency of the Public Registry of Georgia, investigated the unauthorized access to disciplinary proceeding materials by individuals not entitled to such access.

The findings indicated a violation of Article 17 (Data Security, currently Article 27) of the Law of Georgia "On Personal Data Protection".[4] Consequently, in accordance with Article 46 (currently Article 76) of the same Law, the National Agency of the Public Registry of Georgia was declared in violation.

e. Data Processing by LEPL "G. Abramishvili Military Hospital of the Ministry of Defense of Georgia" and an Employee of the Same Hospital through the Electronic System "Medservice"

As a rule, data processing is carried out by employees, and misuse of authority by employees constitutes a significant risk to data security. The importance of appropriately selecting organizational and technical measures for databases increases especially when the data concerns health-related information, due to the heightened confidentiality requirements of such data. Based on a notification, the Personal Data Protection Service examined the legality of the alleged disclosure of medical documentation containing personal data from a military hospital following the death of a patient.

The circumstances indicated a violation of Article 27 (Data Security) of the Law of Georgia "On Personal Data Protection" by the military hospital. Consequently, the institution was declared a violator of the law for the infringement stipulated in subparagraph "a" of paragraph 1 of Article 76 of the Law.

[4] **Law of Georgia "On Personal Data Protection" (Document No. 5669-RS, date of adoption, 28/12/2011, date of publication: 16/01/2012, invalid from June 14, 2023).**

f. Processing of Personal Data Generated by Medical Institutions at the LEPL L. Sakvarelidze National Center for Disease Control And Public Health via Personal E-Mail

The data controller and the data processor are obligated to employ data-secure methods and tools throughout the data processing activities. Based on a notification, the Personal Data Protection Service examined the legality of personal data processing by employees of the Center within the scope of their official duties using personal e-mail accounts.

The findings indicated a violation of Article 27 (Data Security) of the Law of Georgia "On Personal Data Protection." Consequently, the Legal Entity of Public Law — "L. Sakvarelidze National Center for Disease Control and Public Health" — was declared in violation under subparagraph "a" of paragraph 1 of Article 76 of the Law.

g. Data Processing in the Process of Verbal Communication When Providing Services by the LEPL "Levan Samkharauli National Bureau of Forensic Expertise"

To ensure data security, it is essential to take into account the physical arrangement of the service area, the specifics of verbal communication, and the content-related aspects of the service. The Personal Data Protection Service examined the legality of personal data processing by the Bureau during service provision, specifically in the context of verbal communication, as well as data request and retrieval processes.

The circumstances identified during the case study indicated a violation of Article 27 (Data Security) of the Law of Georgia "On Personal Data Protection" by the LEPL "Levan Samkharauli National Bureau of Forensic Expertise." As a result, the Bureau was declared in violation under subparagraph "a" of paragraph 1 of Article 76 of the Law.

h. Prolonged Publication of Ministerial Orders Containing Personal Data on the Website

In the context of modern technological advancement, data processing through electronic means—including the publication of information on websites—requires heightened caution. In cases of ongoing data processing, it is particularly important for the data controller to periodically assess the legal basis for such processing and identify potential risks. In response to a notification submitted to the Personal Data Protection Service, the legality of publishing a substantial volume of personal data of a broad group of individuals—including young beneficiaries of various funding and grant programs—was examined, specifically in connection with ministerial orders from 2012–2014 published on the website of the Ministry of Education, Science and Youth of Georgia.

As of 2024, no valid legal basis for the continued publication of these ministerial orders was identified. Consequently, the Ministry of Education, Science and Youth of Georgia was declared in violation of Article 67 of the Law of Georgia "On Personal Data Protection."

i. Data Processing by LEPL "National Agency of Public Registry" of Interested Persons related to Registration of Rights in the Real Estate Register by Using Telephone Numbers as Search Parameters

Public access to the Register of Rights to Immovable Property serves both to protect the legitimate interests of participants in legal relations, as well as to ensure the transparency of the activities of the registering authority and the implementation of effective public control over it. The Register of Rights to Immovable Property is one of the largest databases of publicly available personal data. When a person tries to search for information in the Register of Real Estate using the website of the LEPL "National Agency of Public Registry", the system redirects him to the Unified Portal of Electronic Services, which informs the visitor that he can search for material related to the immovable property by the person's name, surname and personal identification number. As a result of the test actions carried out in response to the notification submitted to the Service, it was determined that the telephone number of a natural person also provided access to certain information/documentation registered in the register, although it was not possible to identify the owner of the telephone number through the system. Considering this, the Service examined the legality of data processing in this process.

Due to the processing of the telephone number of the "interested person" for a purpose incompatible with the original purpose, based on Article 66 of the Law of Georgia "On Personal Data Protection", LEPL "National Agency of Public Registry" was declared a violator.

j. Data Processing by LEPL "Labor Inspection Service" during the Inspection Process Using Body Cameras

Given the scale, specifics, and risks associated with data processing through video and audio monitoring, and in response to a notification submitted to the Personal Data Protection Service, the Service examined the legality of using audio and video recording by the LEPL "Labor Inspection Service" through security cameras.

It was established that the LEPL "Information Technologies Agency," which was responsible for managing information technologies, violated Article 27 (Data Security) of the Law of Georgia "On Personal Data Protection," and was declared a violator under Article 76 of the Law. Additionally, it was found that the Labor Inspection Service failed to meet the requirements of Article 28[5] of the Law. For this reason, in accordance with Article 77, the LEPL "Labor Inspection Service," as the data controller, was also declared a violator.

[5] **Registration of information related to data processing and notifying the Personal Data Protection Service thereof.**

k. Processing of Data by LEPL "Revenue Service" through Publication of Public Notices on the Website about a Person with Tax Debt

The delivery of a legal act to its addressee is of fundamental importance; however, if this is not possible, legislation allows for the public dissemination of the document. Nevertheless, disclosure is a specific form of data processing, and such processing must be carried out with particular caution. Based on an application received, the Personal Data Protection Service examined the legality of the processing of the applicant's personal data through the public disclosure of documents on the official website of the LEPL "Revenue Service." The applicant was undergoing a tax audit, during which several documents were published on the agency's website for several months. These documents contained the applicant's name, surname, personal identification number, telephone numbers, the amount of fines imposed, and information on tax arrears.

These circumstances indicated a violation of the principles of data minimization and storage limitation, as provided for in subparagraphs "c" and "e" of paragraph 1 of Article 4 of the Law of Georgia "On Personal Data Protection." Accordingly, the LEPL "Revenue Service," as the data controller, was declared a violator under subparagraph "a" of paragraph 2 of Article 66 of the Law.

1.3. Instructions and Recommendations

In order to prevent further violations and to safeguard the rights of data subjects, the Personal Data Protection Service issued a range of recommendations and binding instructions to public institutions. Additionally, during the reporting period, inspection mechanisms were actively employed to monitor compliance with these instructions and to investigate alleged failures to implement them. Based on the findings, a set of key instructions was developed, which must be taken into account by data controllers and data processors:

- To protect the principle of transparency, ensure that the public is provided, through appropriate means, with information regarding specific personal data processing activities, including the scope of data processed, as well as the methods and forms of processing;
- Revise or develop new standard written document templates used in the data processing cycle, in order to ensure the lawfulness, transparency, and accuracy of personal data processing.
- Adjust the search parameters of the existing case management system to enable the retrieval of relevant materials in the future for the purpose of exercising data subjects' rights;
- Modify the operational rules applied in the case management process to obligate agency employees to uniformly enter personal data into the electronic system. This uniformity will facilitate the identification of all necessary documents for the realization of data subject rights;
- Provide data subjects with comprehensive access to information and documentation containing their personal data. In response to requests for correction or erasure of data, issue a well-reasoned decision or explanation. In certain cases, when access rights are restricted for individuals employed in the public sector, clearly communicate the legal grounds and conditions underlying such restrictions;
- Upon identifying instances of unlawful data processing—such as processing without a legal basis, beyond the necessary retention period, for unspecified purposes, or in the absence of adequate organizational and technical safeguards—terminate the processing of the affected data;
- Prevent further dissemination or disclosure of personal data, suspend the publication of relevant documents on the institution's website until the conclusion of the inspection initiated by the Service; upon conclusion, delete the specified document as instructed;
- Standardize the approach to handling documentation containing personal data to ensure consistency and legal compliance;
- Implement comprehensive organizational and technical measures to ensure the reliability, accuracy, and timely updating of outdated personal data on minors reflected in electronic systems;
- With regard to audio and video monitoring, define in writing the purpose, scope, and duration of processing; establish procedures and conditions for accessing, storing, and destroying recordings; and implement mechanisms for safeguarding data subject rights;

- Ensure that warning signs for video monitoring are visibly placed; standardize verbal notification procedures for data subjects; log all data-related actions within video recording/storage systems and restrict access to authorized users only;
- Prohibit the use of personal email accounts by employees for work purposes, and ensure that stored personal data in such accounts is permanently deleted;
- To add an automatic link deactivation (session disconnection) function in the event of temporary user inactivity in the electronic system to reduce the risk of data security and unauthorized access; in addition, creating a password-protected user account on office computers. Similar guidelines were also taken into account in relation to electronic databases, as cases were identified in which different employees used the same user account in the system;
- Ensuring the recording of all actions taken with respect to personal data in electronic systems and taking organizational and technical measures;
- Taking appropriate organizational and technical measures to reduce the risks of unlawful disclosure of data during verbal communication within the physical space of the service;
- Recommending the adoption of technical and organizational measures to prevent possible risks of disclosure of data to third parties during the process of handing over documents containing personal data to the addressee;
- Recording information related to data processing through video-audio monitoring in order to fulfill the obligation provided for in Article 28[6] of the Law;
- Develop and implement an appropriate monitoring mechanism for the facts of access to electronically processed data in order to prevent, detect and suppress unlawful data processing during the reporting period;
- For responsible public agencies, in order to fulfill their obligations related to the incident, record the incident, notify the Service about the incident and inform data subjects;
- Immediately appoint a data protection officer, ensure that his/her activities are free from conflicts of interest, bring the officer's activities into line with the standards and requirements established by Article 33 of the Law (including on appropriate knowledge), as well as proactively publish the identification and contact details of the personal data protection officer in order to facilitate the exercise of their rights by data subjects;
- Since the agency was obtaining more information from the databases of other public institutions than was necessary to achieve a legitimate purpose, it was instructed to determine the adequate and proportionate volume of data for the legitimate purpose and conduct future activities based on it.

[6] **Registration of information related to data processing and notifying the Personal Data Protection Service thereof.**

2. DATA PROCESSING IN THE PRIVATE SECTOR

According to the Law of Georgia "On Personal Data Protection", a number of obligations are imposed on data controllers and data processors, which are intended to ensure compliance with the requirements of European legislation during the data processing process and to promote the development of a legal culture of data protection in Georgia.

In order to monitor the lawfulness of data processing, the Personal Data Protection Service, both on its own initiative (through unscheduled inspections) and based on statements and notifications submitted by data subjects and other interested parties, examined a number of cases concerning the lawfulness of data processing carried out by private organizations and individuals. Several problematic issues were identified, including: the data subject's access to their personal data; data processing in accordance with the principle of transparency; violations of data security (incidents); data processing for direct marketing purposes; data protection in the context of labor relations; and the implementation of video monitoring, among others.

2.1. Key Directions and Trends

a. Data Subject Rights to Access Their Personal Data

The data subject's right to access their personal data is a fundamental objective of data protection legislation and serves as a prerequisite for the exercise of various other rights. This right not only enables the data subject to be informed about the processing of their data but also supports the realization of additional rights established by law. Access to data is essential for allowing the data subject to request the cessation, deletion, destruction, or restriction of data processing. Accordingly, facilitating the exercise of data subject rights by establishing effective mechanisms for informing data subjects and ensuring their practical use has remained a primary challenge for the Service.

In the course of ensuring data subjects' access to their own data, the following instances of non-fulfillment or inadequate fulfillment of obligations by data controllers and processors were identified:

- Cases of failure to provide data subjects with documentation or information containing their personal data, or of providing such documentation/information beyond the deadline established by law, were identified. Such delays cannot justify restricting the data subject's right of access to their own data by the data controller or processor. Accordingly, it is essential that data controllers and processors deliver the requested documentation/information within the statutory period of 10 working days, allowing sufficient time to prepare and transmit the material, considering the nature and volume of the request;[7]

[7] **Paragraph 2 of Article 13 of the Law of Georgia "On Personal Data Protection" provides, in exceptional cases and with appropriate justification, for the possibility of extending the legally prescribed period by no more than 10 working days, of which the data subject must be informed without delay.**

- Based on the processes examined, instances were identified where data subjects were not informed within the ten-day deadline established by law. Additionally, in some cases, the requested information or documentation was not provided to the data subject, and the grounds for refusal were not explained. Consequently, the Personal Data Protection Service issued a mandatory instruction to the data controllers to address these issues. Furthermore, to safeguard the statutory deadline, it is essential that data controllers delegate authority to employees in a manner that ensures insufficient human resources do not cause delays in providing information within the required 10-working day period. Accordingly, data controllers must implement measures that guarantee the effective realization of the data subject's rights;

- Facts of restriction of data subject rights were also identified. In certain cases, the Service deemed it lawful for the data controller to restrict the rights of the data subject in order to protect the rights and freedoms of third parties, about which the data controller ensured the data subject was duly informed. It should also be emphasized that, in the presence of any legal grounds for restricting data subject rights, data controllers must ensure that data subjects are informed of the grounds for such restriction in a manner that does not compromise the purpose or interest underlying the restriction itself;

- In one of the cases, where the matter concerned a request by the data subject to obtain an audio recording, the data controller (the bank) offered the data subject either a so-called transcript of the audio recording or the opportunity to listen to the audio recording at the data controller's office, which the data subject declined. The data subject sought to access not only the content of the communication, but also the recording of their own voice, which is a right guaranteed under paragraph 4 of Article 14 of the Law of Georgia "On Personal Data Protection". Accordingly, the data subject refused the alternative methods of access proposed by the bank and exercised their right to choose the form of access — namely, receiving a copy. Therefore, the Service determined that the data controller was obliged to provide the data subject with a copy of the audio recording containing his/her personal data in accordance with the procedures established by law, excluding the disclosure of third-party data (with the exception of the employee involved).

- In some cases, upon a data subject's request for the transfer of documents containing their personal data, the data controllers explained that copies of the requested documents had already been provided to the data subject. The data subject, however, requested copies of specific documents containing their data covering the entire period of employment. According to the decision of the President of the Personal Data Protection Service, even if the data controller had previously transferred part of the requested documents, they were still obliged to take proactive steps to enable the data subject to exercise their right to obtain copies.[8] Accordingly, the Service clarified that the data controller was legally obliged to provide the data subject with copies of documents containing their personal data, while excluding the personal data of third parties.

[8] According to the principle of transparent data processing, the data subject should be provided with the requested information as easily as possible, without creating any additional obstacles.

b. Data Processing in Compliance with the Principle of Transparency

The principle of transparency is intrinsically linked to the rights of the data subject. Its core requirement is that every data subject must be clearly informed about the processing of their personal data — including who is processing the data, by what means, for what purpose, and to what extent. Furthermore, all information and communication related to the processing must be readily accessible and comprehensible, presented in clear and plain language[9]. When the principle of transparency is properly upheld, data subjects are able to understand the risks associated with the processing of their data, as well as the means available to them for exercising their rights.

It is noteworthy that ensuring the principle of transparent data processing, as a means of facilitating the realization of data subjects' rights, remains one of the principal challenges faced by the Service. The Service has reviewed cases in which data controllers failed to comply with the requirements of the transparency principle during data processing, resulting in the improper execution of processing activities in violation of the applicable legal framework:

- In one case, the method of informing data subjects about the procedures for requesting access to their personal data from the organization did not align with the transparency principle established by law. The organization in question offered both paid and free channels for obtaining specific information; however, it failed to publicly inform data subjects about the availability of the free alternative. Consequently, the Service assessed the existence of an undisclosed mechanism for providing information to data subjects free of charge as a limitation on the effective application of the transparency principle. The Service instructed the organization to ensure that data subjects are adequately informed—via its website and portal—about both the paid and free mechanisms available for requesting specific information, in accordance with the legal requirements governing transparency;

- The company contacted a minor by telephone and, despite the data subject's request, failed to provide the data subject and/or his or her legal representative with information regarding the company's name and, consequently, the identity of the data controller. As a result, the data subject was unable to determine who was contacting him or her, which impeded the exercise of rights guaranteed by law (such as the right to obtain detailed information about the data being processed, to request the cessation of data processing, etc.). Taking into account the factual circumstances of the case, the Service determined that the company's data processing was not in compliance with the principle of transparency;

- The Service also assessed the processing of the data subject's personal data by the bank, which was reflected in the sending of notifications to the individual. The data subject stated that he was no longer a client of the bank, having closed all existing accounts, and therefore should not have been receiving any further notifications from the bank. The bank confirmed that the data subject had indeed closed all of his accounts; however, it explained that account closure alone did not constitute full termination of the legal relationship, and that the data subject remained registered as a client. Although the bank submitted to the Service

[9] **Guidelines on transparency under Regulation 2016/679, 17/EN, WP260 rev.01, Article 29 Working Party, adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, §6.**

records of a general agreement concluded with the data subject—on the basis of which it argued that the data subject had been duly informed that the relationship with the bank would continue even after the closure of accounts—the Service determined that these records did not make it sufficiently clear that the bank would continue to consider the data subject an active client and a party to the agreement, even in the event that all products, services, and accounts were fully cancelled. The Service also noted that the data subject did not have a clear understanding that a specific request was required to fully terminate the legal relationship with the bank, beyond merely refusing all services/products. Accordingly, the bank was instructed to ensure compliance with the principle of transparency by informing the author of the notification that the complete termination of the legal relationship requires a formal and explicit request, and that the cessation of all services/products alone is not sufficient for this purpose;

- During the examination of one particular case, it was established that neither the internal organizational documents adopted by the company nor the employment contract concluded between the company and the employee contained any information regarding the company's potential control or access to the employee's work email, its use following the employee's dismissal, the storage of information contained therein, or the duration of such storage. Accordingly, even if the company had ensured that the applicant was acquainted with the aforementioned documentation, this would not have sufficed to fulfill the requirements of the principle of transparency as defined in Article 4 of the Law. Based on the foregoing, the Service determined that the principle of transparency had not been ensured in relation to the data subject during the data processing activities carried out by the company. Consequently, the company was instructed to develop appropriate internal regulations that would inform employees of the company's potential access to or control of work email, its use following termination of employment, the storage of information contained therein, and the applicable retention period;

- In one of the cases reviewed by the Service, which concerned the processing of a deceased individual's data by a medical institution through disclosure, the representative of the institution stated that they were not obligated to inform the data subject—or the subject's parent, child, grandchild, or spouse—about the right to prohibit data processing following the subject's death. Consequently, the institution, citing the absence of such a prohibition, deemed it permissible to release the information to a third party. It is important to note that the principles established by law- particularly the principle of transparency- constitute not only a normatively binding framework that limits the scope of action of the data controller and/or data processor, but also serve as interpretive tools for clarifying the law's provisions. Accordingly, the Service concluded that although Article 8, paragraph 1, subparagraph "b" of the Law does not explicitly require the data controller to provide this specific information, the intent of the legislator might be reasonably inferred through application of the transparency principle. Failing to do so would undermine the substantive purpose of the norm, which is to ensure the protection of an individual's data even after death.

c. Data Security Breach (Incident) in the Data Processing and the Obligation to Comply with Data Security Requirements

Pursuant to Article 4, subparagraph "f" of the Law, the legislator has assigned data security[10] a general regulatory normative character, designating it as one of the fundamental principles of data processing. In accordance with this provision, technical and organizational measures must be implemented throughout the data processing cycle to ensure the protection of data against unauthorized or unlawful processing, as well as against accidental loss, destruction, and/or damage. The Constitutional Court of Georgia has recognized the "protection of data, i.e., information about a person, from disclosure" as an integral part of the constitutional right to privacy, emphasizing that such protection serves a "valuable legitimate purpose."[11] Furthermore, Article 4, paragraph 7 of the Law imposes an obligation on the data controller to adhere to the principle of data security in the course of data processing. Consequently, the standard for data security protection has been significantly elevated by law—not only through the establishment of data security as a guiding principle, but also by introducing a distinct definition and separate regulatory framework for cases involving data security breaches. An incident is defined as a data security breach resulting in the unlawful or accidental destruction, loss, unauthorized disclosure, alteration, access, collection, retrieval, or any other unauthorized processing of personal data. To protect the rights of data subjects, entities involved in an incident are subject to comprehensive regulatory requirements, particularly when the incident is likely to cause significant damage and/or pose a substantial threat to the fundamental rights and freedoms of individuals. In such circumstances, the data controller is obligated to notify both the affected data subjects and the supervisory authority responsible for oversight. Furthermore, the controller must, when necessary, implement appropriate measures and provide relevant instructions to enhance the security safeguards related to the personal data.

---

[10] Ensuring data security requires the implementation of appropriate measures aimed at preventing and managing data breaches, ensuring the proper execution of data processing operations in line with applicable principles, and facilitating the effective exercise of data subjects' rights. These security measures must encompass not only cybersecurity but also physical and organizational safeguards. It is essential that organizations regularly evaluate the adequacy and effectiveness of their security measures to ensure they remain current and responsive to evolving risks. Accordingly, in determining appropriate data security measures, consideration must be given to modern data protection technologies and practices, recent advancements, implementation costs, and the nature, scope, context, and purposes of the processing. Additionally, the potential impact of the data processing operation on the rights and freedoms of individuals must be taken into account.

See: Recommendations on the Principles of Personal Data Processing, Personal Data Protection Service, Tbilisi, 2024, p. 28. Available at: https://pdps.ge/ka/content/984/rekomendaciebi?page=2 [Accessed: 17.02.2025]

[11] Decision of the Constitutional Court of Georgia of June 7, 2019 No. 1/4/693,857 in the case "A(A)IJ "Media Development Fund" and A(A)IJ "Institute for the Development of Freedom of Information" against the Parliament of Georgia", II, §25.

Considering that data breaches may adversely affect the privacy and data protection rights of data subjects, it is imperative that data controllers and processors strictly comply with the standards of data processing and security measures prescribed by applicable legislation.

In connection with the incident, the Service was contacted by several data controllers, and in one instance, a similar notification was received from a third party. Based on the aforementioned notifications, ongoing inspections established that, in all cases, the technical and organizational measures implemented by the data controllers were insufficient to prevent incidents. Considering the nature of their activities, the said entities were required to take into account, during the data processing, the categories of data processed (including special categories of data), their volume (in one case, amounting to hundreds of thousands of records), the form and storage media (in all cases, data was stored on electronic media), as well as the potential risks to the rights of data subjects—specifically, threats related to attacks on electronic systems, which were significantly heightened due to the volume and categories of data processed by the companies. Based on these factors, the entities were obliged to implement appropriate security measures to effectively prevent unlawful data processing.

The Service determined that, although the data controllers notified the Service of the incident (except in one case), they failed to properly fulfill their legal obligation to provide complete notification. Specifically, none of the data controllers ensured that the Service received full information pertaining to the incident, as required by the Law of Georgia "On Personal Data Protection" and the relevant subordinate normative act. According to the data controllers, the Service was not adequately informed because they deemed it unlikely that the incidents would cause significant damage or pose a substantial threat to the fundamental rights and freedoms of individuals. The Service did not accept these arguments and clarified that the cases exhibited multiple circumstances outlined in Article 5 of the Order No. 19 of the President of the Personal Data Protection Service dated February 28, 2024 "On the Approval of Criteria for Determining Incidents Posing a Significant Threat to Fundamental Human Rights and Freedoms and the Procedure for Notifying the Personal Data Protection Service of an Incident" (hereinafter referred to as the "Rule"). These criteria must be considered by the data controller when assessing the severity of the threat posed by the incident to fundamental human rights and freedoms. In particular, in one case, it was established that the incident involved a breach of confidentiality due to unlawful access to data. Furthermore, the risk of identification of data subjects by a third party was high, as the accessed data included identity documents (identity card and passport). Additionally, the data controller engaged in activities subject to special regulation under the Law of Georgia "On Information Security." The incident was also considerable in scale, involving various data pertaining to several thousand individuals

In one of the cases, the incident was identified as a breach of confidentiality (unlawful disclosure of data), resulting in the exposure of data related to data subjects, including special categories of personal data. Furthermore, a large volume of special category data was disclosed.[12] As a consequence of the incident, the likelihood of identification of the data subjects by a third party was high, since information such as the name, surname, gender, date of birth, and personal identification number of the data subjects was revealed. The Service referred to Article 6

[12] **The user's analysis results were disclosed, indicating the results of the laboratory study.**

of the Rules and, given that, the data controller unlawfully disclosed special categories of data (including analysis responses), the Service concluded that the incident posed a significant risk of threat to the fundamental rights and freedoms of the affected individuals.

Incident management norms constitute an essential legal instrument for the effective protection of data subjects' rights, the prevention of further unlawful processing of their personal data, and the realization of the right to data protection through cooperation with the Service, as the supervisory authority for data protection. A timely qualification of the data disclosure event by the data controller as an incident is of critical importance in this process. Accordingly, the data controller, in compliance with the requirements established by law and the relevant procedures, must ensure the prompt and effective neutralization of any negative consequences arising from the incident, in close coordination with the Service.

d. Data Processing for Direct Marketing Purposes

To ensure the effective exercise of data subjects' rights, the law has newly introduced a specific provision regulating data processing for direct marketing purposes. In particular, Irrespective of the ground for collecting/obtaining data and their accessibility, data may only be processed for direct marketing purposes with the consent of the data subject[13]. In addition to the name, surname, address, telephone number and e-mail address of the data subject, other data shall be processed for direct marketing purposes with the written consent of the data subject. Prior to obtaining the data subject's consent and when carrying out direct marketing, the controller/processor shall inform the data subject, in clear, simple and understandable language, of his/her right to withdraw his/her consent at any time and of the mechanism/procedure for exercising this right. Alos, the controller/processor shall ensure that the data subject has the possibility to request that the processing of data for direct marketing purposes be terminated in the same form in which the direct marketing is carried out, or to determine other available and adequate means to request the termination of the processing. No fee or other restriction shall be imposed on the data subject for exercising the right to withdraw consent. In addition to the above, Article 3, Subparagraphs "i" and "m" of the Law define the concepts of data subject consent and written consent, in particular, consent of the data subject – consent freely and unambiguously expressed by a data subject after the receipt of the respective information, by an active action, in writing (including in electronic form) or verbally, to the processing of data concerning him/her for specific purposes. Written consent of the data subject – consent, signed or otherwise expressed by a data subject in writing (including in electronic form) after the receipt of the respective information, to the processing of data concerning him/her for specific purposes.

According to the new Law of Georgia "On Personal Data Protection", data processing for the purpose of direct marketing is permitted only with the data subject's consent. Prior to the entry into force of the law, it was allowed to process data obtained from publicly available sources for direct marketing purposes. At the same time, data controllers and/or data processors continued to process data for direct marketing regardless of the original purpose of collection, which led

[13] **Law of Georgia "On Personal Data Protection", Article 12, Paragraph 1.**

to a significant increase in the number of applications submitted to the Service in this regard. During the reporting period, hundreds of individuals addressed the Service with applications and notifications about receiving numerous marketing-related short text messages on their phone numbers without having given consent. Several applications concerned repeated messages received from the same companies. In addition to responding to individual applications, the Service identified authorized persons in the electronic communications sector who were providing services to data controllers for direct marketing purposes. Given the number and content of the applications/notifications received, the nature of the companies' activities, and the potential scale of data processing, the Service conducted unscheduled inspections during the reporting period to identify possible unlawful data processing for direct marketing purposes.

Within the framework of the checks (inspections), based on the evidence submitted to the Service by data subjects, it was revealed that dozens of companies (contractor companies) used the services of authorized persons to conduct direct marketing, through which marketing content offers were sent to telephone numbers. Accordingly, the Service also assessed the lawfulness of data processing by these companies for the purpose of direct marketing.

The Service examined cases in which data controllers processed personal data without obtaining the consent of data subjects (including written consent). Furthermore, prior to obtaining consent and during the implementation of direct marketing, data subjects were not clearly, simply, and intelligibly informed of their right to withdraw consent at any time, nor of the mechanism/procedure for exercising this right. Additionally, upon the relevant request of the data subject, the processing of their data for direct marketing purposes was not ceased within the timeframe established by law, and the mechanism for terminating data processing for direct marketing purposes was not made available through the same means as the direct marketing itself. In certain cases, a fee was also imposed for exercising the right to withdraw consent.

In the above-mentioned cases, a number of individuals and legal entities—both data controllers and data processors—were found to have violated the law, and were sanctioned with either a warning or a fine. The Service imposed mandatory obligations on all entities that had processed the telephone numbers of data subjects without their consent, requiring them to cease processing such numbers for direct marketing purposes and to ensure monitoring of data processor, as prescribed by law, which, in turn, serves to prevent unlawful data processing in the future.

Additionally, during the inspections, cases were identified in which contractor companies had obtained the consent of data subjects in accordance with the requirements of the law. Consequently, no violations of the legal provisions were found in cases where data was processed for direct marketing purposes.

e. Processing of a Data Subject's Personal Data through Video Monitoring in a Residential Building

The Law defines video monitoring as a form of data processing, establishes its legal framework and objectives, and regulates issues related to video monitoring in residential buildings, including premises intended for hygiene or other spaces where a data subject has a reasonable expectation of privacy[14].

Applications concerning data processing through video monitoring in residential buildings are frequently submitted to the Service, and, in most cases, such monitoring is carried out by data controllers without complying or inadequately complying with the requirements established by law:

- In a number of cases, it was established that video monitoring of common entrances and shared areas within residential buildings had been implemented without obtaining the written consent of more than half of the property owners (where identifying an owner is not possible, the consent of the possessor may be obtained). Additionally, in certain instances, the video surveillance area extended to the entrances of individual residential units, for which the law requires a decision or written consent from the respective owner or legal possessor. While the protection of property and personal security constitutes a legitimate objective under the law, this alone does not suffice to render data processing through video monitoring lawful. Every individual has the right to freely enjoy their living space, including moving around their home without obstruction or surveillance by others. This right encompasses, on the one hand, the ability to autonomously construct and develop one's private life, and on the other, protection from undue intrusion by others into one's personal space. In such cases, data controllers were instructed to cease video monitoring activities, delete the data obtained therefrom, dismantle installed surveillance cameras, or ensure that video monitoring is carried out in strict compliance with legal requirements;

- In some cases, data controllers failed to place a warning sign indicating that video monitoring was being conducted, and in several instances where such a sign was present, it did not include information about the identity and contact details of the data controller. Accordingly, the data controllers were instructed to install warning signage regarding the implementation of video monitoring in full compliance with the legal requirements;

- In several cases examined by the Service, it was established that although video cameras were installed in residential premises, no actual processing of data subjects' personal data was carried out through video monitoring. However, the presence of the cameras created a misleading impression that video surveillance was in effect. The Service concluded that placing video cameras in areas where video monitoring is not actually conducted might mislead data subjects and give rise to a false perception regarding the processing of their personal data. Consequently, in order to prevent the deception of data subjects, data controllers were instructed either to remove the cameras or, if video monitoring was to be conducted, to ensure full compliance with the legal requirements;

[14] Law of Georgia "On Personal Data Protection" Article 10, Paragraph 4.

- Based on the cases examined, it was established that the data controllers responsible for implementing video monitoring in residential buildings had not taken appropriate technical and organizational measures to ensure the lawful processing of personal data. Specifically, it was revealed that multiple individuals accessed the video monitoring system using a shared username and password; the system was located in a common area and was not secured against unauthorized access by third parties; and the system failed to record all actions performed on video recordings. These shortcomings created significant risks of unlawful acquisition, disclosure, use, destruction, or other unauthorized processing of electronically stored data. Moreover, in the event of such actions, it was not possible to identify the responsible individual. Accordingly, in each case, the data controllers were instructed to implement appropriate technical and organizational safeguards for the data obtained through video monitoring, including: assigning individual usernames and passwords for system access; recording all actions performed with respect to the data in electronic form (including incidents, data collection, modification, access, disclosure (transfer), linking, and deletion), and other relevant measures.

f. Data Protection in the Context of Employment Relations

A significant volume of personal data is processed within the framework of employment relations, as these encompass contractual, pre-contractual, and post-contractual stages. At each of these stages, employers process the personal data of job applicants, current employees, and former employees for various purposes, including the selection of qualified personnel, the conclusion of employment contracts, and the fulfillment of legal obligations. Data processing by employers is frequently conducted through various electronic systems. Given the volume of data involved, multiple individuals often participate in the data processing operations. Consequently, several of them may have access to these electronic systems. Therefore, in the absence of appropriate organizational and technical measures to ensure data confidentiality, the risk of accidental or unlawful data processing increases significantly.

Taking into account the aforementioned factors, the following incidents were recorded during the reporting period in relation to the protection of data subjects' rights within the context of labor relations:

- As part of one of the studies, it was established that, upon the company's instructions, during the performance of work on the electricity distribution network in an open area, the company's employees—who were directly involved in the execution of said work—carried out video monitoring of the preparatory process using shoulder-mounted cameras, which also included audio recording. In the case under consideration, although the company's employees had been informed of the mandatory rules and the purpose of implementing video monitoring during the performance of work on the network, in accordance with the principles established by law—particularly the principle of transparency—and pursuant to Article 10, paragraph 2 of the Law, the company was required to adopt a written document clearly outlining the full procedure for implementing video monitoring of the work

carried out on the company's electricity distribution network. This document should have defined the purpose and scope of video monitoring, its duration, the retention period of the video recordings, the rules and conditions for accessing, storing, and destroying said recordings, as well as mechanisms for protecting the rights of data subjects. Furthermore, although employees were informed about the ongoing audio monitoring, the company had not developed any procedure governing the implementation of audio monitoring for the aforementioned work. Accordingly, due to the absence of these documents, the Service identified an administrative violation and issued an instruction to the company to ensure their development;

- The Service investigated the legality of biometric data processing by an employer, specifically the collection of employees' fingerprints. The investigation revealed that employees were required to register their fingerprints using a specialized device to gain access to the company's buildings and to move within the internal premises. It is noteworthy that, considering the specifics of the company's activities, the Service acknowledged the arguments presented by the company regarding the necessity of processing biometric data in certain areas within the company's premises (such as gaming areas, the so-called "MCR" ("Mission Control Room"), server rooms, uniform and office administration storage rooms, etc.). This includes, in light of the risks inherent to the gaming industry, the necessity of biometric data processing in gaming and related spaces to prevent unauthorized access and to mitigate the risk of disclosing confidential information—such as game "content," including content created by the company, as well as educational and work materials related to the company's activities. However, with respect to some areas, the Service did not consider the processing of biometric data to be a necessary measure for the purposes asserted by the company. Specifically, the arguments presented by the company regarding the necessity of processing biometric data for access control in the gym and changing rooms—intended to prevent overcrowding in the gym and ensure access only by authorized persons, as well as to protect employees' personal belongings and property from unauthorized access and related criminal acts—were considered. However, given the number of employees in the company, the Service did not regard these reasons as a lawful basis for processing biometric data, as the company's objectives can be achieved without such processing. The risks cited by the company in relation to these spaces are inherent to any workplace environment. Regarding the changing rooms, the Service noted that the availability of storage lockers with locking mechanisms, combined with other organizational and technical measures implemented by the company, provided sufficient protection for employees' personal belongings without the need for biometric data processing. In addition to the aforementioned spaces, the Service assessed as unlawful the use of fingerprint registration by employees working in gaming areas (the so-called "studios") to record their shift attendance. This practice, in itself, rendered the processing of biometric data unnecessary for the performance of the company's activities, as the stated purpose could be achieved through alternative mechanisms for recording attendance. Moreover, the company addressed general issues related to the processing of personal data (including special categories) of its employees across various internal documents and outlined the purposes for processing biometric data templates. Nevertheless, the Service did not consider the process to meet the transparency requirements, as the general and fragmented information scattered across various documents did not ensure that data subjects were provided with detailed, clear, and comprehensible information regarding the nature of the biometric data processing. Accordingly, the company

was instructed to cease the processing of biometric data for the purposes of access control to the gym and changing rooms, as well as for shift attendance tracking. Furthermore, in compliance with the principles set forth in Article 4 of the Law, the company was required to define in writing the purpose and scope of biometric data processing, the data retention period, the procedures and conditions for storing and destroying such data, and the mechanisms for protecting the rights of data subjects.

g. Lawfulness of Data Processing in the Electoral Process

The Parliamentary Elections of Georgia were held on October 26, 2024. Following the elections, a number of applications and notifications were submitted to the Service by data subjects requesting an assessment of the lawfulness of the processing of their personal data. Pursuant to the Election Code of Georgia, a political party is authorized to carry out pre-election campaigning (agitation) for the purpose of participating in and securing victory in the elections. In accordance with applicable legislation, activities such as the direct and immediate provision of information to a data subject/voter — including via telephone, mail, e-mail, or other electronic means — for the purpose of soliciting support, fall within the definition of direct marketing. As such, when conducted as part of pre-election campaigning (agitation), these activities must comply with the requirements established by Article 12 of the Law of Georgia "On Personal Data Protection" (Data Processing for the Purpose of Direct Marketing), including with regard to the processing of data belonging to data subjects/voters;

It is noteworthy that, in order to prevent unlawful data processing, the Service issued a public statement during the pre-election period, reminding data controllers and data processors involved in the electoral process of their obligation to process voters' personal data in compliance with the law. Based on the cases reviewed and verified (including through inspections) during the reporting period, it was established that data controllers—primarily political parties—had, in most cases, processed the personal data of data subjects without a legal basis as required by law. Furthermore, in certain instances, violations related to the rules governing data processing for direct marketing purposes were also identified. Specifically:

- During the pre-election period, within the timeframes established by electoral legislation, political parties appointed commission members—i.e. data subjects—to various precinct election commissions based on their designated quotas and processed their personal data. However, in doing so, they either lacked the legal basis required by law or failed to fulfill the statutory obligation to demonstrate the existence of such a basis. Pursuant to Paragraph 2 of Article 5 of the Law, the burden of proving the existence of a lawful ground for data processing rests with the data controller. In the cases examined by the Service, political parties were unable to present objective evidence—beyond oral statements—to substantiate the processing of data subjects' personal data on any of the legal grounds specified in Paragraph 1 of Article 5 of the Law;

- One of the political parties sent e-mail notifications to several dozen data subjects regarding participation in the elections. A representative of the party stated that the messages were merely informational and, therefore, the provisions regulating data processing for the purpose of direct marketing should not apply. However, direct marketing includes activities aimed at shaping interest in image-related and social topics, as well as providing information to data subjects/voters with the aim of gaining their support. Consequently, the political party was obligated to process the data subjects' personal data in compliance with the requirements set forth in Article 12 of the Law;
- In the above cases, the Service considered that political parties processed data of data subjects in violation of the requirements of the law and applied the appropriate sanctions provided for by the law.

h. Data Processing in the Healthcare Sector

Article 6 of the Law sets out the specific legal grounds for the processing of special categories of data. The legislator has explicitly distinguished special category data within the right to data protection framework, establishing a distinct regulatory regime[15] for their processing. Unlike the Law of Georgia "On Personal Data Protection" dated December 28, 2011, the current law redefines the concept of data related to health. According to the law, data concerning health is data related to the physical or mental health of a data subject, including the provision of health care services, which reveal information about their physical or mental health

Information concerning the health of a data subject, due to its sensitive nature, is subject to a heightened standard of protection. Health-related data encompass intimate details regarding an individual's lifestyle, habits, as well as mental and physical condition. The unlawful disclosure of such data may result in substantial harm to the individual's personal and family life, and may negatively affect their employment opportunities and social integration. During the reporting period, several instances were identified in which the obligations established by law were either not fulfilled or inadequately fulfilled, namely:

- Cases were identified in which medical institutions failed to take appropriate organizational and technical measures to ensure data security. For instance, during one of the inspections, it was found that an email containing patients' data—including information about their health status—was mistakenly sent from the clinic's official email address to an incorrect recipient due to a typographical error (specifically, the omission of one Latin letter in the email address). As a result of this human error, the health-related information was disclosed to an unauthorized person, thereby constituting a violation of the data security requirements established by law. Consequently, the clinic was subjected to the applicable legal sanction. To ensure data security, it is essential that medical institutions, as data controllers, implement appropriate organizational and technical measures to minimize the risk of unauthorized access during the disclosure or any other processing of personal data;

[15] **Decision of the Constitutional Court of Georgia of June 7, 2019 No. 1/4/693,857 in the case "A(A)IJ "Media Development Fund" and A(A)IJ "Institute for the Development of Freedom of Information" against the Parliament of Georgia", II, §57.**

- The issue of processing special category data of data subjects without a legal basis remains relevant in the healthcare sector. It is essential that medical institutions (or, in certain cases, individual doctors), as data controllers, prevent any instances of unlawful processing of special category data in their possession, which is crucial for the practical realization of the right to data protection. The Service examined the legality of a doctor's disclosure of special category data (specifically, information regarding the receipt of medical services by several individuals) on the social network "Facebook." Within the framework of the inspection, the provision of medical services by the doctor was confirmed only in relation to one data subject. No evidence was presented to confirm the provision of such services in respect of the remaining individuals. Furthermore, the publication of this information by the doctor in a publicly accessible format created the impression for third parties that the mentioned data subjects had indeed received medical services from the doctor. Such information constitutes special category data. Notably, the doctor failed to identify a legal basis for processing this data, and as a result, was subjected to the legal sanction prescribed by law.

i. Data Processing in the Financial Sector

The financial sector comprises commercial banks, microfinance organizations, lending entities, and distressed asset management companies, which process, among other things, data such as the addresses of data subjects, places of employment, financial obligations and transactions, and family relationships. With the advancement of modern technologies, the number of electronic databases created and used for various purposes in the financial sector increases annually, resulting in a growing risk of errors and violations in the course of data processing through automated means. During the reporting period, data protection in the financial sector represented a significant challenge for the Service. In this context, a number of instances were identified in which the obligations established by law were either not fulfilled or inadequately fulfilled, namely:

- Instances have been identified in the financial sector where third parties were contacted and data was disclosed for the purpose of locating a borrower. In this regard, it should be emphasized that such actions should only be taken when absolutely necessary, as contacting third parties and informing them of the reason for the contact (e.g., locating a borrower) inherently involves the disclosure of information related to the borrower. Accordingly, representatives of the financial sector must first make every effort to reach the borrower using the contact information already available to them. Contacting third parties for this purpose should be considered only as a last resort, if the initial attempts to reach the borrower prove unsuccessful;

- Additionally, instances were identified where representatives of the financial sector continued to contact third parties for the purpose of locating borrowers, despite the expressed resistance of those individuals. If, in the process of locating a specific person, a representative of the financial sector establishes communication with a third party who refuses to cooperate and requests the cessation of the processing of his or her data, the data controller

is obliged to immediately discontinue and refrain from any further processing of that third party's data for the stated purpose;

- In certain cases, representatives of the financial sector were unable to provide objective evidence concerning the source of data subjects' personal data. As the responsibility to substantiate the legal basis for data processing rests with the data controller, the Service did not consider oral explanations sufficient to justify the lawfulness of contacting third parties for the purpose of locating a borrower;

- The Service reviewed the practice of a bank delivering debit cards to clients in an unsealed form and found that, by granting service center employees full and direct access to sensitive card information (such as the cardholder's name, surname, and card number), the bank failed to adequately ensure data security. The broader the access to such data, the higher the risk of accidental or intentional unlawful processing (e.g., photographing or memorizing card details by employees for subsequent misuse). The data controller must implement organizational and technical measures to eliminate these risks. Accordingly, the Service emphasized that the data controller is required to restrict access to customer data to the minimum necessary personnel and only when justified by legitimate need. Consequently, the bank was found in violation of the law and instructed to organize the issuance of new debit cards so that employees of the bank's service centers do not have access to the card data;

- During an inspection of one of the banks, it was determined that, in compliance with the requirement established by the order of the President of the National Bank, the bank was informing the registered owner of real estate used as collateral about the details of the credit agreement secured by that property. According to the order, the bank has five working days to provide this information, and under the bank's internal procedure, the notification is sent on the second day following the loan issuance. In the case under review, the borrower purchased the real estate on the same day as the loan issuance using the bank's funds; however, the bank sent detailed information about the loan agreement to a third party who was still recorded as the owner of the property in the public registry at that time, due to the timing of the registration process. The Service explained that, considering the specific factual circumstances of the case, the bank had the opportunity to assess the nature and purpose of the particular contractual relationship and, accordingly, refrain from applying the general standard procedure it had established for such cases when processing the applicant's data. Furthermore, the bank should have made its decision by balancing the interests of both the owner of the collateral and the borrower (data subject), rather than prioritizing only one party's interests. The bank ought to have disclosed information to the owner of the collateral only if that person remained the owner after the expiration of the standard registration period known to the bank. By doing so, the bank could have complied with the legal principles governing the processing of the borrower's data and fulfilled its legal obligations. Accordingly, the Service concluded that the bank had the opportunity, after the standard registration period had elapsed, to verify the change of ownership in the public registry extract and, based on that verification, assess and determine the extent of its obligations toward the owner of the collateral.

2.2. Case Law

a. Principle of Transparency

An individual submitted an application to the Service requesting an investigation into the legality of the processing of his personal data by a certain company and a response regarding violations of information disclosure rules. The applicant stated that he had requested information from the company about the processing of his data (including a credit report and credit score) as stipulated in Article 13 of the Law, but the company failed to provide this information in full.

The Service determined that the company did not ensure compliance with the principle of transparency for data subjects during the data processing, thereby violating the requirement set forth in Article 4 of the Law. This constituted grounds for an administrative offense and the imposition of administrative liability under Article 66. Accordingly, the company was issued mandatory instructions to rectify the violations.

During the consideration of one case, it was established that the internal organizational documents provided by the company, as well as the employment contract concluded between the company and the employee, did not include information regarding the company's potential control or access to the employee's work email, the use of the work email following the employee's dismissal, the storage of the information contained therein, or the duration of such storage. Accordingly, even if the company had made the aforementioned documentation available to the applicant, it would not have been able to ensure compliance with the transparency requirements set forth in Article 4 of the Law.

The Service examined a case concerning the processing of a deceased person's data by a medical institution through data disclosure. The representative of the medical institution stated that they were not obligated to inform the data subject or the data subject's parent, child, grandchild, or spouse about the right to prohibit data processing following the individual's death. The Service considered that, although Article 8, paragraph 1, subparagraph "b" of the Law does not explicitly impose the aforementioned obligation to inform the data controller, interpreting this provision in light of the principle of transparency is essential; otherwise, the substantive purpose of the norm—namely, the protection of a person's data after death—would be undermined.

b. Principle of Transparency and Data Security

An individual applied to the Service, requesting an investigation into the legality of the processing of his personal data by a taxi service provider through its mobile application.

The company was held administratively liable for violating both the principle of transparency in the data processing process and the requirements related to data security. Furthermore, the company was instructed to provide data subjects, in accordance with the principle of transparency, with clear information regarding which data is mandatory or voluntary during the regis-

tration process, as well as complete and accurate instructions on the procedure for account cancellation and data deletion. From a security standpoint, the company was also ordered to implement a system capable of electronically registering all actions performed on the data within the database.

c. Data Security

The Service was notified by an individual and requested to examine the legality of one of the banks' disclosure of third-party data by sending short text messages to the telephone number of the author of the notification.

The Service explained that the law imposes an obligation on the data controller to implement organizational and technical measures that ensure the protection of data from accidental or unlawful disclosure. Accordingly, the bank, as the data controller, was required to comply with the data security standards established by law. The bank was instructed to adopt such organizational and technical measures that would ensure, through its system, that data about loan officers from the bank's so-called "HR" database could be retrieved only by using the person's unique identifying data.

d. Data Subject Access to Their Own Data

The data subject applied to the Service with a request to transfer documents containing his data to one of the companies.

By decision of the Service, the company was instructed to provide the applicant with copies of the video recordings containing his data in a form that would prevent the identification of third parties depicted in the recordings.

e. International Data Transfer

As part of the inspection, the Service investigated the possible unlawful transfer of data to another state by one of the companies. The company provided taxi services to its customers through a mobile application.

The Service determined that the company violated the requirements of the law during the international transfer (processing) of data of users/data subjects (passengers/drivers) registered from the territory of Georgia through the application. Accordingly, the company was found to be in violation and was issued a fine as an administrative penalty. In addition, the company was ordered to ensure the termination of the transfer of users'/data subjects' (passengers'/drivers') data (global network address/IP address) registered from the territory of Georgia through the application to the Russian Federation.

2.3. Instructions and Recommendations

The decisions taken by the Private Sector Oversight Department in the course of examining the lawfulness of data processing have imposed mandatory instruction and issued recommendations to data controllers and data processors.

The following instructions and recommendations were provided to the data controllers and processors:

- Organizing the data processing process through audio recording in such a way that data subjects are automatically informed about the audio recording and the purpose of its implementation, additionally, in an international language;
- Adoption of organizational and technical measures that ensure, through the so-called "APDB" program, the retrieval of a loan officer's data from the bank's "HR" database only by using the individual's unique identifying data;
- Delete text and audio-video recordings containing the applicant's data posted on the social network "Facebook";
- Delete messages containing third-party data received via email;
- When preparing payment order documents for the purpose of paying state duties, retain court rulings only to the extent necessary for the proper completion of the payment order;
- Implement a phone number verification process during user registration;
- Do not impose any fee or restriction on the exercise of the data subject's right to withdraw consent;
- Provide additional information to data subjects who became subscribers of the company on or after March 1, 2024, at the time of giving consent, regarding the mechanism/procedure for exercising the right to withdraw consent;
- Before obtaining consent from the data subject, inform them in clear and understandable manner about the mechanism/procedure for exercising the right to withdraw consent at any time;
- Obtain the legally required written consent from the data subject prior to processing any data other than the name, surname, address, telephone number, and e-mail address for direct marketing purposes;
- Cease the processing of the data subject's data for direct marketing purposes upon request;
- Discontinue obtaining consent from data subjects for direct marketing purposes through video banking; Cease processing data subjects' data for direct marketing purposes based on consents obtained through videobanking;

- For direct marketing purposes, provide comprehensive information in the consent text about the channels (such as SMS to the telephone number, e-mail, mobile banking, and others, if any) through which marketing messages will be sent to the data subject;

- In the "Standard Terms of Service for Banking Products" posted on the website, the data controller must provide detailed regulation of issues related to direct marketing as stipulated in Article 12 of the Law, including the types of data processed about the data subject and the channels used, such as e-mail, mobile banking, or other means;

- In cases where data processing for direct marketing is conducted through a data processor, the data controller must ensure that the agreement between the parties complies with the requirements established by Article 36 of the Law;

- When data processing for direct marketing is carried out through a data processor, the data controller must request prior information from the data processor regarding data processing in accordance with the law and ensure monitoring of the processing activities by the data processor;

- To prevent misleading data subjects, the data controller must ensure the dismantling of any camera installed in a residential building that simulates video monitoring;

- The data controller must terminate audio monitoring in the residence and delete all personal data collected through audio monitoring;

- The data controller must delete data collected through video cameras located in dental offices, dismantle such cameras, or reposition them so that their field of view does not directly include the procedure space and is directed only towards the entrance of the offices;

- The data controller must ensure that all actions performed on data stored in electronic form within the video recording system are recorded;

- The data controller must create individual usernames and passwords for persons authorized to access the video monitoring system.

- In the event of detecting an incident, ensuring its assessment in accordance with the requirements and criteria established by the Order No. 19 of the President of the Personal Data Protection Service dated February 28, 2024 " On the Approval of Criteria for Determining Incidents Posing a Significant Threat to Fundamental Human Rights and Freedoms and the Procedure for Notifying the Personal Data Protection Service of an Incident" and, where appropriate, notifying the Service of the incident in compliance with the same Rule;

- Organize the issuance of new debit cards to clients in a manner that ensures bank service center employees do not have access to the data on the cards;

- In accordance with the transparency principle outlined in Article 4 of the Law, inform data subjects, including the notifier, that to fully terminate their relationship with the bank, it is insufficient to simply refuse all services/products; rather, a specific request for complete termination of the legal relationship must be made;

- In compliance with the principle of transparency, ensure through the website and portal that data subjects are fully informed about the methods for requesting information (including credit reports and credit scores) regarding the processing of their data by the company. Additionally, provide alternative means for data subjects to obtain this information in an accessible manner, with or without a fee;

- Upon a data subject's request, provide the most comprehensive information possible about the processing of their data, including relevant links (if necessary), explanations, and additional instructions;

- Provide the applicant with an audio recording of a telephone conversation containing their data, while safeguarding the rights of any other persons whose voices are audible in the recording;

- Transfer copies of video recordings containing the applicant's data, collected by video cameras, to the data subject in a format that prevents the identification of third parties depicted in the recordings.

- In compliance with the principles of fairness and transparency stipulated in Article 4 of the Law, ensure that users/data subjects registered on the website are informed of any changes made to the "Personal Data Processing Policy" within a reasonable period of time; Ensuring that users/data subjects previously registered on the website are informed in advance of any upcoming changes to the "Personal Data Processing Policy" within a reasonable period of time;

- Ensuring compliance with the requirements of the principles of fairness and transparency established in Article 4 of the Law, as specifically outlined in a dedicated section of the "Personal Data Processing Policy";

- Ceasing the transfer of personal data (global network address/"IP Address") of users/data subjects (passengers/drivers) registered in the territory of Georgia through applications to the Russian Federation;

- One of the individuals, as an employee of the data controller and/or data processor, was advised to comply with the data security requirements stipulated by the Law of Georgia "On Personal Data Protection", including acting within the scope of the authority granted to them, and to maintain the secrecy and confidentiality of data, including after the termination of their official duties;

- One of the individuals, although processing data for a clearly personal purpose, was advised to process the data of minors only in exceptional cases, and only after ensuring that his personal purpose is reconciled with the best interests of the minor.

3. DATA PROCESSING BY LAW ENFORCEMENT BODIES

3.1. Key Directions and Trends

Examining the lawfulness of personal data processing within the activities of law enforcement agencies, including the conduct of covert investigative actions and the monitoring of activities carried out in the Electronic Communication Identification Data Central Bank, represents one of the key areas of the Personal Data Protection Service's work.

Law enforcement agencies process large volumes of personal data in the course of performing their duties and functions, including conducting police and preventive measures, investigating, prosecuting, enforcing penalties, and protecting against or preventing threats to public security.

The processing of personal data constitutes an interference with the right to privacy, as protected by Article 15 of the Constitution of Georgia and Article 8 of the European Convention on Human Rights. Unlawful data processing may result in significant violations of the rights of data subjects, including discrimination. Therefore, the collection of personal data for the purposes of legal proceedings must be limited to what is necessary and proportionate—either to prevent a real threat or to achieve a specific, legitimate aim such as the prevention, investigation, or prosecution of a particular crime.

The right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, which outlines the core principles governing it: personal data must be processed fairly, for specified purposes, with the consent of the data subject or on another legitimate legal basis[16].

Accordingly, in the activities of law enforcement agencies, it is essential to strike a fair and proportionate balance between the right to privacy and the interests of public security, so as not to hinder legal proceedings and, at the same time, to ensure the protection of personal data in this sector.

The primary objective of the Law of Georgia "On Personal Data Protection" is to safeguard fundamental human rights and freedoms, including the rights to privacy, family life, personal space, and communication. To support the realization of these rights, the new law introduced the role of a personal data protection officer. It is noteworthy that the law enforcement sector fulfilled the mandatory requirement to appoint or designate a personal data protection officer within the timeframe established by Article 90 of the Law, in accordance with Article 33. By June 1, 2024, personal data protection officers had been appointed or designated across all branches of the law enforcement system. In agencies with extensive responsibilities, dedicated structural units were created for personal data protection, or multiple individuals were assigned to this role. This development will contribute to constructive cooperation between law enforcement bodies and the Personal Data Protection Service in fulfilling the latter's mandate to conduct inspections under Article 51 of the Law, including the timely and comprehensive provision of information during inspections.

[16] **Handbook of European Data Protection Law, 2018 Edition.**

During the reporting period, the Service identified violations of the requirements set out in subparagraph "a" of paragraph 1 of Article 86 of the Law of Georgia "On Personal Data Protection" by two agencies. The violations concerned the failure to comply with the established procedure for submitting information and/or documentation to the President of the Personal Data Protection Service or an authorized representative of the Service. As a result, appropriate administrative liability was imposed on the agencies.

It is noteworthy that the law, which entered into force on March 1, 2024, introduced a new offense—obstructing the exercise of the rights granted by law to the President of the Personal Data Protection Service or an authorized representative of the Service—thereby underscoring the importance of complying with mandatory instructions issued by the Service. Moreover, the fulfillment of the functions assigned by law to the Personal Data Protection Officer will contribute to raising awareness and facilitating both the protection of data subjects' rights and the fulfillment of legal obligations by data controllers and/or data processors.

The analysis of inspections on the lawfulness of personal data processing conducted by law enforcement agencies during legal proceedings, along with the findings obtained from covert investigative actions and the monitoring of electronic activities, enables the Personal Data Protection Service to identify prevailing trends and challenges in this area.

By Order No. B/0046-2024 of the President of the Personal Data Protection Service, dated January 18, 2024, the "Main Directions of the 2024 Plan for Checks on the Legality of Personal Data Processing" and the "2024 Plan for Checks on the Legality of Personal Data Processing" were approved. These plans were developed by considering the impact of data processing on specific target groups or sectors, issues raised in statements or notifications submitted to the Service, as well as matters initiated ex officio or identified through the analysis and generalization of the previous year's inspection results.

Accordingly, the planned inspections conducted in law enforcement agencies focused on assessing the lawfulness of personal data processing, including the processing of special categories of data belonging to vulnerable groups—such as minors, persons with disabilities, and individuals under effective state control.

In addition to reviewing data processing practices within the context of labor relations in this sector, particular attention was given to areas introduced or emphasized by the current legislation, including audio monitoring. The inspections also addressed issues related to data security, electronic communications, the processing of data concerning accused and convicted individuals involved in special programs (e.g., suicide prevention), the use of modern technologies, and the implementation of covert investigative actions.

The above-mentioned inspections covered the activities of nearly all law enforcement agencies. Planned inspections were carried out at the Prosecutor's Office of Georgia; the Ministry of Internal Affairs of Georgia; the LEPL "Academy of the Ministry of Internal Affairs of Georgia"; the Special Penitentiary Service, a state sub-agency institution within the Ministry of Justice of Georgia; the LEPL "Operational-Technical Agency of Georgia"; the Ministry of Defense of Georgia; the Investigation Service of the Ministry of Finance of Georgia; the State Security Service; the Special Investigation Service; the National Agency for Crime Prevention, Non-custodial Sentences and Probation; the Ministry of Justice of Georgia; and the Special Service of State Protection of Georgia.

It is noteworthy that during the reporting period, cases of video recordings being made public and data being processed in violation of legal requirements—particularly regarding the disclosure of data in other ways, as well as the improper use of special categories of data such as convictions and health information—have decreased. The situation concerning compliance with the requirements stipulated by the Law on Information on Data has also improved, as evidenced by the reduction in the number of complaints and notifications received during the reporting period compared to 2023. However, the results of several inspections still revealed instances of incomplete provision of information to data subjects or refusal to provide requested materials or documentation.

The degree of compliance with the principle of proportionality in the processing of personal data by law enforcement agencies during legal proceedings remains a significant challenge. During the reporting period, instances of excessive data processing beyond the legitimate purpose and legal basis were once again identified. Issues related to the security sphere also remain problematic, including failures to implement adequate organizational and technical measures—such as recording access to data and applying information security mechanisms (confidentiality, integrity, availability) appropriate to the potential and accompanying threats. Additional concerns include incomplete or absent legal access procedures, improper designation of authorized personnel, the lack of personalized user accounts for individuals with access rights, and other related deficiencies.

It is noteworthy that law enforcement agencies violate the requirements of the law when processing personal data through video and audio monitoring, despite the fact that the law in force since March 1, 2024, establishes specific rules for implementing such monitoring. Articles 10 and 11 define additional obligations for data controllers, according to which those conducting video and audio monitoring must, in accordance with the principles set out in Article 4 of the Law, document in writing the purpose and scope of the monitoring, its duration and storage period, the procedures and conditions for accessing, storing, and destroying recordings, as well as mechanisms to protect the rights of data subjects.

Inspections carried out during the reporting period found no issues with the purpose and legal basis for processing data through video and audio monitoring. However, shortcomings and violations were identified regarding data security. In four cases, facts of incomplete data logging, absence of individual usernames and passwords, and failure or incomplete fulfillment of the obligation to develop the required written documentation were observed.

The Law of Georgia “On Personal Data Protection”, effective from March 1, 2024, has substantially revised the norms, approaches, and standards governing the processing of personal data. On one hand, the legislator clarified issues that had caused practical difficulties under the previous version of the law. On the other hand, new requirements for data controllers were introduced while certain prior obligations were abolished, balanced by other mandatory provisions for controllers. A notable example is Article 28 of the Law, which requires data controllers to maintain records of data processing activities and, upon request, provide this information to the Personal Data Protection Service.

The new law abolished the file system catalogue register and removed the obligation for data controllers to record information included in the file system catalogue in the register. However, Article 28 of the law introduced the obligation for data controllers to record information related

to data processing and, upon request, submit it to the Personal Data Protection Service no later than three working days. The new legislation eliminated the requirement for proactive submission of this document.

The results of inspections showed that, among the innovations of the law effective since March 1, 2024, fulfilling the obligation to record data processing information and notify the Personal Data Protection Service, as specified in Article 28, remains a challenge.

After March 1, 2024, within the framework of eight planned inspections conducted by the Department of Law Enforcement Sector Oversight, it was determined that none of the law enforcement agencies had developed a form for registering data processing activities. Some agencies indicated that the document was in the process of being developed, while others did not consider it necessary to produce a single document. In all such cases, by decision of the President of the Personal Data Protection Service, the agencies were instructed to document the information required by Article 28 of the Law in written or electronic form.

It is noteworthy that during one of the planned inspections, it was established that the agency had not created a single document, either in written or electronic form, reflecting information related to specific data processing activities. The agency believed that since the process was already conducted electronically, with information and documentation recorded in their electronic system, a separate record was unnecessary. However, upon inspection, it was found that the electronic system did not contain all the information required to be recorded by data controllers in accordance with Article 28 of the Law.

The Personal Data Protection Service did not accept the agency's explanation that the obligation under Article 28 of the Law was fulfilled by recording materials and related information in the electronic system. The law imposes this obligation on all data controllers and does not limit it to any specific means of data processing, whether automatic, semi-automatic, or manual. Accordingly, the law does not exempt data controllers who use automatic methods—where certain information is already electronically recorded—from this obligation. In light of the above, the agency was given a mandatory instruction to ensure the registration of information related to data processing in accordance with Article 28 of the Law of Georgia "On Personal Data Protection".

It is important that law enforcement agencies continue to consider and ensure the fulfillment of this obligation. The purpose of enacting this norm is to encourage controller to develop data protection measures that plan in advance for the lawful conduct of these processes and prevent violations of data processing.

3.2. Case Law

a. Data Availability

- **LEPL "Security Police Department" of the Ministry of Internal Affairs of Georgia**

During the reporting period, the Service examined a case regarding the violation of the rules for informing a citizen by the LEPL "Security Police Department" of the Ministry of Internal Affairs of Georgia, based on a citizen's application.

The Personal Data Protection Service concluded that upon receiving the application, the agency should have promptly informed the data subject—without delay or only after additional consultations—about the mandatory requirements specified by law for processing the application. The Security Police Department received a recommendation to this effect. Additionally, it was ordered to provide the applicant with the requested information and documentation within the legally established timeframe.

- **Ministry of Defense of Georgia**

During the planned inspection of the proportionality of processing data of individuals questioned in disciplinary proceedings by the General Inspectorate of the Ministry of Defense of Georgia (Main Department of Inspection in the Military and Civil Direction), it was found that the Ministry informed data subjects only with the following entry in the explanatory protocol: "During the course of the inspection, in order to achieve a legitimate purpose stipulated by law, their personal data is processed in compliance with the requirements of the Law of Georgia "On Personal Data Protection."

The Ministry of Defense was instructed to align the information included in the explanatory protocol with the requirements set forth in Article 24 of the Law, to ensure the data subject's rights are fully realized in cases where there are no grounds for restricting those rights during the data collection process directly from the data subject.

b. Labor Relations

- **Ministry of Defense of Georgia**

As part of a planned inspection, the Service examined the lawfulness of data processing by the Ministry of Defense of Georgia through audio monitoring during the interview process with candidates.

The Service found that the consent form submitted by the Ministry did not clearly inform candidates about the specific purpose of data processing. Consequently, the data controller

was instructed to revise the written consent form in accordance with Article 3, Subparagraph "n" of the Law of Georgia "On Personal Data Protection".

- **Ministry of Defense of Georgia**

As part of a planned inspection, the Service examined the proportionality of data processing of questioned persons during disciplinary proceedings conducted by the General Inspectorate of the Ministry of Defense of Georgia (Main Department of Inspection in the Military and Civil Directions).

To address identified shortcomings, the data controller was instructed to develop two differentiated protocol forms: one for questioning employees and another for third parties. The controller was also required to assess the necessity of the data processed during questioning, ensuring that only data essential for achieving the relevant legitimate purpose are collected through the protocol forms. Additional necessary data should be obtained, when applicable, directly through the content of explanatory notes during the consideration of specific disciplinary cases. Furthermore, the data controller was instructed to document in writing the storage terms for the questioned persons' data for the specific purpose and to specify the actions to be taken upon expiration of the storage period.

- **Ministry of Justice of Georgia**

As part of the planned inspection of the Ministry of Justice of Georgia, the Service examined the proportionality of the processing of data of individuals questioned during disciplinary proceedings conducted by the General Inspectorate.

Since the total procedural timeframes related to disciplinary proceedings did not amount to five years, the Service did not consider the justification for retaining such data for that duration. Accordingly, the data controller was instructed to define purpose-specific retention periods for the data of questioned individuals and to ensure the deletion or destruction of the data upon the expiration of those periods.

c. Vulnerable Groups

- **LEPL "Academy of the Ministry of Internal Affairs of Georgia"**

As part of a planned inspection, the Personal Data Protection Service examined the legality of video and audio monitoring implemented in the specialized interrogation room for minors and adjacent areas by the LEPL "Academy of the Ministry of Internal Affairs of Georgia" (hereinafter referred to as the Academy).

The Academy was recommended to ensure compliance with the requirements of the law by conducting simulation training, including video monitoring using cameras installed in the specialized space or, alternatively, by dismantling those cameras. Prior to simulation or dismantling, and in order to prevent misinterpretation by the minor data subjects regarding the nature of the monitoring, the cameras should be covered.

- **Prosecutor's Office of Georgia**

As part of a planned inspection, the Personal Data Protection Service examined the legality of data processing by the Prosecutor's Office of Georgia in the course of video and audio recording of minors in specialized interrogation spaces.

The Service emphasized that any person involved in the processing of minors' data is obligated to take all necessary measures to ensure that the process is transparent and conducted in a manner that does not endanger the legitimate interests of minors. Furthermore, minor data subjects must be clearly informed and have an understandable view of the data processing procedures. Accordingly, to ensure compliance with the obligations set out in paragraphs 8 and 9 of Article 10 and paragraphs 3 and 4 of Article 11 of the Law, the Prosecutor's Office was issued a mandatory instruction.

- **Prosecutor's Office of Georgia**

As part of a planned inspection, the Personal Data Protection Service examined the legality of data processing by the Prosecutor's Office of Georgia in the course of video and audio recording of minors in specialized interrogation spaces.

The Service emphasized that any person involved in the processing of minors' data is obligated to take all necessary measures to ensure that the process is transparent and conducted in a manner that does not endanger the legitimate interests of minors. Furthermore, minor data subjects must be clearly informed and have an understandable view of the data processing procedures. Accordingly, to ensure compliance with the obligations set out in paragraphs 8 and 9 of Article 10 and paragraphs 3 and 4 of Article 11 of the Law, the Prosecutor's Office was issued a mandatory instruction.

- **Special Penitentiary Service**

As part of a planned inspection, the Personal Data Protection Service examined the legality of data processing in the course of transferring data on convicts involved in the suicide prevention program to other state institutions by the state sub-agency institution of the Ministry of Justice of Georgia — the Special Penitentiary Service.

Although no violation of the law was identified as a result of the inspection, the Special Penitentiary Service was instructed to develop a standard written consent form that would fully

inform the beneficiary about the data to be transferred to the National Probation Agency and the purpose of such transfer, to be confirmed by the beneficiary in accordance with the procedure established by law. In addition, the agency was instructed to ensure the registration of information related to data processing in line with Article 28 of the Law of Georgia "On Personal Data Protection".

d. Video-Audio Monitoring

- **Special Investigation Service**

During the reporting period, as part of a case examined on the basis of an anonymous report, the Personal Data Protection Service assessed the legality of data processing through video surveillance cameras installed in the administrative building of the Special Investigation Service.

As a result of the inspection, the Special Investigation Service was found to have committed administrative violations under subparagraph "a" of paragraph 1 of Articles 69 and 76 of the Law of Georgia "On Personal Data Protection" and was declared in violation of the law. In order to address the identified shortcomings, the Service issued four (4) mandatory instructions to be fulfilled by the agency.

- **Ministry of Defense of Georgia**

As part of a planned inspection, the Personal Data Protection Service examined the legality of data processing carried out by the Ministry of Defense of Georgia (hereinafter referred to as the Ministry) during the interview process with candidates through audio monitoring.

In order to address the identified deficiency, the Ministry was instructed to inform data subjects about the implementation of audio monitoring in accordance with Article 10, paragraph 8 of the Law of Georgia "On Personal Data Protection".

e. Data Security

- **National Agency for Crime Prevention, Execution of Non-custodial Sentences and Probation**

The scope of the planned inspection of the National Agency for Crime Prevention, Execution of Non-custodial Sentences and Probation (hereinafter referred to as the Agency), a legal entity of public law operating under the jurisdiction of the Ministry of Justice of Georgia, included the study of the legality of the Agency's processing of data through the electronic surveillance system for monitoring house arrest.

The Service established the fact of violation of the requirements provided for in Article 27 of the Law of Georgia "On Personal Data Protection" by the Agency. It was recognized as a violator of the law for committing an administrative offense provided for in Article 76 of the same Law, for which a fine was imposed as a penalty. It was also given instructions to eliminate the violations and shortcomings identified within the framework of the inspection.

- **Prosecutor's Office of Georgia**

The Personal Data Protection Service, within the framework of a planned inspection regarding the legality of processing interview data in special spaces for minors during video-audio recording, assessed the circumstances as a violation of the data security requirements and recognized the Prosecutor's Office of Georgia as a violator of the administrative offense stipulated in Article 76 of the Law of Georgia "On Personal Data Protection." The Prosecutor's Office of Georgia was given relevant instructions to remedy the violations and shortcomings identified during the inspection. (The aforementioned decision of the President of the Service has been appealed).

- **Special Penitentiary Service**

Based on a citizen's application, the Personal Data Protection Service examined the issue of data security related to the processing of the applicant's personal data by the Special Penitentiary Service, a state sub-agency institution under the jurisdiction of the Ministry of Justice of Georgia, which was conducted through an email account created on the "Gmail" platform.

The Penitentiary Service was found to have committed an administrative offense under Article 76, Paragraph 1 of the Law of Georgia "On Personal Data Protection" and was issued a warning as a penalty. Additionally, it was ordered to implement organizational and technical measures appropriate to the potential and actual threats, ensuring the protection of data against loss, unlawful processing, destruction, deletion, modification, disclosure, or misuse during electronic data processing.

- **Ministry of Defense of Georgia**

Like many other inspections, the issue of the absence of an electronic journal (commonly referred to as "logging") to record actions performed on data was identified during a planned inspection of the Ministry of Defense of Georgia (hereinafter referred to as the Ministry). This inspection examined the legality of data processing related to audio monitoring conducted by the Ministry during the interview process with candidates.

The Ministry was found to have violated the law by committing an administrative offense under Article 76 and was issued a warning as a penalty, along with receiving appropriate instructions.

3.3. Instructions and Recommendations

Taking into account the cases studied by the Service, the identified deficient processes, specifics and trends:

- Law enforcement agencies should take appropriate measures to eliminate the risks of delays in the execution of data subjects' requests;
- In cases where the data subject cannot be identified from the application or accompanying documents submitted in connection with the exercise of their rights, the applicant should be informed of the deficiency immediately, at the earliest opportunity, in order to avoid exceeding the statutory deadline for reviewing the application and communicating the final outcome;
- Agencies must thoroughly assess the content of the request to ensure the complete transfer of case materials and documentation to which the data subject is legally entitled. In cases of restrictions on the data subject's rights, the agency must ensure access to information without undermining the purpose of the restriction, while strictly adhering to the principle of proportionality;
- In cases where data processing does not exist or the request is refused, provide substantiated information clearly indicating the legal grounds for refusal or restriction as defined by applicable law;
- Where data processing is based on the data subject's written consent, data controllers must ensure that the written consent form complies with the requirements of the Law of Georgia "On Personal Data Protection";
- Employers must assess the necessity and purpose of data processing during the interview stage of a service check, ensuring that only data essential for achieving the specific legitimate purpose is collected through the relevant fields of the forms. Any additional data necessary in the context of the individual case should be obtained directly through the content of the explanation, tailored to the specific circumstances;
- Data controllers shall determine the storage periods for data processed within the framework of official verification for a specific purpose, as well as the actions to be taken with respect to such data after the expiration of the storage period. They must also ensure the deletion or destruction of data retained beyond the necessary period;
- Law enforcement agencies shall conduct video-audio monitoring strictly for the purposes established by the Law of Georgia "On Personal Data Protection," and must define the duration of monitoring in accordance with the principles of necessity and proportionality;
- In spaces where video-audio monitoring is conducted, clearly visible warning signs must be placed, containing all information required under the Law of Georgia "On Personal Data Protection," in such a manner that data subjects are not misled about the presence or timing of the monitoring;

- When transferring video and audio recordings to third parties, act in accordance with the requirements of the applicable legislation and only in cases explicitly defined by law;
- Ensure the prior development of a written document regulating the course of video and audio monitoring, which shall outline the purpose and scope of the monitoring, its duration and storage period, the procedures and conditions for accessing, storing, and destroying recordings, as well as mechanisms for protecting the rights of the data subject;
- Ensure the recording of information related to data processing activities in accordance with Article 28 of the Law of Georgia "On Personal Data Protection";
- In cases where a data processor is involved in the data processing activities, provide that processor with clear and detailed instructions regarding data security measures. Additionally, ensure ongoing monitoring of data processing activities carried out by the processor;
- Access to personal data must be restricted and determined based on the specific duties and official authority of individual employees;
- When data is processed by non-automatic means, physical security measures must be ensured (e.g., storage in a locked cabinet; restricted employee access to premises where documentation is kept; securing doors with locks, etc.);
- When data is processed by automatic means, including through video-audio monitoring, electronic systems must be utilized that allow for the logging of all actions performed on the data, enabling identification of the person responsible for each specific action;
- Access to protected data within electronic systems, including technical tools used for video-audio monitoring, must be granted only through individual usernames and passwords;
- A password management policy must be developed to ensure that system data is protected by strong and complex passwords, in line with best security practices;
- Each person with access to the electronic system must have the technical ability and obligation to change the primary password of the user assigned to him/her.

4. PLANNED INSPECTION ON THE LAWFULNESS OF DATA PROCESSING

4.1. Key Directions and Trends

Planned inspection of the legality of personal data processing is carried out in accordance with the annual inspection plan approved by the President of the Personal Data Protection Service. The purpose of developing the annual inspection plan is to ensure the efficiency and consistency of the Service's activities, taking into account the diversity, dynamism, and complexity of data processing processes.

It is noteworthy that the annual plan is developed based on the study of the legislation regulating data protection, the practice of the Personal Data Protection Service, as well as the results of identifying and analyzing priority and/or high-risk data processing activities across various regions of Georgia. In determining risks with a high likelihood of violating human rights and freedoms in the data processing process, the Service is guided by the "Methodology for Developing a Plan for Planned Inspections of the Lawfulness of Personal Data Processing", which defines the procedure and criteria for selecting public and private sector agencies or organizations for the purpose of examining the lawfulness of personal data processing. Accordingly, the main directions and the plan for planned inspections of the lawfulness of personal data processing for 2024 were developed and approved by Order No. B/0046-2024 of the President of the Personal Data Protection Service, dated January 18, 2024.

It is also noteworthy that during the reporting period, several important directions and trends were identified based on systematically studied data processing practices.

a. Processing Data on Vulnerable Groups and Youth

The processing of personal data of persons with disabilities frequently entails the handling of special categories of personal data, particularly information related to the individual's physical and mental health. Such data is considered sensitive and requires a heightened standard of protection. In the case of minors and young people, it is important to recognize that they may lack full awareness of the risks, consequences, legal safeguards, and rights associated with the processing of their personal data. Unlawful data processing in these contexts can result in violations of dignity, stigmatization, bullying, discrimination, and other adverse impacts on a minor's emotional well-being and overall development. Therefore, protecting persons with disabilities, minors, and young people from such threats—and fostering a legal environment that prioritizes their support—is of critical importance to ensuring the realization of their rights. It is noteworthy that in 2024, the Personal Data Protection Service identified significant violations and deficiencies in the personal data processing practices of this category of data subjects by

various public agencies and private organizations, based on systematically studied cases.

In particular, when implementing video monitoring in schools and vocational educational institutions (colleges), there are frequent instances where the legally required warning signs are either insufficient in number or entirely absent in the areas under video surveillance, both within and around the premises. Moreover, in cases where such signs are present, they often fail to meet the requirements established under Article 10, Paragraph 9 of the Law of Georgia "On Personal Data Protection"—specifically, they frequently omit essential information such as the identity and contact details of the data controller. It is important to emphasize that, in order to ensure the exercise of data subjects' rights, the data controller or data processor is obligated to place video surveillance warning signs in a manner that makes the inscription and imagery visible and comprehensible to any natural person entering the monitored area. Furthermore, from the perspective of ensuring data subject awareness, it is essential not only to place the signs in clearly visible locations but also to ensure that they are easily perceptible—taking into account factors such as font size, color contrast, and overall design—so that they fully comply with the legal requirements.

In schools and vocational educational institutions (colleges), numerous video cameras are installed that are not connected to video recording devices and are non-functional. It is important to note that the mere presence of a video camera, even if it does not record, creates a misleading impression for data subjects regarding the processing of their personal data. This leads to a false perception of an interference with their right to privacy.

During the reporting period, a case was identified in which audio monitoring was conducted alongside video surveillance at a school, and neither the school nor the institution responsible for monitoring the surveillance system (LEPL — Educational Institution Mandatory Service) was aware of it. As a result, audio recordings containing a substantial amount of personal data were processed unlawfully.

In certain cases, video monitoring is conducted in educational areas (classrooms or auditoriums) within schools and colleges. According to the data controllers, the stated purposes of such monitoring—provided during inspections—include ensuring the safety of individuals, protecting property, and identifying individuals responsible for causing damage. However, it is important to emphasize that classrooms and auditoriums, by their nature, serve as learning environments for students and workplaces for teachers. Communication within these spaces is not limited solely to academic matters; it may also involve personal or general interactions—for example, private conversations with students during breaks or activities of a personal nature. Beyond the instructional function, the teacher–student relationship within this environment plays a crucial role in supporting the right to the free development of the individual, which falls under the scope of the right to privacy. Therefore, any interference with the data subject's private life must adhere to the principle of proportionality. Moreover, the purposes cited by data controllers may be achievable through alternative measures that entail less intrusion into the private lives of data subjects.

In a number of cases, schools and universities were found to store the personal data of minors and young individuals (including persons with disabilities) on a permanent basis, without specifying data retention periods or defining procedures for data handling after the expiration of such periods. On the one hand, indefinite storage of such information is inconsistent with the principle established under subparagraph "e" of paragraph 1 of Article 4 of the Law of Georgia

"On Personal Data Protection". On the other hand, prolonged or indefinite data retention increases the risk of unauthorized access, breaches of data processing rules, or data leakage. In one instance, following the expiration of the prescribed retention period for data stored electronically, the data was destroyed manually. It should be noted that non-automated (manual) deletion of records—particularly in the case of large volumes of data—entails a continuous need for human involvement, which increases the likelihood of errors and, as a result, the risk of unlawful data processing.

Additionally, instances of unlawful publication of the personal data of minors and young individuals by municipal authorities and educational institutions were identified on websites and/or social media platforms. Such cases included, for example: the publication of university entrance lists and exam results; personal data of children registered in kindergartens via the kindergarten registration portal; and information relating to beneficiaries of municipal education programs. In many of these cases, the data controllers cited the consent of the data subjects as the legal basis for disclosure. However, they were unable to demonstrate that such consent had been obtained in accordance with the legal requirements. Furthermore, the existence of a legitimate purpose justifying the disclosure of the data could not be substantiated

Inspections conducted by the Service revealed that many schools, colleges, universities, and municipal bodies had not implemented the necessary organizational and technical measures to ensure the security of both electronic and physical data relating to minors, young people, and persons with disabilities. Specifically, cases were identified where personal data in physical form was stored in a manner that made it accessible to unauthorized individuals. With regard to electronic data, organizations often failed to log or inadequately logged actions performed on the data, including in cases where direct access to the database was available. In many instances, electronic systems did not utilize individual user accounts for data access; instead, shared user credentials (a common account and password) were used, thereby increasing the risk of unauthorized or untraceable data access.

There were instances where electronic systems lacked complex password requirements, and passwords were not stored in encrypted form. Additionally, users were unable to change their passwords independently and were required to contact the system administrator to do so. It was also revealed that employees of certain institutions, in the course of performing their official duties, used personal email accounts to process data concerning minor beneficiaries. Furthermore, cases were identified in which individuals were granted access to data despite not requiring such access for the performance of their official responsibilities. These practices—particularly given the sensitive nature of the data—increase the risk of unlawful data processing and misuse of personal data for non-official purposes.

b. Data Processing within the Framework of an Employment Relationship

Within the framework of employment and related relationships, employers collect personal data of various types and volumes. Due to the nature of the employment relationship, employers often have access to employees' sensitive data and possess practical means for processing such information. Moreover, considering the hierarchical structure of employment, the organizational regulation of labor, and the economic dependence of employees on their employers, the processing of employees' personal data requires a heightened level of protection. Accordingly, organizations must ensure that data processing practices take into account the rights and interests of both employees and job applicants. Systematic assessments conducted by the Service have revealed that various public and private entities exhibit recurring violations and deficiencies in the processing of personal data within the context of employment.

In some instances, organizations published legal acts related to labor relations on their websites—such as those concerning employee leave, business trips, appointments, dismissals, and the imposition of disciplinary measures—without possessing an appropriate legal basis for such disclosure. These documents included the full names of employees, thereby allowing immediate identification of the data subjects. Moreover, the majority of these organizations regarded the publication of such documents as proactive disclosure of public information.

A case was identified in which an organization, in breach of the data minimization principle, granted access to employee and prospective employee data to 2,362 (two thousand three hundred sixty-two) employers who did not require such access to perform their duties.

In violation of Article 10, paragraph 3 of the Law of Georgia "On Personal Data Protection", several instances were identified in which video monitoring was conducted in employee workspaces or during the work process. During inspections, the data controllers cited the protection of property and security as the purposes for such monitoring. However, these purposes alone did not justify the lawfulness of video surveillance in cases where the same objectives could have been achieved through alternative means that would have resulted in less interference with employees' private lives. In one case, although the organization had implemented video monitoring in accordance with the general requirements of the law, employees were not provided with written notice clearly specifying the purpose(s) of the surveillance.

Instances were identified in which organizations engaged in unnecessary audio monitoring of employees' workspaces. During inspections, it was revealed that audio recording was being conducted using devices originally installed for video surveillance. In one case, an organization was aware that audio monitoring was taking place but failed to take any measures to cease this form of data processing. Additionally, a case was documented where continuous audio monitoring of employees' workspaces was carried out—even during periods when employees were not interacting with customers—under the justification of service quality control, improvement, and ensuring customer satisfaction. This practice resulted in a high level of interference with employees' private lives and disrupted the fair balance between the legitimate purpose of data processing, the interests of the data controller, and the rights of the data subjects.

Most organizations had not implemented adequate and effective measures to ensure the security of personal data. In some cases, organizations failed to log actions performed on personal data, while others did so only partially. Instances were also identified where data were

shared with unauthorized individuals, and access to protected electronic systems was granted using shared usernames and passwords. Logging actions performed on personal data is one of the most essential organizational and technical safeguards. It enables the identification of individuals responsible in the event of an unlawful disclosure. Moreover, this measure allows organizations to effectively monitor when, by whom, for what purpose, and to what extent data obtained within the framework of the employment relationship have been accessed.

In some cases, organizations had not defined retention periods for data stored in electronic form or planned to retain such data indefinitely—for example, for the purpose of statistical analysis. Instances were also identified where data were retained beyond the period originally specified. Over time, certain data become obsolete, lose their relevance, and no longer serve a justified purpose. Storing personal data only for the period necessary to achieve a legitimate purpose is one of the fundamental principles of lawful data processing.

c. Data Processing in the Healthcare Sector

Health information is classified as a special category of personal data and, due to its sensitive nature, is subject to a heightened standard of protection. Within the healthcare sector, citizens' personal data are processed on a daily basis in the context of various services. This includes processing by medical institutions, dental clinics, laboratories, and legal entities under public law responsible for managing and administering healthcare services. As health-related data may contain intimate details concerning an individual's private life, the provision of medical services, and their physical and mental health, the unlawful processing of such information can not only violate the right to privacy but may also lead to humiliation, stigmatization, or discrimination. Systematic assessments conducted by the Service have identified several violations and shortcomings in the data processing practices of the healthcare sector:

In some cases, medical service providers installed video monitoring systems in rooms designated for medical procedures, resulting in areas where patients receive care and undergo treatments falling within the cameras' field of view. As a result, video recordings of patients receiving medical procedures were obtained. Given that such spaces are associated with a reasonable expectation of privacy for the data subject, the use of video monitoring in these settings is incompatible with the requirements of the law.

A case was also identified in which a medical institution continuously conducted audio monitoring of communications between employees and patients for the purposes of service quality control, improvement, and ensuring customer satisfaction. While pursuing these objectives may constitute a legitimate interest of the institution, the method employed was not proportionate to the nature and volume of data being processed. The use of continuous audio surveillance resulted in disproportionate interference, including with the private lives of employees, thereby constituting a violation of the applicable rules governing audio monitoring.

It was revealed that one of the institutions implementing health protection measures was collecting personal data in volumes exceeding what was necessary to achieve a legitimate purpose. The collection of such unnecessary data poses a risk of disproportionate processing and constitutes a violation of the data minimization principle.

Additionally, cases were identified in which personal data were exchanged between institutions without the existence of a contract or agreement governing such exchange. This practice significantly increases the risk of unlawful data processing.

Most institutions had not implemented adequate and effective measures to ensure the security of personal data. In some cases, actions performed on data were recorded incompletely. Furthermore, employees accessed electronic systems using shared usernames and passwords. Instances of unauthorized data sharing were also identified. Without proper logging of actions taken on data, institutions are unable to effectively monitor who accessed the data, when, for what purpose, and to what extent. This significantly hampers the ability to identify the individual responsible in the event of unlawful disclosure, making accountability difficult or even impossible in such cases.

d. Data Processing in the Financial Sector

Compliance with data processing rules in the financial sector is of paramount importance due to the sensitive nature of financial information and the significant risks associated with its breach. Adherence to legal requirements is not only a statutory obligation for financial institutions but also a critical factor in maintaining consumer trust, preventing adverse consequences, and ensuring overall economic stability. Inspections carried out in 2024 revealed a number of violations and shortcomings in the data processing practices associated with financial activities.

Instances were identified in which data subjects were inadequately informed about matters related to the processing of their personal data. For example, in the context of hotline operations, certain financial institutions (including banks) recorded telephone conversations with customers; however, in some cases, data subjects were not fully informed about the ongoing audio monitoring. In one instance, although customers were warned that their calls would be recorded, there was a possibility that the conversation would not, in fact, be recorded—creating a risk of misleading the data subject by providing false or incomplete information about the processing of their data. Further cases were identified in which customers submitting personal data through the websites of insurance companies were either not informed or were insufficiently informed about the matters required under Article 24 of the Law of Georgia “On Personal Data Protection”. In some cases, organizations failed to present the required information in a single, accessible document; instead, it was dispersed across multiple, often lengthy, documents—contrary to the obligation to provide information in a clear and easily understandable form.

In some cases, improper data processing practices were identified. For example, on the website of one insurance company, customers were able to upload additional documentation—such as medical analyses and examination results related to the insurance case—in addition to the mandatory documents. However, according to the company’s own explanation, submission of such additional documentation had no impact on the review of the insurance case. Additionally, a case was identified in which the personal data of bank employees were transferred abroad in violation of the rules established by Article 37 of the Law of Georgia “On Personal Data Protection”.

Failure to take adequate and effective measures to ensure data security was also identified during inspections of financial organizations. For example, some organizations either did not re-

cord or incompletely recorded actions taken with respect to customer data. Additionally, cases were noted where employees accessed electronically processed data using a shared username, thereby preventing the identification of the individual performing actions on the data.

e. Other Prevailing Data Processing Issues

Certain violations and shortcomings have been identified in the data processing activities of both public institutions and private organizations across various sectors.

As a result of the examination of various data processing activities, instances of extensive data disclosure without an appropriate legal basis, as well as unauthorized disclosure to third parties—including through the granting of system access—were identified.

In some cases, violations of video monitoring regulations were found, including surveillance of spaces for which the institutions had no legitimate purpose or need. Furthermore, certain organizations conducted audio monitoring via video surveillance systems without a corresponding lawful basis, and despite the lack of necessity, no measures were taken to terminate this form of data processing.

Cases were identified in which the obligation to document, in writing, the processes of video monitoring, audio monitoring, and biometric data processing was inadequately fulfilled by the data controllers. Typically, the relevant documentation failed to comprehensively address the requirements set forth by law, such as the purpose and scope of monitoring, the duration and retention period of recordings, the rules and conditions for accessing, storing, and destroying recordings, as well as mechanisms for protecting the rights of data subjects.

A number of cases were identified where processors actively participated in data processing activities. Although agreements concluded between data controllers and data processors generally regulate the provision of services and include data processing tasks, they often fail to comply with the specific requirements outlined in Article 36 of the Law of Georgia “On Personal Data Protection”.

4.2. Case Law

a. Processing Data on Vulnerable Groups and Youth

- **N(N)LE - "Batumi Kindergarten Association"**

Within the framework of a planned inspection, the Service examined the legality of the processing of personal data of public kindergarten pupils during registration via the website of the N(N)LE — "Batumi Kindergarten Union" (hereinafter referred to as the Union of Kindergartens).

In connection with the identified violations, the Service issued a decision recognizing the Union of Kindergartens as a violator of the administrative offenses stipulated in Articles 67 and 76 of the Law of Georgia "On Personal Data Protection." Accordingly, the Union was ordered to rectify the aforementioned violations.

- **Zugdidi and Poti Municipality City Hall**

Within the framework of a planned inspection, the Service examined the legality of the processing of personal data of beneficiaries under the program for promoting the development of opportunities for children and youth implemented by the Zugdidi Municipality City Hall, as well as under the subprogram titled "Niko Nikoladze Scholarship (Award) for Successful Students" implemented by the Poti Municipality City Hall.

In connection with the identified violations, the Service recognized the Zugdidi Municipality City Hall and the Agency as administrative offenders under Article 76 of the Law of Georgia "On Personal Data Protection," and the Poti Municipality City Hall as an administrative offender under Article 67 of the same Law. At the same time, these municipalities and the Agency were ordered to eliminate the aforementioned violations.

b. Data Processing Processes in Private and Public Schools

Within the framework of a planned inspection, the Service examined the legality of the processing of personal data of students by three (3) private schools through electronic journals; the processing of data regarding students' disciplinary violations by two (2) public and two (2) private schools; and the processing of personal data of students with special educational needs through the creation and storage of individual education plans by two (2) public resource schools. During the inspections, more than seven thousand (7,000) students' data were processed in these schools, including one hundred (100) students with disabilities and special educational needs.

In connection with the aforementioned violations, three (3) schools were found to have committed administrative offenses under Article 76 of the Law of Georgia "On Personal Data Protection." Consequently, the schools were ordered to remedy the violations identified during the inspection.

c. Video Surveillance in Schools and Colleges

Within the framework of a planned inspection, the Service examined the legality of video surveillance conducted by two (2) state vocational education institutions/colleges (hereinafter referred to as the colleges), as well as by three (3) public and three (3) private schools. During the inspections, a total of 821 (eight hundred twenty-one) students were enrolled in the colleges, while the schools had a total of 6,348 (six thousand three hundred forty-eight) students.

The schools and the Resource Officers were recognized as administrative offenders for violations under Articles 69 and 76 of the Law of Georgia "On Personal Data Protection," while the colleges were found to have committed administrative offenses under Article 76 of the same Law. At the same time, instructions were issued to eliminate the aforementioned violations.

Within the framework of a planned inspection, the Service examined the legality of personal data processing through electronic academic management portals (hereinafter referred to as the portals) by two (2) private and two (2) public universities. Through these portals, the universities processed the personal data of more than 34,882 (thirty-four thousand eight hundred eighty-two) students. As a result of the inspections, one university was held administratively liable for committing offenses under Articles 68 and 76 of the Law of Georgia "On Personal Data Protection," while the other was found to have committed administrative offenses under Articles 44 and 46 of the Law of Georgia "On Personal Data Protection" adopted on 28 December 2011. At the same time, both universities were instructed to remedy the violations identified during the inspection.

Within the framework of a planned inspection, the Service examined the legality of the publication of personal data of prospective students and applicants for mobility by the LEPL — Shota Rustaveli Theatre and Film State University of Georgia on its website. It was established that the university had published information containing personal data of prospective students and mobility applicants without an appropriate legal basis as required under Article 5 of the Law of Georgia "On Personal Data Protection." As a result, the university was held administratively liable for committing an offense under Article 67 of the Law and was instructed to eliminate the aforementioned violation.

d. Data Protection in the Context of Employment Relations

- **Data disclosure by municipalities**

Within the framework of a planned inspection, the Service examined the lawfulness of publishing legal acts containing personal data by five (5) local self-government bodies (City Halls and Municipal Councils) through their official websites. The inspections revealed that, in addition to legal acts of public interest, the websites of the municipalities frequently published acts issued within the framework of employment relations—such as decisions on employee leave, business trips, appointments to and dismissals from positions, the imposition of disciplinary measures, and similar matters.

Local self-government bodies were found to have committed administrative offenses under Articles 66, 67, and 68 of the Law of Georgia "On Personal Data Protection" in connection with the above-mentioned violations. In addition, they were ordered to remove from their official websites any legal acts that had been published without a lawful basis and in violation of data processing principles.

- **LEPL - "State Employment Promotion Agency"**

Within the framework of a planned inspection, the Service examined the legality of personal data processing through the Employment Information System (hereinafter referred to as the Portal) in connection with the implementation of the Public Works Employment Promotion Sub-Program by the data controller — the Agency. The Portal is designed for the publication of public works vacancies by Providers (administrative bodies that create public work vacancies) within the framework of the Sub-Program and for generating electronic records of users. At the time of the inspection, the Portal contained information on 235,789 (two hundred thirty-five thousand seven hundred eighty-nine) users of the Sub-Program.

As a result, the Agency was held administratively liable for an offense under Article 66 of the Law of Georgia "On Personal Data Protection," while the LEPL "Information Technologies Agency" was found responsible for an administrative offense under Article 76 of the same Law. Both the data controller and the data processor were instructed to eliminate the aforementioned violations.

- **Ministry of Internally Displaced Persons from the Occupied Territories, Health, Labour and Social Affairs of Georgia**

Within the framework of a planned inspection, the Service examined the legality of the processing of personal data of labor migrants by the Ministry of Internally Displaced Persons from the Occupied Territories, Health, Labour and Social Affairs of Georgia (hereinafter referred to as the Ministry) through an electronic portal. It is noteworthy that during the inspection period, the Ministry's electronic system — maintained by the data processor, the LEPL "Information Technologies Agency" (hereinafter referred to as the Agency) — contained data on 33,411 (thirty-three thousand four hundred eleven) immigrants and 469 (four hundred sixty-nine) emigrants.

As a result, both the data controller — the Ministry — and the data processor — the Agency — were held administratively liable for offenses under Article 76 of the Law of Georgia "On Personal Data Protection" and were instructed to eliminate the aforementioned violations.

e. Data Processing in the Healthcare Sector

- **LEPL L. Sakvarelidze National Center for Disease Control and Public Health**

Within the framework of a planned inspection, the Personal Data Protection Service examined the legality of personal data processing by the LEPL — "L. Sakvarelidze National Center for Disease Control and Public Health" (hereinafter referred to as the Center) through the Unified Cancer Information System, in connection with the State Program for Early Detection and Screening of Diseases, specifically breast and cervical cancer screening. It is noteworthy that, within the scope of this service, the Center processes a significant volume of women's personal data, including special categories of data. During the inspection period, the system contained data on 159,364 (one hundred fifty-nine thousand three hundred sixty-four) beneficiaries.

As a result, both the Center and the LEPL "Information Technologies Agency" — were found to have committed an administrative offense under subparagraph "a" of paragraph 1 of Article 76 of the Law of Georgia "On Personal Data Protection" and were issued a warning as an administrative penalty. In addition, LEPL "Information Technologies Agency" was instructed to implement appropriate organizational and technical measures to ensure data security.

- **Kaspi and Telavi municipality city halls**

The Personal Data Protection Service conducted planned inspections of several municipal mayoralties concerning data processing practices within the framework of various social protection sub-programs. Among them, the legality of personal data processing by the Kaspi Municipality City Hall was examined in connection with the implementation of the free medicine

provision sub-program, as well as by the Telavi Municipality City Hall within the medical service and medicine assistance measures sub-program.

As a result, the Kaspi Municipality City Hall was found to have violated the principles and security rules of data processing, while the Telavi Municipality City Hall was held liable for violating data security rules. Both municipalities were instructed to eliminate the identified violations.

- **Medical laboratories and dental clinic**

Within the framework of a planned inspection, the Service examined the legality of video surveillance conducted by medical institutions — specifically, two laboratories and one dental clinic.

All three institutions were found to have violated the law in relation to video surveillance rules, while the dental clinic and one of the laboratories were additionally held administratively liable for violating audio surveillance rules. One of the laboratories was also held liable for breaching data security requirements.

As part of the inspection, all three medical institutions were instructed to eliminate the identified violations.

f. Data Processing in the Financial Sector

- **Bank hotline**

Within the framework of a planned inspection, the Service examined the legality of audio monitoring conducted via hotline services by JSC Liberty Bank, JSC ProCredit Bank, and JSC TBC Bank.

As a result of the inspections, JSC ProCredit Bank and JSC TBC Bank were found to have committed administrative offenses under paragraph 1 of Article 76 of the Law of Georgia “On Personal Data Protection.” All three banks were instructed to eliminate the above-mentioned violations.

- **Insurance companies**

Within the framework of a planned inspection, the Service examined the legality of the collection and storage of personal data of individuals holding health insurance policies by two (2) insurance companies through their websites.

As a result, both insurance companies were held administratively liable under Article 76 of the Law of Georgia "On Personal Data Protection" for violating data security requirements. In addition, one of the insurance companies was found to have committed an administrative offense under Article 66 of the Law due to the disproportionate volume of data processing. Both companies were instructed to eliminate the above-mentioned violations.

- **Private banks**

Within the framework of a planned inspection, the Service examined the legality of biometric data processing during the remote identification process by two (2) private banks.

As a result, both banks were instructed to ensure full compliance with the obligation to inform data subjects in accordance with paragraph 1 of Article 24 of the Law of Georgia "On Personal Data Protection" — specifically, to provide the required information in a simple and comprehensible form (for example, by consolidating all relevant information into a single document). The banks were also instructed to eliminate other violations identified during the inspection.

- **International data transfer by commercial banks**

Within the framework of a planned inspection, the Service examined the legality of international personal data transfers by two (2) commercial banks.

As a result, one of the banks, which had been transferring data to the Republic of Türkiye on the grounds set out in Article 37 of the Law, was found by the Service to have committed an administrative offense under Article 85 of the Law of Georgia "On Personal Data Protection." Both banks were instructed to eliminate the aforementioned violations

g. Cases Related to other Topical Issues of Data Processing

- **LLC Tbilisi Transport Company**

Within the framework of a planned inspection, the Service examined the legality of video surveillance conducted by LLC "Tbilisi Transport Company." It is noteworthy that, under powers delegated by the municipality, the company's primary activity is to provide public transportation services (metro, M3-category buses, cable cars, and minibuses), which are used daily by hundreds of thousands of individuals.

By decision of the Service, the company was found to have committed administrative offenses under subparagraph "a" of paragraph 1 of Article 67, subparagraph "a" of paragraph 1 of Article 69 (violation of video surveillance rules), subparagraph "a" of paragraph 1 of Article 69 (violation of audio surveillance rules), and subparagraph "a" of paragraph 1 of Article 76 of the Law of Georgia "On Personal Data Protection." At the same time, the company was instructed to eliminate the violations and deficiencies identified during the inspection.

- **Legality of Publishing Images in GIF Format by a Company**

Within the framework of a planned inspection, the Service examined the legality of publishing images of individuals in GIF format by a certain company. It is noteworthy that, based on an agreement with the client, the company provides services under the client's specified location and conditions, which include organizing the capturing of GIF-format images at the client's event using appropriate equipment and publishing them on the website.

By decision of the Service, the company was found to have committed administrative offenses, including those under subparagraph "a" of paragraph 1 of Article 67 of the Law of Georgia "On Personal Data Protection," and was instructed to eliminate the violations identified during the inspection.

- **Obligation to define in writing the processes of video monitoring, audio monitoring, and biometric data processing**

During the reporting period, the Service examined numerous cases regarding compliance with the aforementioned obligations. As part of planned inspections of two commercial banks concerning the legality of biometric data processing during remote identification, both banks were instructed to fully comply with the legislative requirements stipulated in paragraph 2 of Article 9 of the Law of Georgia "On Personal Data Protection," including defining the relevant processes in writing.

The Service also conducted planned inspections of two commercial banks regarding the legality of personal data processing via hotline services. The banks were ordered to align their audio monitoring procedures, particularly the recordings restricting data subject rights, with the regulations established by Article 21 of the Law.

In addition, the Service examined the legality of video surveillance in multiple institutions and organizations — including public schools, vocational colleges, and medical facilities — and issued mandatory instructions to evaluate and fully document the processes as prescribed by the relevant legal provisions.

- **Cases of compliance of written agreements/contracts between the data controller and the data processor with the law**

During planned inspections conducted by the Service, multiple instances were identified where data processors participated in the data processing activities. The school was instructed to bring the agreement concluded with the data processor into compliance with Article 36 of the Law of Georgia "On Personal Data Protection."

Within the framework of planned inspections, cases were also identified where data processors used subcontractors[17] in the data processing activities. In such cases, the Service instructed the parties to ensure that agreements include a provision requiring the prior written consent of the data controller when transferring processing responsibilities to other persons.

[17] **Any person to whom the data controller fully or partially delegates rights and obligations related to data processing.**

4.3. Instructions and Recommendations

Cases reviewed and measures taken by the Service during planned inspections confirm that various public institutions and private organizations have violated legal requirements in their data processing activities. To bring these processes into compliance with the law, numerous mandatory instructions have been issued. Based on the analysis of these instructions, all individuals involved in data processing activities should pay attention to the following issues:

- Data controllers must process personal data only when there is a legal basis provided by law. Furthermore, they must predefine the necessary timeframes for achieving the lawful purposes of data processing and, upon the achievement of these purposes, take the measures prescribed in subparagraph "e" of paragraph 1 of Article 4 of the Law. Additionally, personal data must be processed only to the extent necessary to achieve the relevant legitimate purpose.
- Ensuring the secure processing of data is of critical importance. Each person authorized to access data must do so only through a complex password-protected user account assigned specifically to them. Data controllers must ensure comprehensive logging and periodic monitoring of actions performed on electronic data, as this is an effective means of preventing unlawful data processing. It is essential that the information recorded in action logs (including video recording devices) be retained for at least the duration of the storage period for the personal data (including video recordings). Access to personal data must be restricted to employees who require it to perform their official duties. It is critically important to limit access for employees who only need temporary access to personal data to specific time periods, preventing continuous or prior access. Employers must also recognize that the use of personal email accounts by employees during the personal data processing activities contravenes the requirements established by the Law on Data Security, since such email accounts are not controlled by the employer and create risks of unlawful data processing.
- Based on an analysis of the circumstances and risks associated with data processing, appropriate measures must be developed to ensure the physical security of data (For example, the space designated for data processing should be arranged in a way that prevents unauthorized individuals from accessing personal data; data should be stored in lockable cabinets and/or other secure locations where access by unauthorized persons is not possible and other similar precautions should be taken).
- In the process of implementing video surveillance in general and vocational educational institutions, it is important to dismantle cameras that are non-functional. Warning signs required by law regarding the ongoing video surveillance must be clearly visible in all areas where surveillance is conducted. Since video surveillance systems often have the technical capability to record audio, it is essential to monitor whether audio surveillance is also being conducted. It must be taken into account that audio surveillance constitutes an intense interference with an individual's private life and may only be carried out in cases of justified necessity, in full compliance with the requirements established by law.
- Data controllers must cease conducting video surveillance in spaces designated for medical procedures, as individuals have a reasonable expectation of privacy in such areas.

- Data controllers who process the same data or participate in joint data processing activities must assess whether they qualify as joint data controllers. In such cases, they are required to fully comply with the obligations established under Article 35 of the Law with respect to joint data controllers.
- In cases where the data controller receives data in real-time from another subject's electronic system, it is important to ensure the proper volume, consistency, and uniformity of data processing. To achieve this, the issue of real-time data exchange between the subjects should be regulated through a written agreement.
- In cases where data is collected directly from the data subject, it is essential that data controllers ensure the provision of complete and accurate information regarding data processing, in compliance with the requirements of Article 24 of the Law. Furthermore, this information must be presented to the data subject in a simple and understandable form.
- The basis for international data transfer provided for in subparagraph "d" of paragraph 2 of Article 37 of the Law (the data subject's written consent) may be used only as an exception. Specifically, to ensure the protection of the fundamental rights of the data subject, it must first be verified whether the recipient country is included in the list of countries with adequate data protection guarantees, as approved by the order of the President of the Service. If the recipient country is not on this list and, therefore, cannot ensure adequate protection of personal data, the data controller must first attempt to establish such guarantees by concluding an agreement with the respective state, a competent public authority, a legal entity, a natural person, or an international organization. Only if it is impossible to establish such guarantees is international data transfer on the basis of the data subject's written consent considered permissible.
- In the process of collecting data directly from the data subject, data controllers must ensure the full provision of information required by law to the data subject. The contract between the data controller and the data processor must explicitly incorporate the conditions set out in paragraphs 1 and 2 of Article 36 of the Law
- Data controllers that carry out video surveillance, audio surveillance, or process biometric data are obliged to fully define the processing procedures in writing, in compliance with the requirements of the Law.

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

1. KEY DIRECTIONS AND TRENDS

One of the main areas of activity of the Personal Data Protection Service is the monitoring of the conduct of covert investigative actions, which includes overseeing the implementation of covert investigative measures and monitoring the activities carried out in the electronic data identification central bank.

The rights and obligations, forms of control, and relevant law enforcement and judicial bodies' procedures related to covert investigative actions defined by Article 40[16] of the Law of Georgia "On Personal Data Protection", valid until March 1, 2024, have been almost identically regulated under Article 54 of the new Law of Georgia "On Personal Data Protection". According to this, the Personal Data Protection Service continuously uses electronic control and special electronic control systems to monitor the conduct of covert investigative actions — including covert telephone communication surveillance and recording, as well as real-time geolocation determination.

Taking into account the specifics of conducting covert investigative actions, apart from the above, no other covert investigative actions are carried out through the electronic control system. Therefore, the Service is provided with physical documentation (court rulings and prosecutor's resolutions) authorizing the conduct of covert investigative actions. Within the scope of supervision, the Service compares the physical copies of court rulings and prosecutor's resolutions with the data specified in these documents to verify their accuracy and conformity with the electronic systems.

Based on the monitoring of the compliance between the documentation authorizing covert investigative actions and the data reflected in the electronic systems, the Personal Data Protection Service is empowered, pursuant to Article 143[6], paragraph 5 of the "Criminal Procedure Code of Georgia", to suspend a covert investigative action through the electronic control system if:

- An electronic copy of the judge's order authorizing the covert investigative action — covert telephone communication interception and recording — which contains only the requisites and operative part, was not submitted to the Personal Data Protection Service.
- A physical copy of the judge's order authorizing the covert investigative action — covert telephone communication interception and recording — which contains only the requisites and operative part, was not submitted to the Personal Data Protection Service immediately upon issuance of the order, but no later than 48 (forty-eight) hours thereafter.
- An electronic copy of the prosecutor's resolution authorizing the covert investigative action — covert telephone communication interception and recording — in cases of urgent

necessity, which contains only the requisites and operative part, was not submitted to the Personal Data Protection Service.

- Within 12 (twelve) hours from the start time indicated in the decision authorizing the covert investigative action, the Personal Data Protection Service was not provided with a physical copy of the prosecutor's resolution — containing only the requisites and the operative part — authorizing the covert investigative action of telephone communication interception and recording in cases of urgent necessity.
- The requisites and/or the operative part of the prosecutor's resolution submitted to the Personal Data Protection Service, either through the electronic system or in physical (documentary) form, contained ambiguities or inaccuracies.
- The information contained in the electronic version of the prosecutor's resolution submitted to the Personal Data Protection Service via the electronic system, and the information included in the physical (documentary) copy of the same resolution (specifically, the date and place of issuance; reference to the relevant article of the Criminal Code of Georgia under which the investigation is conducted; the prosecutor's name, surname, and signature; confidentiality classification; stamp; type of covert investigative action to be carried out; and the time period for the action (indicating both start and end dates and times) did not match.

It is noteworthy that the authority of the Personal Data Protection Service to suspend a covert investigative action also applies in cases where an ambiguity or inaccuracy is identified in the prosecutor's resolution. In the event such a deficiency is found in a judge's ruling, a notification is sent via the electronic control system to the LEPL — "Operative-Technical Agency of Georgia," as the body exclusively authorized to carry out the specific covert investigative action.

In the event of the suspension of a covert investigative action by the Personal Data Protection Service, the relevant authorities involved in the execution of such actions (LEPL — "Operative-Technical Agency of Georgia," the court, and the prosecutor or the authorized representative of the relevant investigative body), within the scope of their competence, are obliged to submit to the Service, within 3 (three) days from the suspension, both the material and electronic copies of the judge's ruling or the prosecutor's resolution confirming the elimination of the grounds for suspension. The Personal Data Protection Service confirms receipt of the evidence substantiating the elimination of the deficiency electronically, on the basis of which the covert investigative action may be resumed.

In the event that the Personal Data Protection Service identifies ambiguity or inaccuracy in a judge's ruling, the prosecutor is obliged, upon receipt of such information, to apply to the court that issued the ruling for correction of the deficiency. In turn, the court must remedy the ambiguity or inaccuracy in the ruling within 12 (twelve) hours from receiving the request and must provide the corrected ruling to the Personal Data Protection Service within 24 (twenty-four) hours after the correction.

The monitoring function also includes overseeing the post-completion measures of covert investigative actions. Specifically:

- Pursuant to the imperative requirement of Article 143⁶ of the Criminal Procedure Code of Georgia, the authorized state body, namely the LEPL — "Operative-Technical Agency of Georgia" must, immediately upon completion of a covert investigative action, prepare a protocol. This protocol must precisely state the legal basis for conducting the covert investigative action, its start and end times, the place of protocol preparation, the type of covert investigative action carried out and the technical means used during its conduct, the location where the covert investigative action was conducted, and the object of the covert investigative action.
- The report on the completion of the covert investigative action must be immediately submitted to the Personal Data Protection Service.
- Information obtained as a result of covert investigative actions must be immediately destroyed if it has no value for the investigation, if it was obtained during covert investigative actions conducted without a court order under urgent necessity, and despite the court's recognition of its legality, the prosecution did not present it as evidence to the court adjudicating the case on its merits; or if the material obtained through covert investigative actions does not relate to the criminal activity of the person but contains information about their or another person's private life. In such cases, following the decision of the prosecutor to suspend or terminate the covert investigative action, Article 143⁸, paragraph 5 of the Criminal Procedure Code of Georgia obliges the investigative body conducting the covert investigative action to draw up a report on the destruction of the material obtained through the covert investigative action, which must also be submitted to the Personal Data Protection Service.

The Personal Data Protection Service also exercises control over covert investigative actions through inspection (audit) of the lawfulness of data processing conducted by the data controller or data processor.

Taking into account the deficiencies and trends identified in its activities, the Personal Data Protection Service annually sets priority directions for the following year. For 2024, these priorities include the processing of data in the course of real-time geolocation determination and the verification of compliance with the legal obligation to submit reports on the completion of covert investigative actions to the Service.

Regarding the above-mentioned matters, the Personal Data Protection Service conducted 4 (four) planned inspections.[18] During these inspections, the Service identified 2 (two) violations and issued 4 (four) mandatory instructions for implementation, of which 1 (one) has been fulfilled, while the deadlines for completing the remaining 3 (three) have not yet expired. Additionally, the Service issued 2 (two) recommendations as part of these inspections.

[18] **Three (3) covert inspections were conducted.**

2. DECISIONS

a. State Security Service of Georgia

In 2024, a planned inspection was conducted regarding the Anti-Corruption Agency (Department) of the State Security Service of Georgia, as an authorized investigative body, concerning the obligation to submit protocols on the completion of covert investigative actions to the Personal Data Protection Service for the period from September 1, 2023, to March 14, 2024, in accordance with Article 143[6], Paragraph 14 of the Criminal Procedure Code of Georgia.

The inspection revealed that the State Security Service duly ensures the submission of protocols on the completion of covert investigative actions to the Personal Data Protection Service. Accordingly, no violations were identified during the inspection.

b. LEPL "Operational-Technical Agency of Georgia"

The Personal Data Protection Service conducted a planned inspection[19] of the LEPL — "Georgian Operational-Technical Agency" regarding the fulfillment of the obligation to provide, in real time, to the Personal Data Protection Service the logging data of automatic geolocation determination of mobile communication devices initiating notifications in the LEPL — "Public Safety Command Center 112," operating under the governance of the Ministry of Internal Affairs of Georgia, through the special electronic system for real-time geolocation control.

Based on the evidence obtained during the inspection, no violations were identified, nor was there a need to issue any directives or recommendations.

- **Control mechanism of the Personal Data Protection Service over the processing of electronic communication identification data during the conduct of investigative actions related to computer data**

From the perspective of the supervisory function of the Personal Data Protection Service, the mandate of the Service extends to investigative actions envisaged by Articles 136–138 of the Criminal Procedure Code of Georgia. The investigative actions under these articles, which do not constitute covert investigative actions, concern the request for information/documents relevant to a criminal case stored in computer data storage means, the ongoing collection of internet traffic data, and the extraction of substantive data.

[19] **The inspection began in late 2023 and ended in early 2024.**

It is advisable that the control mechanisms be regulated at the legislative level regarding the mandatory notification to the Personal Data Protection Service about the outcomes of information requests from computer systems and computer data storage means. Furthermore, it is recommended to revisit the issue in order to address the aforementioned inconsistencies through legislative amendments.

c. Investigation Service of the Ministry of Finance of Georgia

Within the framework of a planned inspection, the Personal Data Protection Service examined the compliance of the Investigative Department of the Tbilisi Main Directorate of the Investigative Service of the Ministry of Finance of Georgia with the obligation to submit to the Personal Data Protection Service the protocol on the completion of covert investigative actions carried out from June 1, 2024, to October 1, 2024, as prescribed by Article 1436, paragraph 14 of the Criminal Procedure Code of Georgia.

As a result of the inspection of the Investigative Service of the Ministry of Finance of Georgia, a violation was identified under subparagraph "a" of paragraph 1 of Article 66 of the Law of Georgia "On Personal Data Protection". At the same time, the Investigative Service of the Ministry of Finance of Georgia was recommended to adopt organizational measures to ensure the immediate submission of protocols on the completion of covert investigative actions to the Personal Data Protection Service.

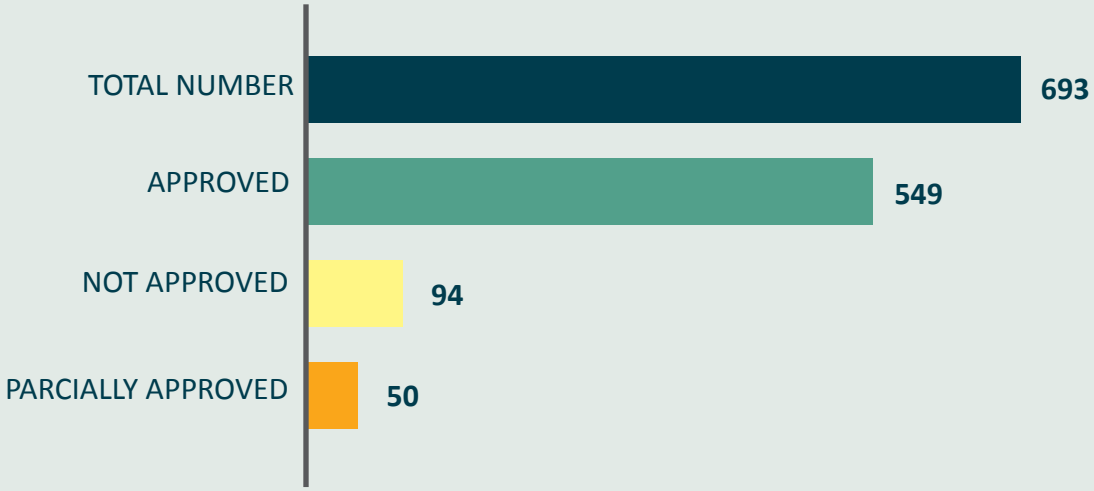
3. INSTRUCTIONS AND RECOMMENDATIONS

Covert investigative actions must be conducted by investigative bodies in full compliance with the rules and conditions established by the Criminal Procedure Code of Georgia, including the obligation to immediately submit protocols on the completion of covert investigative actions to the Personal Data Protection Service. Additionally, it is essential to adhere to the principles of data processing set forth by the Law of Georgia "On Personal Data Protection", such as data minimization, which entails processing only the amount of data necessary to achieve the relevant legitimate purpose.

According to the practice of the Service, delays in the submission of court rulings/prosecutor's decrees authorizing covert investigative actions, as well as protocols on the completion of such actions, continue to be observed.

In light of the identified trends, in 2025, the Personal Data Protection Service will pay particular attention to examining the legality of those processes that continue to present challenges.

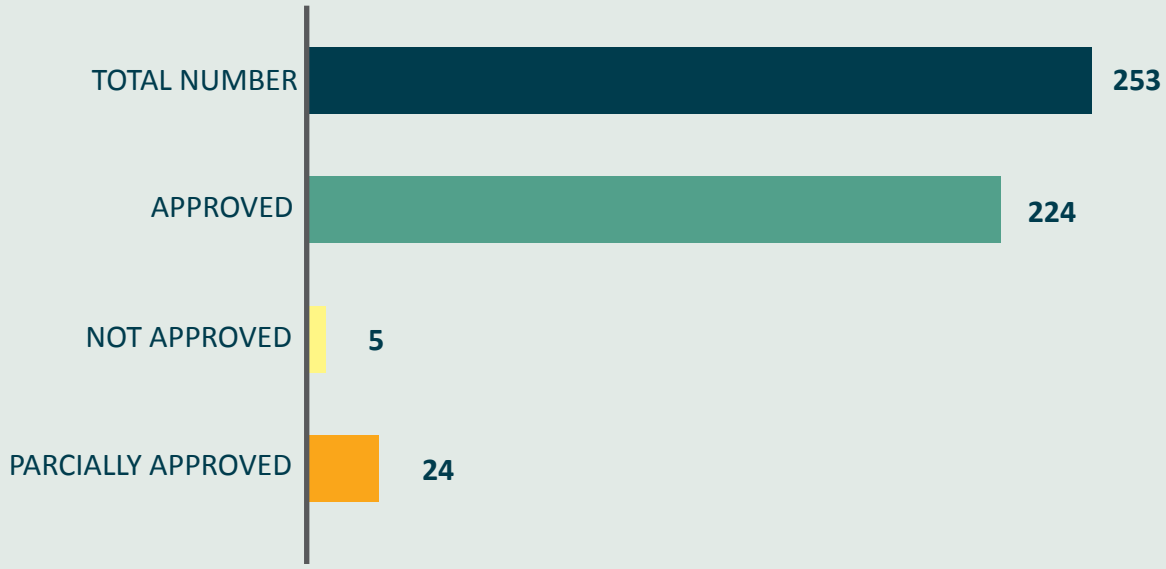
COURT RULINGS ON SECRET EAVESDROPPING AND RECORDING OF TELEPHONE COMMUNICATIONS



During the reporting period (2024), the court considered a total of 693 motions related to the secret eavesdropping and recording of telephone communications. The outcomes were as follows: 79% (549 motions) were fully approved, 14% (94 motions) were not approved, 7% (50 motions) were partially approved.

In comparison, in 2023, the court reviewed 859 motions on the same subject, with the following results 87% (744 motions) were fully approved, 9% (80 motions) were not approved, 4% (35 motions) were partially approved.

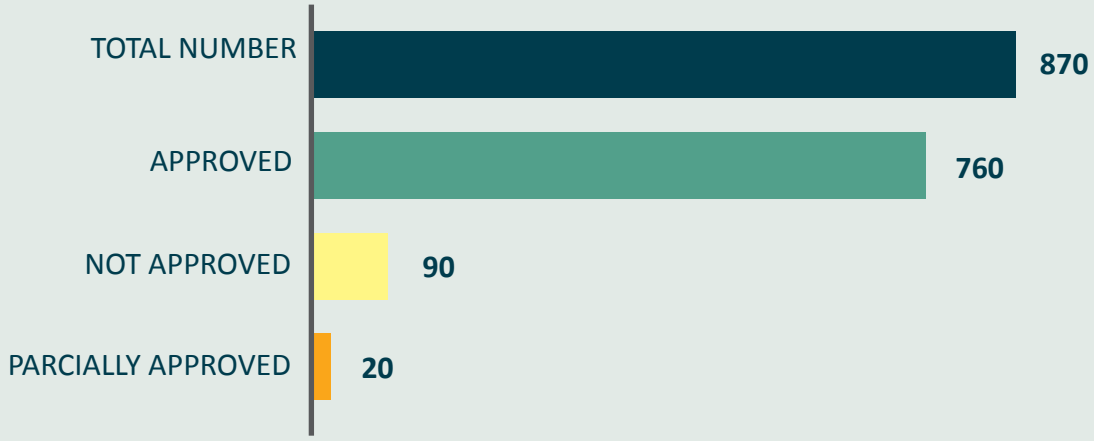
COURT RULINGS ON EXTENDING THE PERIOD FOR SECRET EAVESDROPPING AND RECORDING OF TELEPHONE COMMUNICATIONS



In 2024, the court reviewed 253 motions requesting an extension of the term for secret eavesdropping and recording of telephone communications. The outcomes were as follows: 224 motions (89%) were fully approved, 24 motions (9%) were partially approved, 5 motions (2%) were not approved.

In 2023, the court considered 228 similar motions, with the following results: 198 motions (87%) were fully approved; 22 motions (9%) were partially approved; 8 motions (4%) were not approved.

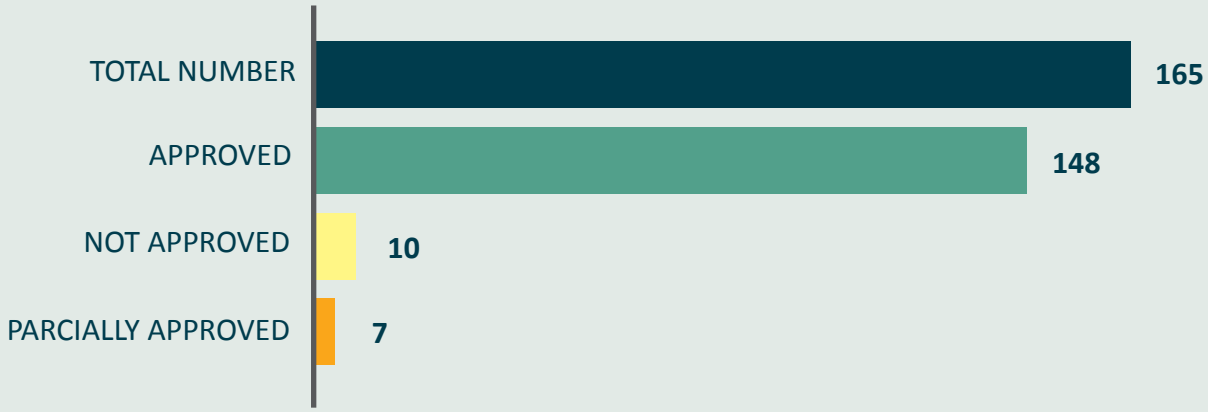
THE COURT RULINGS REGARDING THE COVERT VIDEO AND/OR AUDIO RECORDING, PHOTOGRAPHING



In 2024, the court reviewed 870 motions related to covert video and/or audio recording and photography. Of these, 88% (760 motions) were fully approved, 10% (90 motions) were not approved, and 2% (20 motions) were partially approved.

In 2023, the court reviewed 1,022 motions on the same subject. Of these, 93% (952 motions) were fully approved, 6.5% (66 motions) were not approved, and 0.4% (4 motions) were partially approved.

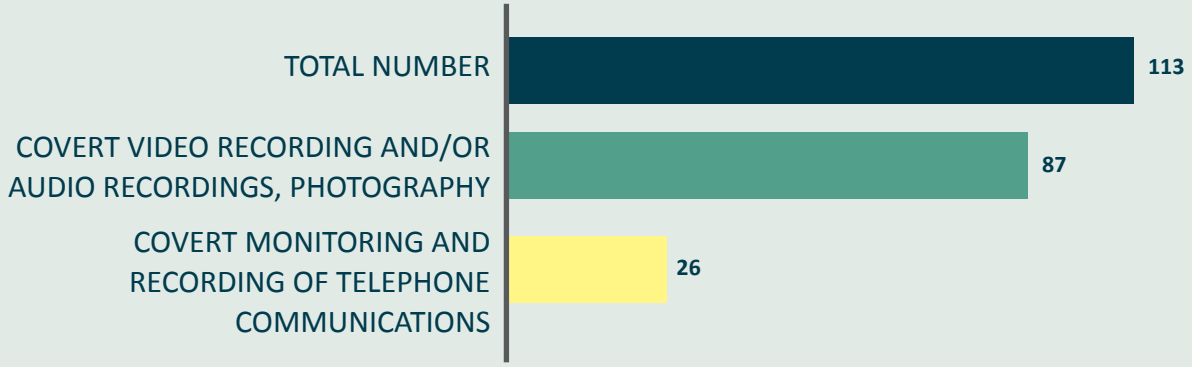
THE COURT RULINGS REGARDING EXTENSION OF TERM OF COVERT VIDEO AND/OR AUDIO RECORDING, PHOTOGRAPHING



In 2024, the court reviewed 165 motions for the extension of the period for covert video and/or audio recording and photography. Of these, 90% (148 motions) were fully approved, 6% (10 motions) were not approved, and 4% (7 motions) were partially approved.

In 2023, the court reviewed 122 such motions, of which 86% (105 motions) were fully approved, 12% (15 motions) were not approved, and 2% (2 motions) were partially approved.

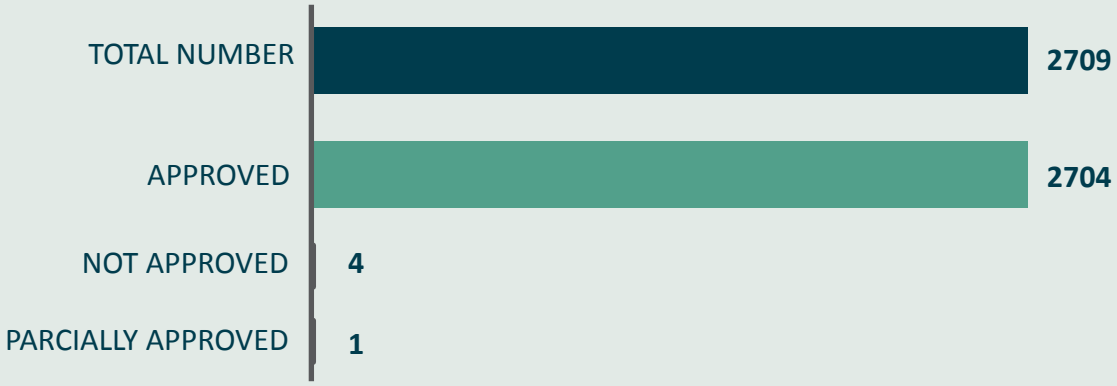
PROSECUTOR'S DECREES SUBMITTED TO THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA



In 2024, the Service was presented with 113 prosecutor's decrees authorizing covert investigative actions in cases of urgent necessity. Of these, 77% (87 decrees) concerned covert video and/or audio recording and photography, while 23% (26 decrees) concerned covert eavesdropping and the recording of telephone communications.

In 2023, the Service was presented with 126 prosecutor's decrees authorizing covert investigative actions in cases of urgent necessity.

COURT RULINGS SUBMITTED TO THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA



In 2024, the Personal Data Protection Service was presented with court rulings and, in cases of urgent necessity, prosecutor's decisions concerning requests for investigative actions, documents, or information under Article 136 of the Criminal Procedure Code. During the reporting period, the Service received 2,709 court rulings related to Article 136, of which 99.81% (2,704 rulings) were fully approved, 0.04% (1 ruling) was not approved, and 0.15% (4 rulings) were partially approved.

In 2023, the Service received 1,519 court rulings related to Article 136, of which 99% of the prosecutor's motions were approved.

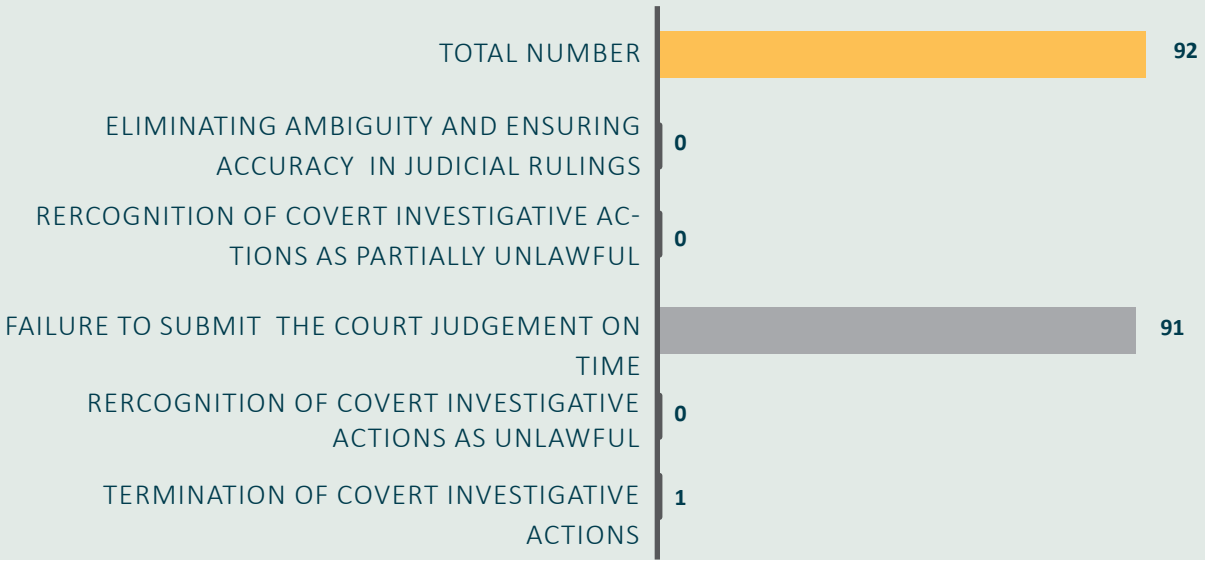
PROSECUTOR'S DECREES ON THE SUBMISSION OF INFORMATION OR DOCUMENT OCCASIONED BY THE URGENT NECESSITY

60

In 2024, the Personal Data Protection Service was presented with 60 prosecutor's decrees requesting investigative actions, documents, or information under Article 136 of the Criminal Procedure Code, submitted on the grounds of urgent necessity.

In 2023, 34 such prosecutor's decrees were submitted to the Service on the same legal basis.

USING THE SUSPENSION MECHANISM



In 2024, the Service used the suspension mechanism for covert eavesdropping and recording of telephone communications (through the electronic control system) in 92 cases. Of these, 91 were due to the late submission of a court ruling, and 1 was due to the termination of a covert investigative action.

In 2023, the Service used this suspension mechanism in 76 cases.

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

9

In 2024, the LEPL — "Georgian Operational-Technical Agency" — was notified 9 times about ambiguities and inaccuracies in court-issued permits for the covert interception and recording of telephone communications through the electronic control system. In 2023, the Agency received six such notifications.

NUMBER OF INCIDENTS DETECTED IN THE PROCESS OF COVERT EAVESDROPPING AND RECORDING OF TELEPHONE COMMUNICATIONS

1

In 2024, one (1) incident was detected during the process of covert eavesdropping and recording of telephone communications, as identified through the electronic control system.

ACTIVITY RECORDED IN THE CENTRAL BANK OF ELECTRONIC COMMUNICATIONS IDENTIFICATION DATA

89

In 2024, based on information received through the electronic control system of the Central Bank of Electronic Communication Identification Data, data was accessed 89 times by the LEPL "Operational-Technical Agency" pursuant to relevant court decisions.

In 2023, under the same procedure, data was accessed 69 times by the LEPL "Operational-Technical Agency," also on the basis of court decisions.

A DEFECT OR INCIDENT IDENTIFIED AS A RESULT OF MONITORING THE ACTIVITY CARRIED OUT IN THE CENTRAL BANK OF ELECTRONIC COMMUNICATION IDENTIFICATION DATA

During the reporting period, no deficiencies or incidents were identified as a result of monitoring the activities carried out within the Centralized Database of Electronic Communications Identification Data.

NOTIFICATIONS SUBMITTED BY ELECTRONIC COMMUNICATIONS COMPANIES

1965

In 2024, a total of 13 electronic communications companies submitted notifications to the Personal Data Protection Service. These notifications concerned the provision of information to law enforcement authorities, carried out on the basis of a 1965 court ruling during the reporting period.

In 2023, notifications were submitted to the service by 11 electronic communication companies, which during the reporting period provided information to law enforcement officials based on 1,756 court rulings.

CITIZENS' COMPLAINTS REGARDING COVERT INVESTIGATIVE ACTIONS CITIZENS' COMPLAINTS REGARDING COVERT INVESTIGATIVE ACTIONS

The protection of human rights and fundamental freedoms, including the right to privacy, is a core mission of the Personal Data Protection Service. In this regard, particular attention is given to overseeing and ensuring accountability in the area of covert investigative actions.

In 2024, no citizens contacted the Service regarding covert investigative actions allegedly carried out against them.

By contrast, in 2023, the Service received requests from four (4) individuals seeking information as to whether covert investigative measures had been conducted in relation to them.

COURT RULINGS ON THE REMOVAL AND FIXATION OF INFORMATION FROM COMMUNICATION CHANNELS AND COMPUTER SYSTEMS DURING COVERT INVESTIGATIVE ACTIONS

During the reporting period, the court did not consider any motion related to the removal and fixation of information from communication channels and computer systems during covert investigative actions.

In 2023, the court considered three (3) such motion: one (1) was granted; two (2) were denied.

COURT RULINGS ON THE ONGOING COLLECTION OF INTERNET TRAFFIC DATA

During the reporting period, the court did not consider any motion regarding the ongoing collection of Internet traffic data.

In 2023, the court considered one (1) such motion, which was granted.

NUMBER OF COURT RULINGS EXTENDING THE ONGOING COLLECTION OF INTERNET TRAFFIC DATA

1

The court reviewed one motion requesting an extension of the ongoing collection period for Internet traffic data until 2024, which was subsequently granted.

III

Enhancing Public Awareness and Educational Activities

CHAPTER III. ENHANCING PUBLIC AWARENESS AND EDUCATIONAL ACTIVITIES

1. AWARENESS-RAISING ACTIVITIES

In the modern era, data processing has become an integral part of everyday life, making personal data protection increasingly relevant. Public awareness and awareness raising in this field are essential, as effective data, protection cannot be achieved solely through legislative regulation—a thoughtful and responsible approach by each individual is also necessary. Therefore, the measures and activities actively implemented by the Service to raise public awareness are of particular importance. Equally vital is the Service's accountability to the public—ensuring the provision of comprehensive information about the state of data protection and the activities undertaken.

During the reporting period, the Personal Data Protection Service actively utilized all available communication channels and tools to effectively disseminate information to the public. In particular, in 2024, the Service made active use of social networks, traditional media, face-to-face meeting formats, as well as visual, video, and audio materials. The Service continuously monitors modern trends and emerging needs, striving to introduce innovations tailored to the interests of stakeholders. In this regard, the past year was no exception.

The year 2024 was especially significant for the Service, as the Law of Georgia "On Personal Data Protection" entered into force. The Service held numerous face-to-face meetings with data controllers, during which its representatives provided participants with detailed information about the innovations introduced by the new law. Various informational materials on current issues were distributed throughout the year via online platforms. The Service offered multiple formats of engagement to interested parties, including virtual meetings. Both traditional media and online channels were actively used to inform data subjects (citizens) about their rights.

Activities carried out by the Service to raise public awareness included:

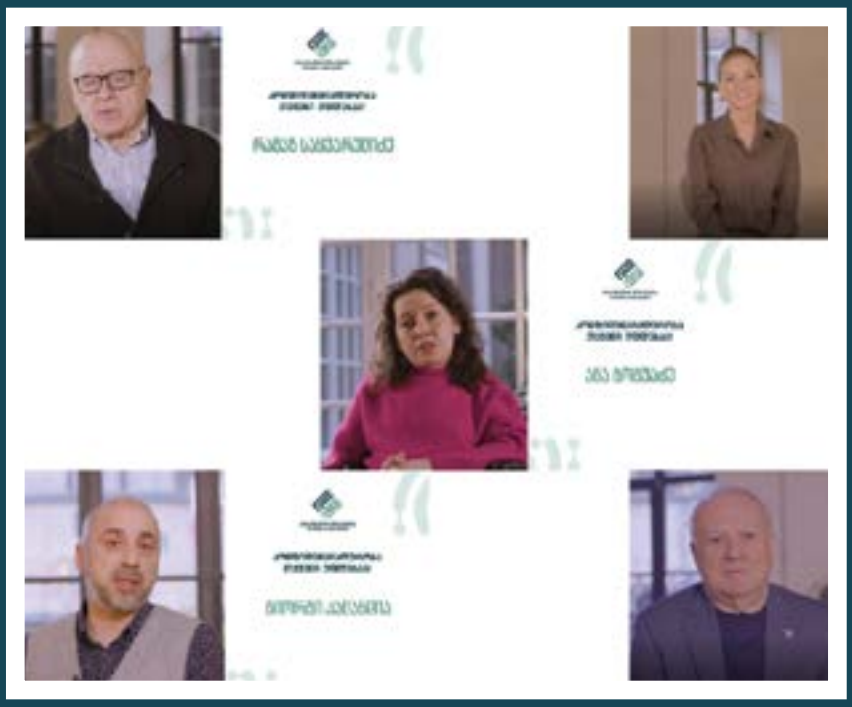
- **Video Materials**

The Service produced a total of 20 podcasts and 9 video clips, including one graphic video.

- Podcasts on Legal Innovations:

- **The Service produced 20 podcasts explaining the innovations introduced by the new Law of Georgia "On Personal Data Protection". Notably, 10 of these podcasts were made accessible to persons with disabilities through the inclusion of a sign language interpreter. The podcasts were disseminated across three platforms—Facebook, YouTube, and Spotify—and attracted nearly 600,000 views in total.**

- A graphic video explaining the key changes under the new law was created by the Service. A shorter version of this video aired as a public service announcement on the Public Broadcaster and Adjara Television, while the extended version was published on the official website and shared via social media. The total number of views reached approximately 130,000.



- **As part of the awareness campaign "Privacy is Your Right", the Service produced 7 video clips. Five of these were launched on January 28—International Data Protection Day—and featured well-known figures such as historian Giorgi Kalandia, psychologist Ramaz Sakvarelidze, doctor Nugzar Uberi, META project manager Mariam Sharangia, and photographer Ana Goguadze, each speaking on the importance of personal data protection. In the latter half of 2024, two additional videos were produced to engage regions with ethnic minority populations. These videos, in Armenian and Azerbaijani languages respectively, featured Doctor Varduhi Mosoyan and writer Kamran Kiriakov discussing the significance of data protection. All videos were published on the Service's website and social media platforms. The campaign received a strong public response, with a total of 1,012,986 views on Facebook alone.**

- One of the Service's key priorities during the reporting period was to enhance awareness around the protection of minors' personal data. Throughout the year, several guidelines on this subject were issued, and training sessions were held for students, teachers, and school administrators. In addition, a dedicated video featuring minors was published, in which they express their views and feelings about data protection. This initiative was aimed at both encouraging young people to reflect on their rights and highlighting the sensitivity of children's personal data. The video garnered approximately 127,000 views on social media platforms.

An essay competition was organized for schoolchildren across various regions of Georgia, attracting around 150 participants. The aim of the competition was to raise awareness among students about the importance of personal data protection.

- **Development of a Communication Strategy**

With financial support from the United States Agency for International Development (USAID), the Service has developed a comprehensive long-term communication strategy. The strategy was prepared by consultants from the firm "Gepra" in close collaboration with representatives of the Service.

The strategy is designed for three years and defines the main principles of the Service's strategic communication. Its goal is to raise public awareness of the Personal Data Protection Service as the body supervising the lawfulness of personal data processing, to increase public awareness of the issue of personal data protection, and to establish a culture of personal data protection and privacy.

- **Social Media**

Throughout the year, the Service actively utilized its official pages on various social media platforms—including Facebook, LinkedIn, X (formerly Twitter), and YouTube—to disseminate information. Alongside updates on meetings and other institutional activities, the Service regularly published its decisions, the "World Practice" series, announcements, press releases, quarterly activity reports, and statistical data. In 2024, two new thematic sections—"DataTech" (analytics) and "Datanewsroom"—were launched. These segments provide interested parties with insights into global developments in the field of data protection, as well as information on the data processing practices of popular applications and social networks.

The audience for the Service's official Facebook page continued to grow, reaching 23,500 subscribers as of December 2024.

During the year, the Service published 303 posts on Facebook, which generated 1,645,230 user impressions and 351,085 page visits.

- **„WhatsApp" channel**

Since July 2024, the Personal Data Protection Service has also begun sharing key updates and noteworthy trends related to its activities through its official WhatsApp channel.

- **New Website of the Service**

The new official website of the Personal Data Protection Service (www.pdps.ge) was launched on March 1, 2024. The website has been fully aligned with the requirements of the new Law "On Personal Data Protection", enhancing accessibility and providing users with improved access to information related to personal data protection.

In accordance with legal obligations, the new platform includes integrated functionalities that allow users to Report data protection incidents directly to the Service, Notify the Service about the designation or appointment of a personal data protection officer.

During the reporting period, the combined number of visitors to both the old and new websites totalled 167,994.

• Media Engagement

The year 2024 was particularly active in terms of the Service's media engagement. The adoption of the new Law "On Personal Data Protection" significantly increased media interest in the activities of the Personal Data Protection Service.

Throughout the year, the Service actively cooperated with various media outlets—including television, radio, print media, and online news agencies—to raise public awareness of the changes introduced by the new law and to promote a broader understanding of personal data protection issues.

Public information, transparency, and accountability remain among the Service's top priorities. In line with this, media representatives were invited to all major events organized by the Service.

Information was proactively disseminated about matters of high public interest, including key activities, events, and precedent-setting decisions of the Service.

In 2024, 30 press releases were distributed to media outlets and news agencies; Representatives of the Service participated in 25 programs, including news segments, morning and afternoon shows, as well as specialized radio and television broadcasts covering topics such as business, economics, and healthcare; Multiple interviews and expert; commentary were published in online media; Numerous statements were provided in response to journalists' inquiries on topical issues.

• Recommendations

During the reporting period, the Service prepared, translated, and published 28 recommendations related to the Law of Georgia "On Personal Data Protection", which entered into force on March 1, 2024:

1. Recommendation on Implementation of Measures Related to the Data Breaches;
2. Recommendation on Personal Data Protection Officer;
3. Recommendation on Right to Data Portability;
4. Recommendation on the Principle of Transparency;

5. Recommendation 05/2020 on Consent;
6. Recommendation 2/2019 on the processing of personal data in the context of the provision of online services to data subjects pursuant to Article 6(1)(b) of the GDPR;
7. Recommendation on the Right to Data Portability;
8. Recommendation 4/2019 on Article 25 Data Protection by Design and by Default;
9. Recommendation on Principles of Personal Data Processing;
10. Recommendation on Rights and Profiling Related to Automated Individual Decision-Making for the purposes of Regulation 2016/679;
11. Recommendation 3/2019 on the Processing of Personal Data by Video Devices;
12. Recommendations on Rights Related to Automated Individual Decision-Making and Profiling;
13. Recommendations on the Processing of Personal Data of Minors;
14. Guidelines 8/2020 on the Targeting of Social Media Users (Offering Information to a Target Groups);
15. Recommendations on the Implementation of Video and Audio Monitoring;
16. Guidelines 02/2021 on Virtual Voice Assistants;
17. Guidelines 04/2022 on the Method of Calculating Administrative Fines under the General Data Protection Regulation;
18. Recommendations on Data Protection Impact Assessment (DPIA);
19. Minimum Standard for Personal Data Protection Officers;
20. Failure of the Controller to Comply with the Request of the Data Protection Supervisory Authority (Comparative Legal Review);
21. Recommendations on Standard and Essential Contractual Clauses Between the Controller and Processor;
22. What You Need to Know About the Processing of Biometric Data;
23. Real-Time Video Monitoring in Kindergartens;
24. Guidelines for Small and Medium-Sized Enterprises;
25. Protection of Personal Data of Persons with Disabilities (PWDs) (Theory and Practice);
26. Newsletter: “Voter Rights and Certain Aspects of Personal Data Protection in the Electoral Process”;
27. Guideline on Inspection Techniques and Methods;
28. Guideline on the Processing of Personal Data for the Purposes of Voter Registration and Authentication.

2. CONDUCTED TRAININGS AND PUBLIC LECTURES

From January 1 to December 31, 2024, the Personal Data Protection Service actively carried out awareness-raising initiatives through lectures and training sessions.

In total, the Service held 108 meetings, reaching 6,522 participants. These included lectures tailored for specific agencies and organizations, both online and in-person sessions on legislative amendments, training courses for personal data protection officers, and regional outreach meetings.

Engagement was carried out with a wide range of stakeholders, including public and private sector representatives, educational institutions, and other relevant actors.

In addition, 260 consultation meetings were held with interested parties to discuss the innovations introduced by the new law.

PERSONAL DATA
PROTECTION SERVICE

IV

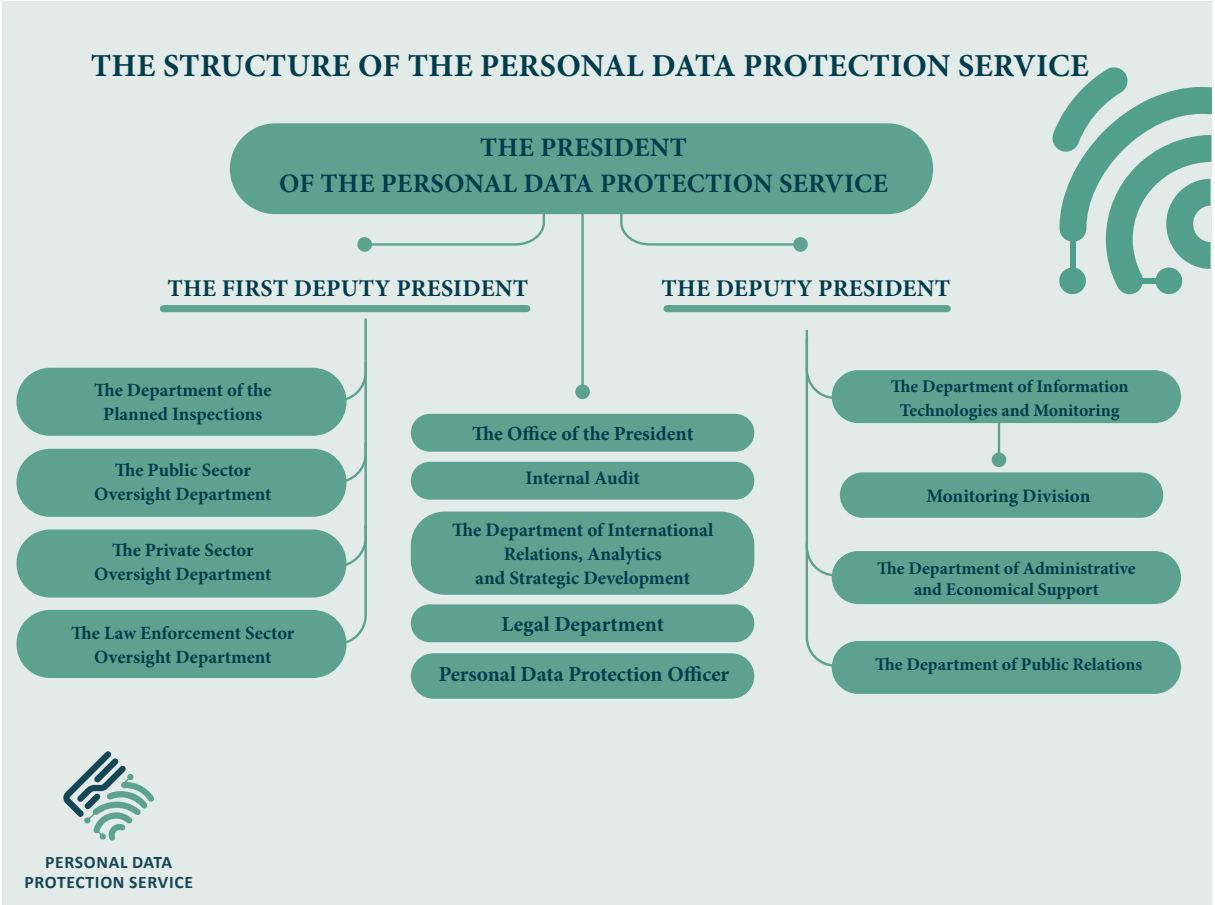
ADMINISTRATIVE MANAGEMENT OF THE SERVICE

CHAPTER IV. ADMINISTRATIVE MANAGEMENT OF THE SERVICE

1. ISSUES OF ORGANISATIONAL MANAGEMENT OF THE SERVICE

1.1. Institutional Strengthening and Internal Organization of the Service

In order to strengthen the Personal Data Protection Service and fulfill its strategic objectives—including staffing structural units and ensuring the full and effective implementation of the powers granted under the Law of Georgia "On Personal Data Protection", effective from March 1, 2024—the number of staff positions at the Service increased by 17 (seventeen) units. As of January 1, 2024, the total number of staff units stands at 84 (eighty-four).



- **Internship Program**

During the reporting period, the Personal Data Protection Service actively implemented its internship program, aimed at enhancing the qualifications and supporting the professional development of students and graduates from relevant higher education institutions. The program provided interns with the opportunity to gain practical experience, improve their competencies, and develop essential professional skills. It is noteworthy that five (5) students successfully completed their internship at the Service.

As of December 29, 2024, the number of people employed in the Personal Data Protection Service, categorized by employment type and gender:

#	INFORMATION ABOUT EMPLOYEES	NUMBER	NUMBER OF WOMAN	NUMBER OF MAN	WOMAN - %	MAN- %
1	TOTAL AMOUNT OF ACTING EMPLOYEES	95	46	49	48%	52%
2	STATE OFFICIALS	3	1	2	33%	67%
3	PROFESSIONAL CIVIL SERVANTS APPOINTED TO A MANAGERIAL POSITION	20	12	8	60%	40%
4	PROFESSIONAL CIVIL SERVANTS APPOINTED TO NON-MANAGERIAL POSITION	51	28	23	55%	45%
5	CONTRACT EMPLOYEES	21	5	16	24%	76%

1.2. Enhancing Employee Qualifications and Organizational Ethics

The year 2024 was significant in terms of employee professional development and qualification enhancement. During the reporting period, employees of the Personal Data Protection Service participated in various training activities and retraining programs. Specifically, within the framework of 18 sessions, 95 employees were retrained across several disciplines, including: time management; prevention of sexual harassment and related response mechanisms; emergency behavior protocols; first aid; and the development of both personal and professional competencies.



Within the framework of the European Union project "Support to Supervision of the Security Sector in Georgia," the Service co-organized a training session focused on current issues of personal data protection and the implementation of the new Law of Georgia "On Personal Data Protection," which came into force in March 2024. The training was led by EU expert Jekaterina Macuka, Head of the Latvian Personal Data Protection Supervisory Authority, and was conducted in line with European standards. Additionally, a virtual working meeting was held with representatives of the Croatian Personal Data Protection Supervisory Authority. The discussion covered two key topics: "Conducting Inspections Using the Data Protection Standard Model" and "Data Protection Impact Assessment".

The Service also launched an internal initiative, "Employees for Employees," as part of its ongoing qualification improvement efforts. Through this program, staff members delivered lecture-style trainings for their colleagues. As part of the same initiative, introductory training sessions were conducted to support the onboarding and integration of new employees. Staff also took part in trainings related to the rights of persons with disabilities and standards for effective communication with them.

During the reporting year, 37 (thirty-seven) competitive selection processes were announced, resulting in the employment of 28 (twenty-eight) new candidates. In accordance with the applicable legislation and based on performance evaluations for 2024, 12 (twelve) employees received a promotion in civil service grade. Furthermore, 35 (thirty-five) employees were awarded the appropriate state special rank of the Personal Data Protection Service.

2. BUDGET AND PERFORMANCE OF THE PERSONAL DATA PROTECTION SERVICE OF GEORGIA

2.1. Budget of the Service

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, with the necessary appropriations allocated under a separate budget code. The approved budget for 2024 amounted to 8,000,000 GEL. As of January 1, 2024, the Service had a total of 84 (eighty-four) staff positions, of which 65 (sixty-five) were filled by appointed civil servants. In accordance with its official structure and staffing list, the organizational structure of the Service includes nine (9) departments and the President's Office of the Service.

During the reporting period, the cash execution of the budget amounted to 7,303,385.95 GEL, which represents 91.29% of the annual plan.

№	ARTICLE OF BUDGET CLASSIFICATION	DETAILED PLAN	CASH FLOW PERFORMANCE
1	REMUNERATION	4 877 000	4 630 467
2	GOODS AND SERVICES	1 980 000	1 675 452
3	GRANTS	6 000	5 680
4	SOCIAL SECURITY	100 000	86 007
5	OTHER EXPENSES	135 000	108 372
6	NON-FINANCIAL ASSETS	902 000	797 409
	TOTAL	8 000 000	7 303 386

2.2. Salary, Bonus and Monetary Reward

During the reporting period, employees of the Personal Data Protection Service — including the President and Deputy Presidents of the Service — received a total of 3,698,300.18 GEL in basic salaries and 11,616.91 GEL in rank-based salary supplements.

Additionally, a total of 680,748.87 GEL was paid in bonuses, distributed as follows: 147,025.75 GEL in mandatory bonuses for employees holding special ranks, as provided by the Law of Georgia "On Personal Data Protection"; 33,647.12 GEL in mandatory bonuses in accordance with Article 26, Paragraph 4 of the Law of Georgia "On Public Service"; 500,076.00 GEL in bonuses for performing additional functions and overtime work.

In 2024, staff members were also awarded a bonus totalling 239,800.80 GEL.

The total labor remuneration for the average annual number of employees under an employment contract (22 employees) amounted to 592,068.00 GEL.

2.3. Vehicles

As of January 1, 2024, the Personal Data Protection Service had 10 (ten) vehicles on its balance sheet. The actual expenses for technical maintenance during the reporting period amounted to 12,197.27 GEL, while fuel costs totalled 41,670.42 GEL.

2.4. Real Estate Included In the Balance Sheet of the Service

№	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, BAKU STR. N48	PROPERTY OF A/R OF ADJARA; RIGHT TO USE BEFORE THE DEMAND	THE ADMINISTRATIVE BUILDING WHERE THE WESTERN REPRESENTATIVE OFFICE IS LOCATED

In order to provide employees with appropriate working space, four (4) structural units of the Service were located in leased private property. The lease cost for 2024 amounted to 160,992.93 GEL. As of 2024, the Service had two (2) real estate properties on its balance sheet, located at the following addresses: N. Vachnadze №7, Tbilisi, and Baku №48, Batumi.

By letter №5/40800 dated July 20, 2022, the LEPL "National Agency of State Property" transferred to the Personal Data Protection Service the right to lifelong use of premises located at Pushkin №10 / N. Vachnadze №7 / Tabukashvili №10, Tbilisi. One of these properties (land with cadastral code: 01.15.04.022.003, 01.511), with a total area of 162.39 sq. m, was officially registered under the name of the Personal Data Protection Service by the LEPL "National Agency of Public Registry" on August 24, 2022.

To accommodate expanded functions and responsibilities, and to create office, training, and conference spaces, the Service undertook renovation works on the specified area, located on the first floor of a building that holds the status of a cultural heritage monument. The renovations were carried out based on the consent of Tbilisi City Hall. The total cost of the renovation amounted to 373,170 GEL, while the cost of furnishing the space with office furniture and equipment totalled 39,914 GEL.

It is worth noting that the Service actively conducts training and consulting activities in the newly equipped space, significantly reducing budgetary expenses.

2.5. Business Trips and Other Expenses

During the reporting period, the Personal Data Protection Service incurred 26,965.00 GEL in domestic business trip expenses and 175,861.73 GEL in international travel expenses. Telecommunications costs amounted to 14,937.94 GEL. Additionally, in 2024, advertising expenses totaled 20,486.08 GEL. It is noteworthy that all advertising expenditures were exclusively directed toward activities aimed at raising public awareness.

Annexes

ANNEX №1. COMPLIANCE OF THE LAW OF GEORGIA "ON PERSONAL DATA PROTECTION" WITH THE EUROPEAN UNION'S DATA PROTECTION LEGAL FRAMEWORK

As a result of the adoption of the Law of Georgia "On Personal Data Protection" in 2023[20], which entered into force on March 1, 2024, national legislation regulating personal data protection has significantly aligned with European standards. Notably, the Personal Data Protection Service has published a special report on the implementation of the new law. This report outlines the practical application of newly introduced legal institutions, identifies challenges encountered during the implementation process, and details the activities undertaken by the Service.[21] The new law fully incorporates the core principles and legal mechanisms enshrined in the European Union's personal data protection framework—namely, the General Data Protection Regulation (GDPR)[22] and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (repealing Council Framework Decision 2008/977/JHA)[23]. Importantly, the law has received positive evaluation from international experts in the field. One such expert stated: *"The new Law of Georgia 'On Personal Data Protection' demonstrates that the legislator has thought intensively and carefully analyzed the EU data protection legislation, for which it deserves sincere congratulations! Georgia has already largely brought its national data protection law into line with the standards of the GDPR through the new law."*[24]

In addition, the Personal Data Protection Service has undertaken numerous initiatives to incorporate best European practices and standards, promote European values, and establish robust safeguards for the protection of personal data.[25]

This chapter provides a brief comparative legal overview of the relationship between the Georgian legislation and the aforementioned EU legal instruments.

---

[20] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 03/07/2023.

[21] Special Report on the Activities of the Personal Data Protection Service Implementation of the Law of Georgia "On Personal Data Protection", 2025.

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as the "Regulation" or "GDPR").

[23] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereinafter referred to as the "LED").

[24] N. Bernsdorf, "The New Law on Personal Data Protection in Georgia – A Brief Overview," Journal of Personal Data Protection Law, No. 1, 2024, 128.

[25] Special Report of the Personal Data Protection Service on International Activities Carried Out by the Service in 2022–2024 for Implementing the Best European Practices and Standards in Personal Data Protection Law, 2024.

1. GENERAL PROVISIONS

The aim of the Law of Georgia "On Personal Data Protection" is to safeguard the fundamental rights and freedoms of individuals, including the right to respect for private and family life, personal space, and communication, in the context of personal data processing. Similarly, the General Data Protection Regulation (GDPR) protects the fundamental rights and freedoms of natural persons, with particular emphasis on the right to the protection of personal data. One of the key objectives of the GDPR is to ensure the protection of individuals with regard to data processing while also laying down rules for the free movement of personal data. Notably, paragraph 3 of Article 1 of the GDPR explicitly prohibits restrictions on the free flow of personal data within the European Union on grounds relating to the protection of individuals with respect to personal data processing. As for the LED, it establishes minimum standards for the protection of individuals in connection with the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences, the execution of criminal penalties, and the protection against and prevention of threats to public security. The Directive imposes a clear obligation to safeguard the rights and freedoms of individuals, including the protection of their personal data.

• Scope of Application

The Law on Personal Data Protection applies to data processing conducted within the territory of Georgia by automatic and semi-automatic means, as well as to non-automatic processing if the data forms or becomes part of a file system. It also applies to data processing by non-resident entities using technical means available in Georgia, if such means are not used solely for data transit. However, the law does not apply to data processing carried out for personal or family activities. It also excludes processing by mass media aimed at informing the public, although such processing remains subject to the legal requirements for ensuring data security. Furthermore, the law does not apply to processing for academic, artistic, or literary purposes. The law does not apply to data processing carried out within the framework of state and economic security, defense, intelligence, and counterintelligence activities; nor to semi-automatic and non-automatic processing of data classified as state secrets for the purposes of crime prevention, investigation, criminal prosecution, operational-search measures, and the protection of public order; nor to data processing for the purpose of legal proceedings in court. With regard to the population census conducted under the Law of Georgia "On Official Statistics", only the provision regulating the grounds for processing special categories of data is inapplicable.[26] It is noteworthy that the law explicitly establishes an obligation of good faith in cases where a person involuntarily becomes a recipient of personal data. Furthermore, the law prohibits the misuse of access to personal data and any subsequent unlawful processing.

[26] **See Article 6 of the Law.**

The EU Regulation applies to the processing of personal data by automated and semi-automated means, as well as to processing by non-automated means where the data are, or are intended to become, part of a filing system. It governs data processing operations in both the private and public sectors. However, it does not apply to data processing carried out by EU institutions and bodies, or to activities that fall outside the scope of EU law. Additionally, it does not apply to processing carried out by a natural person in the course of a purely personal or household activity. The GDPR also applies to the processing of personal data by a controller or processor not established in the EU, where goods or services are offered to data subjects located within the EU.[27]

The LED applies to data processing operations carried out by competent authorities. It covers processing by automated, semi-automated, and non-automated means where the processed data form part of a filing system or are intended to become part of such a system. Consequently, its scope does not extend to files or records unless they are structured according to specific criteria. The Directive does not apply to data processing falling outside the jurisdiction of EU law, nor to processing operations carried out by various EU institutions or bodies.[28]

Based on a comparative legal analysis of the exceptions provided under Georgian and EU law, it is noteworthy that the GDPR defines exceptions for data processing conducted for personal and family purposes. Regarding state and economic security, defence, intelligence, and counter-intelligence activities, it is important to note that the LED explicitly excludes activities related to national security and the work of agencies or units operating in that domain. [29] However, it does apply to data processing carried out in the context of public security.

As for the exception under Georgian law concerning the semi-automatic and non-automatic processing of data classified as state secrets for the purposes of crime prevention, investigation, criminal prosecution, operational-search measures, and the maintenance of public order, it is notable that the Directive does not extend to such activities when they fall outside the scope of EU law.

Importantly, according to the preamble of the EU Regulation, in order to safeguard the independence of the judiciary in the performance of its judicial duties and decision-making process, the powers of supervisory authorities should not extend to data processing carried out by courts in the exercise of their judicial functions. Accordingly, the exception under Georgian law for the processing of data in the context of legal proceedings is consistent with EU data protection standards.

To ensure a balance between the right to personal data protection and the right to freedom of expression, the EU Regulation also provides, under Article 85(1) and (2), for exceptions in cases where data are processed for journalistic purposes or for academic, artistic, or literary expression. In this context, Member States may introduce exemptions or derogations from Chapters 8 (Remedies, Liability and Sanctions), 10 (Delegated Acts and Implementing Acts), and 11 (Transitional Provisions) of the Regulation, where necessary to reconcile data protection with freedom of expression.

---

[27] **See Article 3 of the Regulation.**

[28] **See Article 2 of the LED.**

[29] **Preamble to the LED, § 11.**

It is also worth noting that the Law of Georgia "On Personal Data Protection" imposes an obligation to ensure appropriate safeguards when processing personal data for archiving in the public interest, scientific or historical research, or statistical purposes, thereby aligning with the principles set forth in the EU Regulation. It is also worth noting that the Law of Georgia "On Personal Data Protection" imposes an obligation to ensure appropriate safeguards when processing personal data for archiving in the public interest, scientific or historical research, or statistical purposes, thereby aligning with the principles set forth in the EU Regulation.

Within the framework of national legislation on exceptions, it is noteworthy that the Law of Georgia "On Personal Data Protection", under Article 2, Paragraph 5, establishes an obligation of good faith for any person who inadvertently receives personal data not intended for them. Specifically, such a person must respect the rights of the data subject and refrain from any unlawful processing of the data. By introducing this obligation, the Georgian law sets a notably higher standard than that found in the EU Regulation and the LED, as neither instrument contains an explicit provision of comparable content.

- **Definition of Terms**

It is noteworthy that all three instruments—the GDPR, the LED, and the Georgian Law—define core sectoral terms in a similar manner.[30] However, in certain instances, the Georgian legislation additionally defines specific concepts that are not explicitly addressed in the relevant provisions of the GDPR or the LED. These include, for example: processing of data by automatic, semi-automatic, and non-automatic means; category of data recipient; personal data protection officer; video monitoring; audio monitoring; direct marketing; and data depersonalization. Conversely, unlike the GDPR and the LED , the Law of Georgia "On Personal Data Protection" does not define certain terms that pertain to legal mechanisms outside the scope of national regulation. These include, for example: main establishment, enterprise, international processing, international organization, group of undertakings, concerned supervisory authority, and binding corporate rules.

[30] **See Article 3 of the Law; Article 4 of the Regulation and Article 3 of the LED.**

2. LAWFULNESS OF DATA PROCESSING

• Principles of Data Processing

In line with the secondary legislation of the European Union, the Law of Georgia "On Personal Data Protection" sets out six fundamental principles governing personal data processing: lawfulness, fairness, and transparency (notably, the LED does not explicitly include transparency as a principle)[31]; purpose limitation; data minimization; accuracy; storage limitation; and data security.[32] All three instruments stipulate that the responsibility for demonstrating compliance with these principles (accountability) lie with the data controller or the processor.

It is important to highlight that Georgian legislation, unlike EU law, establishes an additional safeguard under the principle of lawful, fair, and transparent processing: personal data must also be processed in a manner that does not infringe upon the dignity of the data subject.[33] This specific requirement is not explicitly included in EU legislation. Under Georgian law, the obligation to ensure transparency in data processing is subject to certain exceptions as prescribed by law. In this regard, it is worth noting that, due to the nature and functions of law enforcement authorities, the principle of transparency is not included in the LED.

• Grounds for Data Processing

It is worth noting that all legal bases provided for under EU legislation are also present in Georgian national legislation.[34] In addition, Georgian law establishes the following legal bases: law provides for data processing; the data are publicly available according to the law or have been made publicly available by the data subject; and data processing is necessary to protect important public interests. With regard to these grounds, it should be noted that while the GDPR provides for data processing "for the performance of a task carried out in the public interest" or "in the exercise of official authority vested in the controller", it does not explicitly recognize the legal basis set out in Georgian law—namely, that data processing is necessary to protect important public interests.[35] As for the LED, given its specific scope, data processing is inherently linked to the exercise of authority by competent authorities. Furthermore, Georgian law places an explicit obligation on the controller to justify the legal basis for processing personal data.

According to the GDPR—as in Georgian legislation—one of the grounds for processing personal data is the consent of the data subject[36], with the conditions for obtaining and withdrawing consent regulated by a dedicated provision, namely Article 7 of the GDPR. In Georgian law, the conditions for obtaining consent are regulated both in relation to specific types of data

---

[31] **See Article 4(1) of the LED.**

[32] **See Articles 4 of the Law, 5 of the EU Regulation and 4, 5 and 7 of the LED.**

[33] **Article 4, paragraph 1, subparagraph "a" of the Law.**

[34] **See Articles 5 of the Law, 6 of the EU Regulation and 8 and 9 of the LED.**

[35] **Subparagraph "g" of paragraph 1 of Article 5 of the Law.**

[36] **For more information on this, see Section 3 on data subject rights.**

processing and through special provisions addressing the obligations of the controller when consent is obtained or withdrawn by the data subject[37] (e.g., in relation to direct marketing, audio surveillance, etc.). Thus, the standard set by Article 7 of the GDPR is reflected across several specific articles[38] in Georgian law. These provisions define the concept of consent, the procedure for its provision, and the obligations of the controller or processor when obtaining or responding to the withdrawal of consent. A comparative legal analysis of the GDPR and the Law of Georgia "On Personal Data Protection" shows that both acts place the burden of proof for the existence of valid consent on the controller. Furthermore, the conditions for withdrawing consent are consistent in both frameworks. In addition, both laws require the controller to assess the necessity of obtaining consent when determining whether it was given voluntarily.[39]

- **Legal Grounds for Processing Special Categories of Data**

The Law of Georgia "On Personal Data Protection" and the legislation of the European Union both establish special provisions regarding the processing of special categories of data. Article 9 of the GDPR, titled "Processing of special categories of personal data," is prohibitive in nature: its first paragraph defines the concept of such data and prohibits their processing, while paragraph 2 sets out specific exceptions under which processing is permitted.

A similar approach is adopted by the LED, which also defines special categories of data and permits their processing only if "the safeguards provided for in this Directive for the protection of the rights and freedoms of the data subject are ensured."[40] Georgian law mirrors this standard, requiring appropriate safeguards to protect the rights of the data subject and the existence of at least one legal basis specified in a special provision of the law to justify such processing. Based on a comparative legal analysis, it is notable that Georgian law incorporates all the legal bases for processing special category data found in the GDPR—except for one: the ground that allows processing when it is "necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity." Conversely, Georgian legislation includes additional legal bases not provided for in EU law.[41] As for the other legal grounds provided for under Georgian law,[42] these are not envisaged by the legislation of the European Union. In addition, the EU Regulation provides a specific provision regarding the processing of data related to criminal convictions and the commission of crimes.[43] Instead, these cases are governed by the general standard established in Article 6 of the Georgian law.

It is also noteworthy that Georgian law sets a higher standard in terms of consent for processing special category data. Specifically, when such processing is based on the data subject's consent, the law requires that consent be given in written form. The GDPR, by contrast, does not mandate the written form for consent in such cases.

---

[37] **Law, Article 32. See Article 3(l) and (m) of the Law, as well as Articles 20 and 32.**

[38] **See Article 3(l) and (m) of the Law, as well as Articles 20 and 32.**

[39] **See Article 7(4) of the Regulation and Article 32(2) of the Law.**

[40] **See Article 10 of the LED.**

[41] **Article 9, paragraph 2, subparagraph "f" of the Regulation.**

[42] **See Sub-paragraphs "g", "j", "m", "n", "o", "p", "q", "r", "s" of paragraph 1 of Article 6 of the Law.**

[43] **See Article 10 of the Regulation.**

- **Processing of Personal Data of Minors**

The Law of Georgia "On Personal Data Protection" and the General Data Protection Regulation (GDPR) both include specific provisions regarding the processing of personal data of minors. While Article 6 of the LED differentiates between various categories of data subjects, it does not contain a dedicated provision addressing the processing of minors' personal data. A comparative legal analysis reveals that the scope of Article 8 of the GDPR is limited to setting standards for the processing of minors' data in the context of offering information society services directly to a child. In contrast, Georgian legislation applies to the processing of minors' personal data across a broader range of areas and sectors, not limited to electronic services.[44] Moreover, Georgian law more comprehensively defines the standards for processing minors' data. These include the obligation to take into account the best interests of the child, as well as—when processing special categories of personal data—the requirement for written consent and stricter criteria regarding the validity of consent given by a parent or other legal representative. Regarding the age threshold for valid consent, Georgian law aligns with the standard established by the GDPR. In addition, both legal frameworks impose an obligation on the data controller to take reasonable measures—considering available technologies—to verify that consent has been provided or authorized by the person holding parental responsibility.

- **Other Specific Cases of Data Processing**

Georgian legislation also regulates the processing of personal data of a deceased person as a data subject. It is noteworthy that the GDPR does not contain a specific provision regarding the protection of data of deceased persons. According to Recital 27 of the GDPR preamble, "Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons." In contrast to national legislation, the GDPR does not establish a specific provision for the processing of biometric data; however, Article 9(4) of the Regulation states: "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

As for the LED, although it does not set out a specific rule on these categories of data, Article 10 stipulates that the processing of such data is permissible where appropriate safeguards are in place to protect the rights and freedoms of the data subject, and where the processing is based on one of the legal grounds provided for under Union or Member State law.

It is also worth noting that, unlike the Law of Georgia "On Personal Data Protection"[45], the legislation of the European Union does not provide for specific provisions governing video and audio surveillance. Nevertheless, the general standards of lawful data processing apply to such activities, including the obligation to adequately inform data subjects.[46]

---

[44] **See Article 7 of the Law.**

[45] **See Articles 10 and 11 of the Law.**

[46] **See Articles 13 and 14 of the Regulation.**

Article 12 of the Law of Georgia governs the processing of data for direct marketing purposes. According to Recital 70 of the GDPR preamble, "Where personal data are processed for direct marketing purposes, data subjects should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing. This right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information."

Moreover, Article 21(2) of the Regulation stipulates that, where data are processed for direct marketing purposes, the data subject shall have the right to object at any time to such processing. Article 21(3) further provides that, once the data subject objects to processing for direct marketing purposes, the data may no longer be processed for such purposes. Consistent with this standard, Article 12(4) of the Law of Georgia provides that, upon receiving a relevant request from the data subject, the processing of personal data for direct marketing purposes must be terminated no later than 7 working days from the date of the request. This provision reflects the principle established under Article 21(3) of the GDPR in Georgian legislation.

3. DATA SUBJECT RIGHTS

Georgian and EU legislation establishes the obligation of data controllers and processors to protect the rights of the data subject:

Category of data subject rights	Law of Georgia	EU regulation	LED
Right of data subjects to receive information on the processing of data	Article 13	Article 15	Article 14 Article 15
Right to access and to obtain a copy	Article 14	Article 12	Article 12
Right to the rectification, update and completion of data	Article 15	Article 16	Article 16, paragraph 1
Right to the termination of the processing, erasure or destruction of data	Article 16	Article 17 Article 21	Article 16, paragraph 2
Right to the blocking of data	Article 17	Article 18	Article 16, paragraph 3
Right to the data portability	Article 18	Article 20	[does not include]
Automated individual decision-making and related rights	Article 19	Article 22	Article 11
Right to withdraw consent	Article 20	Article 7, paragraph 3	[does not include]
Right to appeal	Article 22	Articles 77 Articles 78 Articles 79	Articles 52 Articles 53 Articles 54

According to the Law of Georgia "On Personal Data Protection" and European Union legislation, the data subject has the right to request confirmation from the controller as to whether personal data concerning him or her are being processed, whether the processing is lawful, and to receive relevant information free of charge upon request. It is noteworthy that the Law of Georgia, like the General Data Protection Regulation (GDPR) and the LED, ensures that information provided to the data subject is transparent, easily understandable, clear, and accessible. A key distinction lies in the response timeframes. The Law of Georgia sets a shorter deadline for responding to data subjects than the GDPR. Specifically, under Article 13 of the Georgian law,

information must be provided no later than 10 working days from the date of the request. In exceptional circumstances, and based on appropriate justification, this period may be extended by no more than 10 additional working days, and the data subject must be informed of such an extension immediately. In contrast, Article 12 of the GDPR stipulates that the controller shall provide the requested information without undue delay and in any event within one month of receiving the request. This period may be extended by an additional two months where necessary, considering the complexity and number of requests. The categories of information that may be accessed under Georgian law and the EU Regulation are identical, though both frameworks ensure the core right of access. In both legal systems, the data subject has the right to access their personal data and obtain copies free of charge. Georgian law provides for exceptions where fees may apply: a) if a fee is prescribed by Georgian legislation; or b) where the controller imposes a reasonable fee, based on the resources required to provide the data in a form other than the one in which they are stored, and/or due to the frequency of the requests.[47] Similarly, the GDPR allows controllers to charge a reasonable fee or refuse to act on the request if it is manifestly unfounded or excessive, particularly due to its repetitive nature.[48] In such cases, the fee must be proportionate to the administrative costs of providing the information, communication, or action requested. A similar approach is also adopted under the LED.[49]

It is noteworthy that Georgian legislation, unlike EU law, establishes a stricter timeframe for the exercise of the data subject's right to rectify, update, and/or complete inaccurate or incomplete data. In particular, pursuant to Article 15, paragraph 2 of the Law of Georgia "On Personal Data Protection", unless otherwise provided by Georgian legislation, such actions must be taken no later than 10 working days from the date of the request. If the request is refused, the data subject must be informed of the grounds for refusal and the procedure for appealing the decision must be explained. Moreover, Georgian law imposes an additional obligation on the controller to inform the data subject if objective circumstances render it impossible to fulfill the request. It also requires the controller to notify all data recipients, as well as other controllers and processors to whom the data has been transferred, about the rectification, update, or completion of the data.[50]

Regarding the right to erasure (right to be forgotten), a comparative analysis reveals that Georgian law provides for broader grounds for refusing to implement the data subject's request than those established under the GDPR. Under the GDPR, the controller is not obliged to erase the data if the processing is necessary for: The exercise of the freedom of expression and information; Compliance with a legal obligation under EU or Member State law, or for the performance of a task carried out in the public interest or in the exercise of official authority; Public interest in the area of public health (Article 9(2)(h) and (i), and Article 9(3)); Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes (Article 89(1)), where erasure would render impossible or seriously impair the achievement of the objectives of the processing; Establishment, exercise, or defense of legal claims.[51]

---

[47] **See Article 14, paragraph 1, subparagraphs "a" and "b" of the Law.**

[48] **See Article 12, paragraph 5 of the Regulation.**

[49] **See Article 12, paragraph 4 of the LED.**

[50] **See Article 15, paragraphs 5 and 6 of the Law.**

[51] **See Article 17, paragraph 3 of the Regulation.**

It is noteworthy that Georgian legislation, similar to the General Data Protection Regulation (GDPR), establishes legal grounds for restricting the data subject's right to erasure and for refusing related requests. These grounds include: data processing for the establishment, exercise, or defense of legal claims; processing necessary for the exercise of the right to freedom of expression and information; and processing carried out for archiving purposes in the public interest, as well as for scientific or historical research or statistical purposes, provided for by law—where the exercise of the right to interruption, erasure, or destruction of data would render impossible or seriously impair the achievement of the processing purposes.[52] In addition to these grounds, Article 16(3) of the Law of Georgia "On Personal Data Protection" further provides that the controller may refuse to interrupt, erase, or destroy data relating to the data subject (including profiling), even where a legal basis for processing exists under Articles 5 and 6 of the same Law.[53] Nevertheless, it is important to highlight that Georgian law, in contrast to the GDPR, sets a shorter deadline for responding to such requests. Specifically, unless otherwise provided by law, the controller is required to stop the processing and/or erase or destroy the data within 10 working days of receiving the request. If the request is denied, the data subject must be informed of the reasons for refusal and the procedure for appealing the decision.[54]

The right of a data subject to request data blocking is guaranteed under both Georgian and EU legislation. Notably, Georgian law provides for data blocking under similar circumstances as those outlined in the GDPR, while also introducing additional grounds for such a request, as set out in subparagraphs "d" and "e" of Article 17(1). At the same time, the Georgian law sets out specific grounds for restricting this right.[55] Unlike the GDPR and the LED, Georgian legislation establishes standards for determining the duration of blocking, mandates the linking of the blocking decision to the specific data, and requires that the data subject be informed immediately, but no later than three working days following the submission of the request, regarding either the implementation of the blocking or the grounds for refusal.[56]

The right to data portability, also referred to as the right to transfer data, is a newly introduced right under Georgian legislation. It is noteworthy that the Georgian regulation aligns with the relevant provisions of the GDPR. Under the GDPR, this right may be restricted when data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority conferred on the controller. Additionally, the exercise of the right to portability must not adversely affect the rights and freedoms of others.[57]

The regulation of automated individual decision-making and the associated rights under Article 19 of the Law of Georgia "On Personal Data Protection" is also in accordance with EU law. Specifically, the Georgian law, the GDPR, and the LED all guarantee that the data subject shall not be subject to a decision based solely on automated processing, including profiling, which

---

[52] **See Article 16, paragraph 3 of the Law.**

[53] **See Article 16, paragraph 3, subparagraph "a" of the Law.**

[54] **See Article 16, paragraph 2 of the Law.**

[55] **See Article 17, paragraph 2 of the Law.**

[56] **See Article 17, paragraphs 4 and 5 of the Law.**

[57] **See Article 20(3) and (4) of the Regulation.**

produces legal effects or significantly affects the data subject. Legal bases for restricting this right are also provided and, upon comparative analysis, are found to be mutually compatible. Furthermore, all three legal frameworks—the Georgian law, the GDPR, and the LED—permit the use of special categories of data in automated decision-making only where such processing is strictly necessary and adequately safeguarded. Under the GDPR, this is permitted if one of the conditions in Article 9(2)(a)[58] or (g) [59] is met and appropriate safeguards for the rights and freedoms of the data subject are in place. Georgian law allows the use of special categories of data for automated decision-making where similar safeguards are implemented, and where one of the legal bases under Article 6(1), subparagraphs "a", "f" or "k" applies. These include: the written consent of the data subject; processing for purposes of crime prevention, investigation, prosecution, the administration of justice, execution of penalties, or other public legal interests (subparagraph "f"); and data processing to ensure information security and cybersecurity (subparagraph "k").

The Law of Georgia "On Personal Data Protection" also specifically regulates the withdrawal of consent granted by the data subject. Like the GDPR, it grants the data subject the right to withdraw consent at any time. Furthermore, it details the standards for exercising this right, including the right to withdraw consent without explanation or justification, and the obligation of the controller to cease data processing and/or delete or destroy the data within 10 working days from the date of the request. Georgian law also ensures that the withdrawal may be made in the same form as the consent was originally given and guarantees the data subject's right to be informed of the legal consequences of withdrawing consent.[60]

The rights of the data subject include the right to appeal, which represents one of the most effective legal remedies for safeguarding the rights afforded to individuals. It is noteworthy that Georgian legislation, consistent with EU law, provides data subjects with the ability to apply to a supervisory authority, a court, and/or a higher administrative authority for the protection of their personal data rights.[61]

Restrictions on the rights of the data subject are permissible when they are established by law, pursue the essence of fundamental rights and freedoms, and constitute a necessary and proportionate measure in a democratic society.[62] In accordance with Article 21 of the Law of Georgia "On Personal Data Protection", such restrictions are allowed in order to protect interests that are also recognized by the General Data Protection Regulation (GDPR). However, unlike

---

[58] "There is the explicit consent of the data subject to the processing of such personal data for one or more specific purposes, unless, under Member State law, the data subject cannot object to the prohibition referred to in the first paragraph."

[59] "The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law, which shall be proportionate to the purpose pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject."

[60] See Article 20 of the Law.

[61] See Article 22 of the Law.

[62] See Article 21, paragraph 1 of the Law.

the GDPR, Georgian legislation additionally allows for restrictions on the basis of protecting state, commercial, professional, and other types of legally protected secrets.[63] The Georgian law also introduces the principle of proportionality in relation to restrictions, requiring that any limitation of data subject rights be proportionate to the legitimate aim pursued. Furthermore, it places the burden of proof on the data controller to justify the necessity of the restriction, and imposes an obligation to inform the data subject of such restrictions—unless doing so would jeopardize the legitimate interest of the restriction. Unlike the EU Regulation, however, the Georgian law does not include a specific obligation requiring that legal measures taken to restrict data subject rights contain minimum transparency elements, such as: the purpose of data processing, the categories of data affected the scope of the imposed restriction, or safeguards against unlawful use, access, or disclosure of the data.[64]

[63] **See Article 21, paragraph 1, subparagraph "h" of the Law.**

[64] **See Article 23, paragraph 2 of the Regulation.**

4. OBLIGATIONS OF THE CONTROLLER AND THE PROCESSOR

Georgian legislation, in alignment with the General Data Protection Regulation (GDPR) and the LED, establishes a general obligation for both the controller and the processor to take all necessary measures to ensure compliance with the law and, where required, to demonstrate such compliance.[65] In particular, Article 24 of the GDPR obliges the controller to implement appropriate technical and organizational measures to ensure, and be able to demonstrate, that data processing is carried out in accordance with the Regulation. These measures must be reviewed and updated where necessary. Similarly, Article 12 of the LED provides for the obligation to adopt appropriate measures to safeguard the rights of the data subject.

Beyond obligations related to the exercise of the data subject's rights, both Georgian and EU data protection frameworks impose a duty on the data controller to inform the data subject in two distinct cases: (a) when the data are collected directly from the data subject; and (b) when the data are collected from a third party, rather than directly from the data subject. Notably, Georgian legislation explicitly specifies the timing of such information disclosure in the case of direct collection—requiring that the information be provided either before or immediately after the commencement of data collection. A comparative legal analysis of Article 13(1) and (2) of the GDPR and Article 24(1) of the Law of Georgia "On Personal Data Protection" reveals that both instruments establish a comparable standard regarding the minimum scope of information that must be communicated to the data subject. Furthermore, Georgian legislation places particular emphasis on ensuring access to information for minor data subjects. Unlike the corresponding provisions of the GDPR, the national law explicitly requires that information be presented in a simple and understandable language suitable for minors. Georgian legislation also sets forth an exception to the obligation to provide information to the data subject, where special laws prescribe different procedures for notification, provided that such deviation does not result in a violation of the data subject's fundamental rights and freedoms. In such cases, upon a written request from the data subject, and where no legal basis exists to restrict the right in question, the controller is obliged to provide the requested information within 10 working days. In instances where data are not collected directly from the data subject, both Georgian and EU law require that the data subject be informed not only of the basic details of the processing, but also of the nature of the data being processed and the source of their collection, including whether the data originated from publicly available sources.

The issue of the period for informing the data subject is of particular relevance. According to Article 25 of the Law of Georgia "On Personal Data Protection", "the responsible person shall provide the data subject with information within a reasonable time or, if the data are used to contact the data subject, immediately after the first communication with him or her; and if the disclosure of the data is planned, prior to such disclosure, but no later than 10 working days from the date of obtaining the data," provided that no legal grounds exist to restrict the subject's right. By comparison, Article 14 of the GDPR establishes that the information must be provided to the data subject within a reasonable time after the data have been obtained, and

[65] **See Article 23, paragraph 1 of the Law.**

in any case no later than one month, taking into account the specific circumstances of the processing. If the data are used for communicating with the data subject, the information must be provided no later than at the time of the first communication; and if the data are intended to be disclosed to another recipient, the information must be provided no later than at the time of the first disclosure. Both instruments provide for similar exemptions from the obligation to inform the data subject, albeit with important distinctions. Under the GDPR, the controller is not required to provide the information if the collection or disclosure of data is laid down by Union or Member State law to which the controller is subject, and which contains appropriate measures to safeguard the data subject's legitimate interests; or where professional secrecy obligations apply under Union or Member State law, including statutory obligations of confidentiality. In all cases, the confidentiality of the data must be preserved.[66] According to Georgian law, the obligation to provide information to the data subject does not apply to controllers and/or processors if the collection or disclosure of such data is prescribed by law or is necessary for the fulfillment of a duty imposed by Georgian legislation[67]. Considering the purpose and specific nature of these situations, it may be concluded that the exceptions provided under Georgian law and those under the GDPR are functionally equivalent, though not identical in formulation.

With respect to the obligations imposed on data controllers and processors, Georgian law, in line with the General Data Protection Regulation and the LED, provides for the implementation of certain legal and organizational measures, including the following institutional standards:

- **Privacy by Design and by Default**

Privacy by Design and by Default functions as a preventive measure, which must be considered at the stage of determining the means of data processing. The purpose of this standard is to ensure that all stages of the processing cycle are conducted in full compliance with legal requirements and the fundamental principles of data protection. This is achieved by integrating the principles of confidentiality and data security both at the system design stage and throughout the processing lifecycle.[68] It is noteworthy that Georgian legislation fully reflects the regulatory approach of the General Data Protection Regulation and the LED regarding the obligation to incorporate data protection standards during the design and development of products and services ("Privacy by Design") and to ensure data protection by default settings ("Privacy by Default").[69] However, unlike the GDPR, which provides for the possibility of demonstrating compliance through data protection certification mechanisms[70], Georgian legislation does not recognize or provide for such an instrument.

---

[66] **Subparagraphs "c" and "d" of paragraph 5 of Article 14 of the Regulation.**

[67] **Article 25, paragraph 3 of the Law.**

[68] **Personal Data Protection Service of Georgia, Guideline on Privacy by design and by default, 2024.**

[69] **See Article 25 of the Regulation and Article 20 of the LED.**

[70] **See Article 42 of the Regulation.**

- **Data Security**

It is noteworthy that, under the Law of Georgia "On Personal Data Protection", which entered into force in March 2024, data security is recognized as one of the fundamental principles of data processing. This principle is further regulated by Article 27 of the Law, which imposes an obligation on controllers to implement appropriate technical and organizational measures to ensure that data processing is carried out in compliance with the law.

The General Data Protection Regulation (GDPR) and the LED similarly require the implementation of such measures. In line with national legislative requirements, both instruments call for the assessment of various contextual factors when determining appropriate safeguards. These include the nature and scope of data processing, the categories of personal data involved, the volume and purpose of processing, the means employed, the specific risks posed to data subjects, the evolving nature of technologies, and the cost of implementation.[71] The GDPR and the LED also set out various examples of technical and organizational measures, many of which are reflected in Georgian legislation. These include, but are not limited to, access control mechanisms, data storage security, and monitoring of data carriers. Importantly, the measures listed are not exhaustive.[72] Moreover, Georgian law imposes an explicit obligation on both controllers and processors to ensure the recording of all data operations in electronic form (commonly referred to as "logging").[73] In cases where data are processed in non-electronic form, all operations related to the disclosure and/or modification of data must also be recorded. This standard aligns with the LED's emphasis on risk assessment and the implementation of specific technical safeguards, including device-level access control, data carrier control, and storage monitoring.[74]

Additionally, Georgian legislation mandates that controllers and processors define the scope of employee access to personal data and undertake awareness-raising activities, including after the termination of employment or official authority, particularly with respect to the protection of confidentiality.

[71] **See Article 32(1) of the Regulation and Article 29(1) of the LED.**

[72] **See Article 27(2) of the Law.**

[73] **Article 27(4) of the Law.**

[74] **See Article 29(2) of the LED**

- **Recording of Information Related to Data Processing and Notification to the Personal Data Protection Authority**

A comparative analysis of Article 28 of the Law of Georgia "On Personal Data Protection", Article 30 of the GDPR, and Article 24 of the LED reveals that Georgian legislation establishes a comparatively high standard for the recording of data processing activities and the obligation to notify the supervisory authority. Specifically, in addition to the information required to be recorded under the GDPR and the LED, Georgian law obliges the controller, its designated representative (if any), and any involved processor to document incidents involving data security breaches.[75] Furthermore, upon request, the recorded information must be submitted to the Personal Data Protection Authority without delay and no later than three working days.[76] Notably, neither the GDPR nor the LED specifies a concrete timeframe for providing such information to the supervisory authority.[77] The national law also includes specific obligations applicable to law enforcement bodies, regulated under a dedicated provision.[78]

It is worth noting that the GDPR contains an exception to the obligation to maintain records of processing activities for enterprises employing fewer than 250 persons[79], provided certain conditions are met. Georgian law, by contrast, does not provide any such exemption, thereby applying the obligation uniformly across all controllers and processors, regardless of size.

- **Obligation to Notify the Data Protection Authority of a Data Breach**

Both Georgian and EU legislation impose an obligation on controllers to notify the data protection supervisory authority of a personal data breach. This obligation pertains to the management of such incidents and must be fulfilled within 72 hours of discovering the breach. In accordance with Article 33 of the GDPR and Article 30 of the LED, the notification must be made without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If the notification is not made within this timeframe, the controller must provide a justification for the delay. Georgian legislation, by contrast, does not incorporate the standard of "immediate" notification. The statutory maximum period for notifying the Personal Data Protection Service is strictly defined as 72 hours following the discovery of the incident. Notably, Georgian law does not include a provision allowing for an explanation in the event of delay beyond this timeframe.

---

[75] **The EU Regulation provides for the obligation to record any personal data breach, including the relevant facts, the consequences caused and the measures taken, pursuant to Article 33(5).**

[76] **See Article 30(4) of the Regulation.**

[77] **See Article 24, paragraph 3 of the LED.**

[78] **Law, Article 28, paragraphs 4-7. See also Special Report on the Activities of the Personal Data Protection Service "Implementation of the Law of Georgia "On Personal Data Protection", 2025, pp. 55-59.**

[79] **Regulation, Article 30, paragraph 5.**

Under all three instruments—the GDPR, the LED, and the Law of Georgia "On Personal Data Protection"—the obligation to notify the supervisory authority does not apply where the breach is unlikely to result in a risk to the rights and freedoms of natural persons. However, Article 29 of the Law of Georgia goes further by requiring the controller to provide additional information to the supervisory authority, including the nature, scope, and timing of the incident, as well as whether the controller intends to notify the data subject(s) and within what time frame, in accordance with the procedure set out in Article 30 of the Law. A significant departure from the GDPR and the LED is found in the Georgian law's provision empowering the Personal Data Protection Service to disclose information about the breach to the public. Specifically, where, in light of the nature of the breach, the potential harm, and/or the number of data subjects affected, the controller fails to inform or is unable to inform the data subjects, the supervisory authority may itself disclose the relevant information. This competence is grounded in Article 29(6) and Article 30(3) of the Law, which also enumerate exceptions to the obligation to notify data subjects. In contrast, under the GDPR, if the data subject has not been informed, the supervisory authority may require the controller to notify the data subject or may assess whether an exception to such notification applies.

Finally, it is important to note that the criteria for determining whether an incident constitutes a significant threat to fundamental human rights and freedoms, along with the procedure for notifying the Personal Data Protection Service of such incidents, are defined by Order No. 19 of the President of the Personal Data Protection Service, dated 28 February 2024, "On Approval of the Criteria for Determining an Incident Posing a Significant Threat to Fundamental Human Rights and Freedoms and the Procedure for Notifying the Personal Data Protection Service of an Incident."

- **Obligation to Inform the Data Subject About the Data Breach (Incident)**

Pursuant to Article 34 of the General Data Protection Regulation (GDPR), "where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, without undue delay, communicate the personal data breach to the data subject." It is noteworthy that, in contrast to the GDPR, both the LED and the Law of Georgia "On Personal Data Protection" condition this obligation on the high likelihood of a high risk to the rights and freedoms of natural persons. This indicates that Georgian legislation sets a more stringent threshold for determining when notification must occur, as it requires a predictive assessment of likelihood in addition to the presence of risk, thereby establishing a stricter informational standard in favor of the data subject.

In addition, the Georgian law expressly requires that any notification to the data subject be provided in plain and understandable language,[80] thereby reinforcing accessibility and clarity as key components of effective communication. The law provides for only two narrowly defined exceptions to this obligation: (1) when notification would endanger the protection of the public interest, and (2) where the controller has implemented appropriate security measures that

[80] **See Article 30, Paragraph 1 of the Georgian Law.**

have mitigated the significant risk of harm to the data subject's fundamental rights and freedoms. The LED similarly allows for the delay, restriction, or omission of notification to the data subject based on the grounds set out in Article 13(3). However, such measures are permissible only where they are necessary and proportionate in a democratic society and where the fundamental rights and legitimate interests of the data subject are duly taken into account, in light of the purposes specified in that provision.

- **Data Protection Impact Assessment**

A data protection impact assessment (DPIA) is a process intended to mitigate elevated risks of violations of fundamental rights and freedoms, particularly those arising from complex or high-risk data processing operations. It involves a systematic description and evaluation of the processing in terms of its necessity and proportionality, as well as the potential consequences for individuals. According to Article 31(1) of the Law of Georgia "On Personal Data Protection", "If, taking into account the new technologies, the categories of data, the volume, the purposes and means of data processing, the risk of a violation of fundamental rights and freedoms of individuals is likely to be high, the controller shall be obliged to carry out a data protection impact assessment in advance." Similarly, Article 35 of the GDPR provides that where a particular type of data processing—especially when involving the use of new technologies and considering its nature, scope, context, and purposes—is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to conduct a DPIA prior to initiating the processing. The GDPR also permits the use of a single DPIA for a set of similar processing operations that present comparable high risks. The GDPR standard is based on a presumption of high risk, triggered by specific contextual factors such as innovative technologies or large-scale processing. Georgian law, on the other hand, is based on the high probability of risk—i.e., a more explicit predictive threshold—requiring a DPIA when there is a high probability of the infringement of rights due to the nature of the processing, particularly in light of the technologies involved and the categories and volume of data. This threshold is comparable to that found in the LED, which also refers to a "high probability" of risk as a determining factor.[81]

According to EU law, a single data protection impact assessment may be used to evaluate similar processing operations that are likely to result in comparable high risks. Georgian legislation, however, does not contain an explicit provision permitting such a consolidated assessment. Nonetheless, the national regulation reflects the criteria set out in Article 35(3) of the GDPR, identifying circumstances under which the conduct of an impact assessment is particularly necessary. These include, for example, the large-scale processing of special categories of personal data, the systematic and large-scale monitoring of data subjects' behavior in public spaces, or the adoption of fully automated decisions that produce legal, financial, or other significant effects on the data subject.[82]

Both Georgian and EU legislation specify the essential content of a data protection impact assessment document. A comparison of the respective standards indicates that the Georgian

[81] **For further information, see Data Protection Authority, Recommendations on Data Protection Impact Assessments (DPIA), 2024.**

[82] **See Article 31, Paragraph 2 of the Law.**

framework aligns with the GDPR and the LED, albeit with some distinctions. While EU law sets out a minimum list of required elements, it also imposes a broader obligation on the controller to include, within the assessment document, measures designed to address identified risks. These measures must encompass appropriate safeguards and mechanisms for ensuring the protection of personal data and demonstrate compliance with the Regulation, taking into account the legitimate interests and rights of data subjects and other affected individuals.[83] In contrast, Georgian law requires the DPIA document to include a description of the data categories, the purposes and legal grounds of the processing, its proportionality and operational aspects, an assessment of potential threats to fundamental rights and freedoms, and a description of the technical and organizational measures implemented to ensure data security.[84]

Importantly, where a high risk is identified through the impact assessment, Georgian law obliges the controller to adopt all necessary measures to significantly reduce the risk and, if needed, to consult the Personal Data Protection Authority. Should the identified risk remain substantial despite the implementation of additional technical and organizational measures, the processing activity may not be carried out. Unlike EU law, Georgian legislation also establishes specific rules regarding the duration of retention of the DPIA, the relevance of a high number of data subjects as a risk factor, and the conditions under which the controller may be exempt from the obligation to make the assessment document publicly available.[85]

It is noteworthy that the General Data Protection Regulation (GDPR) allows the supervisory authority to establish a list of processing operations that are subject to the requirement of conducting a data protection impact assessment (DPIA), as provided for under Article 35(1) of the Regulation. In this context, the criteria for determining the circumstances that trigger the obligation to carry out a DPIA, as well as the procedure for such assessment, are set forth in Order No. 21 of the President of the Personal Data Protection Service of Georgia, dated 28 February 2024.[86]

In alignment with the GDPR and the LED, Georgian legislation also provides for the possibility of consulting the supervisory authority for personal data protection. However, it is important to highlight that EU law governs this matter more comprehensively. Under the GDPR, the controller is required to consult the supervisory authority prior to commencing processing activities if the intended processing is likely to result in a high risk to the rights and freedoms of natural persons, unless the controller has taken sufficient measures to mitigate such risks. In this regard, consultation is mandatory before processing begins.[87] By contrast, Georgian law provides for consultation only "where necessary," without imposing a mandatory requirement based on a specific risk threshold.[88] Both Georgian and EU law prescribe a minimum set of information to be provided to the supervisory authority in the context of such consultation, and these requirements are substantially consistent in content.

---

[83] **See Article 35, paragraph 7 of the Regulation.**

[84] **Law, Article 31, Paragraph 2.**

[85] **See Article 31, paragraphs 4, 7 and 8 of the Law.**

[86] **Order No 21 of 28 February 2024 of the President of the Personal Data Protection Service "On the Approval of the Criteria for Determining the Circumstances Giving Rise to the Obligation for a Data Protection Impact Assessment, and the Assessment Procedure".**

[87] **See Article 36, paragraph 1, of the Regulation.**

[88] **Law, Article 31, Paragraph 5.**

- **Personal Data Protection Officer**

One of the legislative novelties introduced by the Law of Georgia "On Personal Data Protection" is the institution of the Personal Data Protection Officer. It is noteworthy that the national legislation fully incorporates the standard established by European Union law regarding Personal Data Protection Officers. This includes the circumstances that give rise to the obligation of appointment or designation, which are further regulated by a normative act[89] of the Personal Data Protection Service, the possibility of establishing a joint officer, and the appointment/designation of an officer who is an employee of the data controller, provided that such appointment does not create a conflict of interest. It is important to note that under EU law, the data controller is obliged to publicly disclose the contact information of the Personal Data Protection Officer and also notify the supervisory authority for personal data protection. The same obligation is also provided by the national legislation, with the distinction that the notification period to the Personal Data Protection Service is set at 10 working days from the appointment or designation of the officer, as well as from their replacement.[90]

The Law of Georgia "On Personal Data Protection", similar to European Union law, defines the functions and duties of the Personal Data Protection Officer, as well as the standard[91] for fulfilling the obligations imposed on them. The GDPR does not establish explicit qualification requirements for the Personal Data Protection Officer, including licensing; however, it is mandatory that the officer possesses appropriate competence, which may be demonstrated through a relevant professional certification program[92]. It is important to note that neither the national legislation nor European law prescribes specific legal grounds for the dismissal of a Personal Data Protection Officer or the termination of their contract.

[89] Order No 22 of 28 February 2024 of the President of the Personal Data Protection Service "On Determining the Category of Controllers and Processors Who Are Not Obliged to Appoint or Designate a Personal Data Protection Officer".

[90] See Article 37, paragraph 7 of the Regulation, Article 32(4) of the LED and Article 33, paragraph 8 of the Georgian Law.

[91] See Articles 38 and 29 of the Regulation, Articles 33 and 34 of the LED, and Article 33, paragraphs 1, 3, 4 - 7 of the Georgian Law.

[92] See also: Personal Data Protection Service, Recommendation on the Personal Data Protection Officer, 2024.

- **Special Representative**

This institution is provided for both by the Law of Georgia "On Personal Data Protection" and by the General Data Protection Regulation.[93] It is noteworthy that the Law Enforcement Directive does not contain provisions regarding the appointment of a special representative.

According to the Regulation, the territorial scope determining the obligation to appoint a special representative applies to controllers and/or processors registered outside the territory of the European Union. In contrast, the Law of Georgia "On Personal Data Protection" imposes an obligation to appoint or designate a special representative on controllers and/or processors registered outside the territory of Georgia. Due to the specific nature of regulating this obligation, the exceptions established by national and European legislation also differ. In particular, under the Georgian law, the obligation to appoint or designate a special representative does not arise if the controller and/or processor is established in an EU Member State and is subject to the personal data protection rules applicable within the EU, or if it is established in a state recognized by the European Union as ensuring an adequate level of data protection;[94] The GDPR provides exceptions in cases where: the data controller is a public authority; the data processing is carried out periodically, is not large-scale; does not involve the large-scale processing of special categories of data as specified in paragraph 1 of Article 9 of the Regulation, or the processing of data relating to convictions and criminal offenses in accordance with Article 10 of the Regulation; and, considering the nature, context, scope, and purposes of the processing, it is less likely to pose a risk to the rights and freedoms of natural persons. It should be noted that, under the Law of Georgia "On Personal Data Protection", the procedure for the registration of a special representative is established by a normative act of the President of the Personal Data Protection Service.[95]

- **Other Obligations of the Data Controller and the Data Processor**

The Law of Georgia "On Personal Data Protection" also defines the obligations of the data controller in cases of obtaining consent from the data subject and withdrawal of such consent, as well as the roles of joint controllers and data processors. National legislation establishes a standard similar to that of the European Union Regulation regarding the obligations of the data controller in relation to obtaining and withdrawing consent. Specifically, Article 32 of the Law, similar to Article 7 of the GDPR, requires that if consent is obtained in writing, the text must be drafted in clear, simple, and understandable language. Under both Georgian and EU law, when assessing the voluntariness of consent, it must be considered, among other circumstances,

---

[93] See Article 34 of the Georgian Law and Article 27 of the Regulation.

[94] See Article 34, paragraphs 6 and 7 of the Georgian Law.

[95] Order №20 of 28 February 2024 of the President of the Personal Data Protection Service Tbilisi "On the Approval of the Procedure for Registering a Special Representative by the Personal Data Protection Service".

whether consent is a necessary condition for concluding a contract or receiving a service and whether the service can be provided or the contract concluded without such consent. The Law also establishes the obligation to inform the data subject, prior to obtaining consent, about their right to withdraw consent and the consequences of such withdrawal.[96] Similarly to the EU Regulation, the Law establishes the obligation to implement a free, simple, and accessible mechanism for the withdrawal of consent, including the possibility of using the same form for withdrawal as was used by the data subject when giving consent.[97]

The requirements of Georgian law regarding joint controllers, including the obligation to define, by a written agreement, each party's duties and responsibilities for ensuring compliance with the law, fully correspond to the standards established by the EU Regulation and the LED.[98] Similarly, to the European Union legislation, the Georgian Law regulates various aspects of the legal relationship between the data controller and the data processor, as well as the essential terms of the written agreement concluded between them, including issues related to obligations and responsibilities.[99] The difference lies in the fact that, under the GDPR, adherence to an approved code of conduct by the processor, as provided for in Article 40 of the Regulation, or the use of approved certification mechanisms in accordance with Article 42, may serve as a demonstrative element of the processor's compliance with obligations, whereas this aspect is not regulated by the national legislation.[100] It is noteworthy that, under the LED, the contract or other legal act concluded between the controller and the processor must be executed in writing, including in electronic form.[101]

[96] See Article 32, paragraphs 3 and 7 of the , as well as Article 7, paragraphs 3 and 4 of the Regulation.

[97] See Article 32, Paragraph 8 of the Georgian Law and Article 7, Paragraph 3 of the Regulation.

[98] See Article 35 of the Georgian Law, Article 26 of the EU Regulation and Article 21 of the LED.

[99] See: Personal Data Protection Service, Recommendations on the essential and standard terms of the contract concluded between the person responsible for processing and the person authorized to process, 2024.

[100] See Article 28, paragraph 5, of the Regulation.

[101] See Article 22, paragraph 4, of the LED.

5. TRANSFER OF DATA TO ANOTHER STATE AND INTERNATIONAL ORGANISATION

The international transfer of data is regulated by Articles 37–38 of the Law of Georgia "On Personal Data Protection", Articles 44–50 of the EU Regulation, and Articles 35–40 of the LED. According to Article 44 of the Regulation, the transfer of personal data from a third country or an international organization to another third country or international organization is permissible only if the parties involved in the data processing comply with the requirements of the GDPR to ensure that the guarantees for the protection of natural persons established by the Regulation are fully upheld. The LED takes an identical approach: the relevant provisions consider, as prerequisites for the admissibility of international data transfers, on the one hand, compliance with data protection legislation requirements, and on the other hand, confirmation of the existence of appropriate safeguards for the protection of data subjects' rights.

It is noteworthy that the Georgian Law fully aligns with the approach of the above-mentioned international instruments in regulating the transfer of data to another state or an international organization. Specifically, according to Article 37 of the Law, the transfer of data to another state or an international organization is permissible if the requirements for data processing established by this Law are met and if appropriate safeguards for data protection and the protection of data subjects' rights are ensured in the respective state or international organization.

In terms of additional authorization for the transfer of data to countries and international organizations that provide adequate safeguards for data protection, the regulation is identical under all three instruments. No separate authorization is required, and the list of such countries and organizations is approved by the relevant legal act. In the case of Georgia, this list is approved by the President of the Personal Data Protection Service, while under the EU Regulation and the LED, it is approved by the European Commission.

As for the criteria necessary to determine the existence of adequate safeguards for data protection, these are defined in an almost identical manner. Similar to international instruments, the Georgian law also focuses on compliance with data protection legislation and international obligations, as well as on the guarantees for the protection of the rights and freedoms of data subjects, including the availability of effective legal remedies. In this regard, the interpretation provided by national legislation is much broader. While the EU Regulation and the LED use the term "case law" to refer to legal protection mechanisms, the Georgian law generalizes this concept and includes not only the practice established through judicial proceedings but also, among others, the role of the supervisory authority, which is also explicitly emphasized in the text of the norm.

In the national legislation, the periodic review of the list of countries and/or international organizations providing adequate data protection safeguards, as well as the procedure for making amendments following such reviews, is regulated identically to the European framework. All three instruments stipulate that decisions to amend or revise this list do not have retroactive effect. At the same time, the Georgian law specifies the periodicity for reviewing the list and sets a defined timeframe—"at least once every three year."

Similar to the Regulation and the Directive, the provisions governing data transfers based on an adequacy decision establish the obligation of the European Commission[102], the European Commission is required to publish in the official journal of the European Union and on its website the list of third countries, parts thereof, specific sectors, and international organizations that ensure adequate safeguards for the protection of personal data. In terms of publicly publishing the list, Georgian law is fully aligned with the requirements of the GDPR, as the normative act issued by the President of the Personal Data Protection Service is publicly published both in the official printed journal and on the Service's official website.[103]

It is noteworthy that all three legal acts establish the existence of adequate safeguards for data protection and legal remedies for the protection of data subjects' rights as a criterion for the admissibility of international data transfers. However, the Georgian law contains a different wording in this part. While all three acts list the cases in which there is a legal basis for international data transfers, differences can be found both in the scope of the listed cases and in the applicable procedures. According to the relevant provision of the national law, among other mechanisms, the data controller may ensure adequate safeguards for data protection by entering into a contract with the data recipient, in which case it is necessary to undergo the permit issuance procedure. Under EU law, the transfer of personal data to third countries or international organizations is permitted in two ways: (1) on the basis of an adequacy decision adopted by the European Commission, or (2) if the controller or processor provides appropriate safeguards for the data subject, including enforceable rights and effective legal remedies. Article 37, paragraph 2 of the Law encompasses a wide range of legal grounds under which the international transfer of data is permissible. These include, inter alia, the transfer of data as provided for by Georgia's international treaties and agreements; as well as cases where data transfer is stipulated by the "Criminal Procedure Code of Georgia" (for the purpose of conducting investigative actions), the Law of Georgia "On the Legal Status of Aliens and Stateless Persons", the Law of Georgia "On International Cooperation in Criminal Matters", the Law of Georgia "On International Cooperation in the Law Enforcement Field", the Organic Law of Georgia "On the National Bank of Georgia", or a normative act adopted on the basis of the Law of Georgia "On Facilitating the Prevention of Money Laundering and Terrorism Financing". As for the transfer of data based on the data subject's consent, for reasons of significant public interest, or for the vital interest of the data subject, all three instruments under consideration recognize and share these grounds.

It is noteworthy that neither the General Regulation nor the LED provides a legal definition of "international transfer of personal data to a third country or an international organization." According to Article 4(23) of the GDPR, a data controller or processor has representation in more than one Member State, or when the data processing has, or is likely to have, a substantial impact on data subjects in more than one Member State.[104] Georgian law also does not define this concept.

---

[102] See Article 45(8) of the Regulation and Article 36(8) of the LED.

[103] Article 38, paragraph 2 of the Law stipulates that the President of the Service shall issue a normative act approving the list of countries that provide adequate guarantees for data protection. Consequently, this normative act must be published in the official printed media and on the website of the Legislative Herald of Georgia<https://matsne.gov.ge/ka/document/view/6119485>.

[104] The General Data Protection Regulation (GDPR), A Commentary, Christopher Kuner, Lee A. ByGrave, Christopher Docksey, Oxford University Press, 2020, 762.

Since the GDPR does not provide an exact definition of international data transfer, the "European Data Protection Board" (EDPB) developed guidelines on international data transfers and established three cumulative criteria under which a processing operation is considered a "data transfer":[105]

- **The data controller or processor ("exporter") is subject to the EU General Regulation for a specific data processing activity.**

The requirements of Article 3 of the Regulation must be met, meaning that the data controller or processor must be subject to the GDPR for the specific purposes of the data processing activity.

- **The data "exporter" discloses, transfers, or otherwise makes personal data available to another data controller, joint controller, or processor ("importer")**

The data "exporter" discloses or otherwise makes the data available to another data controller or processor through the transfer of data.

- **The data "importer" is either an international organization or located in a third country, regardless of whether this "importer" is subject to Article 3 of the EU General Regulation for the specific purposes of data processing .**

According to this criterion, the data "importer" is geographically located in a third country, regardless of whether the rules established by the GDPR apply to them. As clarified by the "European Data Protection Board" (EDPB), the purpose of this criterion is to ensure adequate protection of individuals, which is guaranteed by the Regulation.

When all three criteria are met, it constitutes a data transfer and, accordingly, Chapter V of the General Regulation applies. Similarly, the international transfer rules and established practices in force in Georgia allow us to conclude that all three criteria are recognized, and the norms defined by the respective chapter of the Law apply to processing activities within the scope of the Law when one of the parties involved in the processing, namely the data recipient, is another state or an international organization.

---

[105] **Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 7-12 https://shorturl.at/kY7Ea.**

6. MANDATE AND SCOPE OF EXERCISE OF POWERS OF THE SUPERVISORY AUTHORITY

The General Data Protection Regulation (GDPR) provides that each Member State shall designate one or more independent public authorities responsible for overseeing the implementation of the Regulation. The aim is to protect the fundamental rights and freedoms of natural persons in relation to personal data processing and to facilitate the free movement of personal data across the European Union (referred to as the "supervisory authority").

Georgian legislation, in line with EU law, recognizes the importance of establishing a supervisory authority—the Personal Data Protection Service—and reflects the GDPR's general approach regarding its core areas of activity. These include consultation, oversight and monitoring in the field of data protection, verification of the lawfulness of data processing, examination of complaints, public awareness-raising, and more.

However, unlike EU legislation, Georgian law does not regulate certification, accreditation, or authorisation mechanisms. It also does not confer any mandate related to the support of the European Data Protection Board (EDPB).

It is noteworthy that the GDPR provides, within the article regulating the functions of the supervisory authority, that the exercise of such functions shall be free of charge for the data subject, and, where applicable, for the data protection officer. At the same time, it allows supervisory authorities to charge a fee or refuse to act on requests that are manifestly unfounded or excessive, particularly due to their repetitive nature, provided that such refusal is duly justified. In this regard, Georgian law is partially aligned with EU legislation. Specifically, the activities of the Personal Data Protection Service and the mechanisms for the exercise of data subject rights, as well as institutional support provided to data protection officers (e.g., through consultations and educational measures), are free of charge. However, Georgian legislation does not provide for the possibility of the supervisory authority to impose a fee or refuse to perform its functions on the grounds of a request being unfounded or excessive.

6.1. Principles of the Supervisory Authority's Activities

The General Data Protection Regulation (GDPR), the LED, and Georgian law all unequivocally establish the principles of independence of the supervisory authority and the prohibition of subordination to any external body or official in the course of fulfilling its functions and exercising its powers.

Notably, Georgian law goes further by explicitly criminalizing any form of undue influence on the supervisory authority or its employees, as well as unlawful interference in the performance of their official duties. This serves as a legal safeguard to strengthen and ensure the effective implementation of the principle of institutional independence. Notably, Georgian law goes further by explicitly criminalizing any form of undue influence on the supervisory authority or its employees, as well as unlawful interference in the performance of their official duties. This serves as a legal safeguard to strengthen and ensure the effective implementation of the principle of institutional independence.

The GDPR, in its provisions on the establishment of supervisory authorities, affirms that members of the authority must refrain from any actions incompatible with their duties, a principle also reflected in the LED. Georgian law mirrors this principle through specific norms concerning the incompatibility of the position of the President of the Personal Data Protection Service. Issues related to conflict of interest and incompatibility for other employees of the authority are regulated under a separate legislative act, ensuring compliance with this standard.

The GDPR further reinforces the principle of independence by requiring Member States to ensure that the composition and internal accountability of the supervisory authority are determined by the authority itself. Georgian legislation reflects this by granting the President of the Personal Data Protection Service the authority to approve the structure, rules of operation, and internal distribution of powers within the Service, as established under the Regulation of the Personal Data Protection Service.

This principle is also reflected in the financing mechanisms of the supervisory authority. All three legal frameworks—the GDPR, the LED, and Georgian law—emphasize the need for an independent budget. While EU legislation requires that financial oversight be conducted in a manner that does not compromise the authority's independence, Georgian law introduces a specific safeguard: any reduction in the Service's budget may occur only with the prior consent of the President of the Service, thereby shielding the authority's independence from indirect financial influence.

6.2. Rules for the Establishment of a Supervisory Authority

According to the General Data Protection Regulation (GDPR), "Member States shall ensure that each member of the supervisory authority is appointed in a transparent manner and is elected by the parliament, the government, the head of state, or an independent body empowered to do so by the law of the Member State."[106]

From the available alternatives set out in the GDPR, Georgian legislation has adopted the parliamentary model. It is important to note that both the GDPR and the LED regulate the procedure for appointing the head of the supervisory authority. In contrast, Georgian law provides that only the President of the Personal Data Protection Service be elected by the Parliament, while personnel decisions concerning other staff members of the Service are made by the President of the Service.

[106] **See Article 53, paragraph 1, of the Regulation.**

Georgian law also outlines specific eligibility requirements for the President of the supervisory authority, going beyond the general requirement under the GDPR and the LED that members possess subject-matter knowledge and experience. According to Article 41(1) of the Law of Georgia "On Personal Data Protection", a candidate for the position must be a citizen of Georgia, without a criminal conviction, with a higher legal education, and at least five years of professional experience in the justice or law enforcement system or in the field of human rights protection. The candidate must also possess a high professional and moral reputation. The law also defines the grounds for termination of employment of supervisory authority staff, including the expiration of the term of office, voluntary resignation, or reaching the mandatory retirement age. In addition, it sets out distinct grounds for the early termination of the President's mandate—such as loss of Georgian citizenship, deteriorating health, a final court conviction, or appointment to an incompatible position. As in international instruments[107], failure to perform official duties or the entry into force of a court judgment may also result in dismissal.

The Georgian legal framework mirrors the GDPR's provisions on the establishment and functioning of the supervisory authority, including rules on appointment and qualifications, prohibitions on conflicting activities and benefits, and rules governing conduct during and after the term of office. Notably, Georgian law establishes a fixed term of office for the President of the Service and restricts consecutive re-election—a person may not be elected to the position twice in a row. The GDPR and the LED leave the decision on re-election to national legislatures.

EU legislation also requires members of the supervisory authority to uphold the principle of confidentiality both during their term of office and after it ends. Similarly, Georgian law obliges employees of the Personal Data Protection Service to maintain the confidentiality and security of all information obtained during the performance of their official duties. This confidentiality obligation continues to apply after the termination of employment, in alignment with international standards.

6.3. Powers of the Supervisory Authority to Examine the Lawfulness of Data Processing

The powers of supervisory authorities to examine or inspect data processing practices are similarly regulated under the General Data Protection Regulation (GDPR), the LED, and Georgian law. These frameworks authorize supervisory bodies to take direct measures in response to violations of data protection rules. However, there are notable differences in scope. Specifically, Georgian legislation does not provide for certain powers established under the GDPR, such as accreditation and authorization, certification, and the approval of binding corporate rules. Conversely, Georgian law grants certain unique powers to the supervisory authority. These include the authority to conduct covert investigative actions and to exercise oversight over the activities involving the Central Bank of Electronic Communications Identification Data, which are not addressed in the GDPR or the LED.

[107] **See Article 53, paragraph 4 of the Regulation; Article 43, paragraph 4 of the LED.**

Under Article 83 of the GDPR, supervisory authorities have the power to impose both corrective measures[108] and administrative fines.[109] It is important to note that some EU Member States have supplemented the GDPR with national legislation, further regulating the imposition of fines. According to Article 83(1), administrative fines must be "effective, proportionate, and dissuasive," and must be set at a level that discourages further non-compliant data processing activities.[110] At the same time, Article 83(7) allows Member States discretion to decide whether and to what extent public authorities may be subject to administrative fines. As a result, legal approaches differ across the EU—while some Member States exempt public bodies from fines, others impose sanctions comparable to those applied to private entities Under Georgian law, the Personal Data Protection Service is authorized to apply the relevant measures established by national legislation to both public and private sector entities in the event of violations. This ensures that data protection obligations are universally enforced, regardless of the entity's legal status.[111]

It is also worth noting that transparency of the supervisory authority's activities is emphasized across both EU and Georgian frameworks. The requirement to publish an annual report is set forth in the GDPR and the LED. Georgian law mirrors this obligation and goes further by providing for the publication of special reports. Specifically, the Personal Data Protection Service of Georgia is authorized to publish such reports at any time on its own initiative on matters it deems significant, thereby strengthening public awareness and institutional accountability.

6.4. Procedure for Lodging a Complaint with a Supervisory Authority

The right of an individual to lodge a complaint with a supervisory authority in order to protect their rights, to challenge a decision in court, and to bring a dispute against the data controller or processor is provided under Articles 77, 78, and 79 of the GDPR, as well as Article 52 of the LED. In this context, the supervisory authority has discretionary power to assess complaints concerning potential violations of data protection rights. Additionally, Article 57(1) (f) of the GDPR outlines the functions of the supervisory authority in relation to complaints: complaints must be examined with due diligence and in full compliance with legal requirements. Moreover, any decision taken by the supervisory authority—whether it grants or rejects the complaint—must be legally reasoned and substantiated.[112]

---

[108] See Article 58 of the Regulation.

[109] Bovens M., Analysing and Assessing Accountability: A Conceptual Framework, in: European Law Journal, 13(4), 2007, 447-468.

[110] Ayres I., Braithwaite J., Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press, 1992.

[111] See Article 52 of the Law.

[112] Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements, version 1.0, adopted on 2 feb., 2021.

A similar regulatory framework exists under Georgian law. Specifically, Article 22(1) and Article 50(2) and (7) of the Law of Georgia "On Personal Data Protection" establish the procedure for submitting and reviewing complaints. It is important to note that, in the process of examining applications, complaints, or notifications, the Personal Data Protection Service of Georgia is guided not only by the law but also by the "Rules for Examining the Lawfulness of Personal Data Processing", approved by Order No. 34 of the President of the Service, dated March 1, 2024.

7. RIGHT TO APPEAL TO A COURT

Article 78(1) of the General Data Protection Regulation (GDPR) sets out the general principle that individuals have the right to appeal to a court against a decision taken by a public authority. In line with this provision, the data subject has the right to seek judicial protection in order to safeguard their interests and to challenge a decision made by a supervisory authority. This right is similarly recognized in Article 53 of the LED. Correspondingly, Article 22(1) and Article 63(1) of the Law of Georgia "On Personal Data Protection" establish the general rule that an individual has the right to appeal a decision issued by the President of the Service in court, within the time limits prescribed by law.

Additionally, Article 78(2) of the GDPR sets a specific timeframe, stating that if the data subject's complaint is not examined within three months or if they are not informed of the outcome as required under Article 77, they are entitled to bring the matter before the court for the protection of their rights.

Furthermore, Article 79(1) of the GDPR grants the data subject the right to effective judicial protection if they believe their data have been processed in violation of the Regulation. Article 79(2) addresses the rules concerning jurisdiction in such cases. As noted, Article 22(1) of the Law of Georgia reinforces an individual's ability to appeal to the Service, a court, or a higher administrative body in the event of a violation of the rights and rules established by law. This approach mirrors the guarantees provided in Article 53 of the LED, ensuring access to effective legal remedies in both legal frameworks.

8. COMPENSATION FOR PERSONAL DATA PROCESSING INFRINGEMENTS

It is noteworthy that, in cases of certain personal data processing infringements, Article 82 of the General Data Protection Regulation (GDPR) and Article 56 of the LED establish the right of the data subject to receive compensation. These provisions aim to restore the legal status of an individual who has suffered material or non-material (moral) damage as a result of unlawful data processing. Although this matter is specifically regulated by dedicated norms in European

legislation, Georgian law does not contain a parallel provision explicitly addressing the right to compensation in the context of personal data protection. However, the right to claim compensation for damages—including those arising from unlawful data processing—is governed more generally by the Civil Code of Georgia.

9. GENERAL RULES AND CONDITIONS FOR IMPOSING ADMINISTRATIVE FINES

Regarding the prerequisites and procedures for imposing administrative fines, Georgian law reflects the spirit of Article 83 of the General Data Protection Regulation (GDPR), although it does not fully align with it. In particular, a different approach is applied in the calculation of fines: under the GDPR, the amount of the fine is linked to the annual turnover of a legal entity, with fines reaching up to €10,000,000 or, in the case of an enterprise, up to 2% of the total worldwide annual turnover of the preceding financial year—whichever is higher.

Notably, unlike the GDPR and the LED, Georgian law establishes fixed amounts for fines. However, compared to the sanctions that were in force until March 1, 2024, the amounts have been significantly increased. Specifically, the legislator linked the fine to the offender's organizational form and annual turnover. The amount is not calculated as a percentage of turnover but is instead set as a fixed amount: 10,000 GEL if the annual turnover does not exceed 500,000 GEL, and 20,000 GEL if the turnover exceeds that threshold. For instance, a violation of any of the legal principles of data processing may result in a warning or a fine of 1,000 GEL for individuals, public institutions, non-entrepreneurial (non-commercial) legal entities, as well as legal entities, branches of foreign enterprises, and individual entrepreneurs with an annual turnover not exceeding 500,000 GEL. The same violation committed by a legal entity (except a non-entrepreneurial/non-commercial one), a branch of a foreign enterprise, or an individual entrepreneur with an annual turnover exceeding 500,000 GEL will result in a warning or a fine of 2,000 GEL. Accordingly, Georgian law provides for an increased threshold of sanctions based on the offender's legal status and income level.

It is also notable that Georgian legislation distinguishes between aggravating and mitigating circumstances, whereas Article 83(2) of the GDPR only provides a general indication of factors that must be considered when imposing or calculating a fine. Moreover, the aggravating and mitigating factors listed in Georgian law do not entirely coincide with those under the GDPR. For example, Georgian law explicitly states that if a violation is committed by a minor, this is a mitigating circumstance—something not specified in the GDPR, according to which the recurrence of similar violations by a data controller or processor must be taken into account when determining fines. Georgian law takes a more specific approach by defining repetition: a violation is considered repeated—and therefore an aggravating circumstance—if the same administrative offense is committed again within one year. Georgian law also allows for a percentage reduction in the fine in the presence of mitigating circumstances, a flexibility not expressly provided in Article 83 of the GDPR.

In calculating the final amount of the fine, all circumstances relevant to the case must be assessed before a final decision is made.[113] Articles 61–64 of the Law of Georgia, which govern the assessment and reconciliation of mitigating and aggravating circumstances during fine calculation, are fully consistent with this approach.

In terms of determining sanctions, Article 84 of the General Data Protection Regulation (GDPR) emphasizes the role of Member States and provides that they must adopt national legislation establishing sanctions for violations of the Regulation not already covered by Article 83. While the provision is addressed specifically to EU Member States, Article 52 of the Law of Georgia "On Personal Data Protection" similarly defines the authority of the Personal Data Protection Service in cases of violations of data protection laws or other normative acts regulating data processing. In particular, under Article 52, the Service is authorized to require a person to take one or more of the following measures: a) Require the rectification of the violation and correction of deficiencies related to data processing, in the manner and within the timeframe specified by the Service; b) Require the temporary or permanent cessation of data processing if the measures and procedures implemented by the data controller or data processor do not comply with the data security requirements established by Georgian legislation; c) Request the termination of data processing, or the blocking, deletion, destruction, or depersonalization of data, if the data processing is considered to be in violation of Georgian law; d) Request the termination of data transfers to another state or international organization if such transfers are conducted in violation of Georgian legislation; e) Provide written advice and recommendations to the data controller and/or data processor in cases involving minor violations of data processing rules; f) Impose administrative liability on the violator.

[113] **EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 2.1, Adopted on 24 May 2023**

10. EXCEPTIONAL CASES

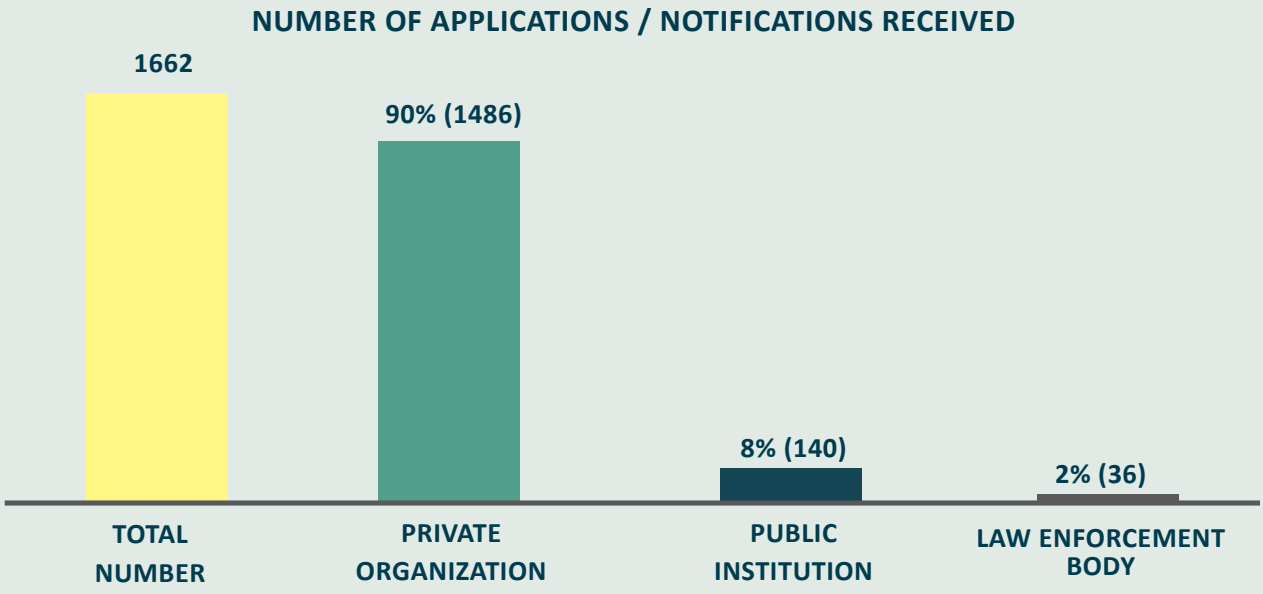
Article 85 of the General Data Protection Regulation (GDPR) seeks to strike a balance between the protection of personal data and freedom of expression. It recognizes that, in certain circumstances, processing personal data is essential for exercising freedom of expression and information—covering journalistic activity and access to information—and it expressly permits exemptions for academic, artistic, and literary purposes. These principles are fully mirrored in Georgian law, specifically in Article 2(2)(e)–(f).

Article 89 of the GDPR further stipulates that personal-data processing undertaken in the public interest—such as for scientific or historical research or statistical purposes—must be subject to safeguards that protect data subjects' rights and freedoms. To uphold the principle of data-minimization, the provision highlights technical and organizational measures like anonymization and pseudonymization, and underscores the importance of confidentiality.[114] Similar measures appear in Articles 4 and 9 of the LED. Correspondingly, Georgian law incorporates analogous safeguards—for example, Article 4(6), Article 6(m), and Article 16(3)(d)—to regulate data processing for archiving in the public interest, scientific or historical research, and statistical purposes.

[114] **EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 Apr. 2020, 11**

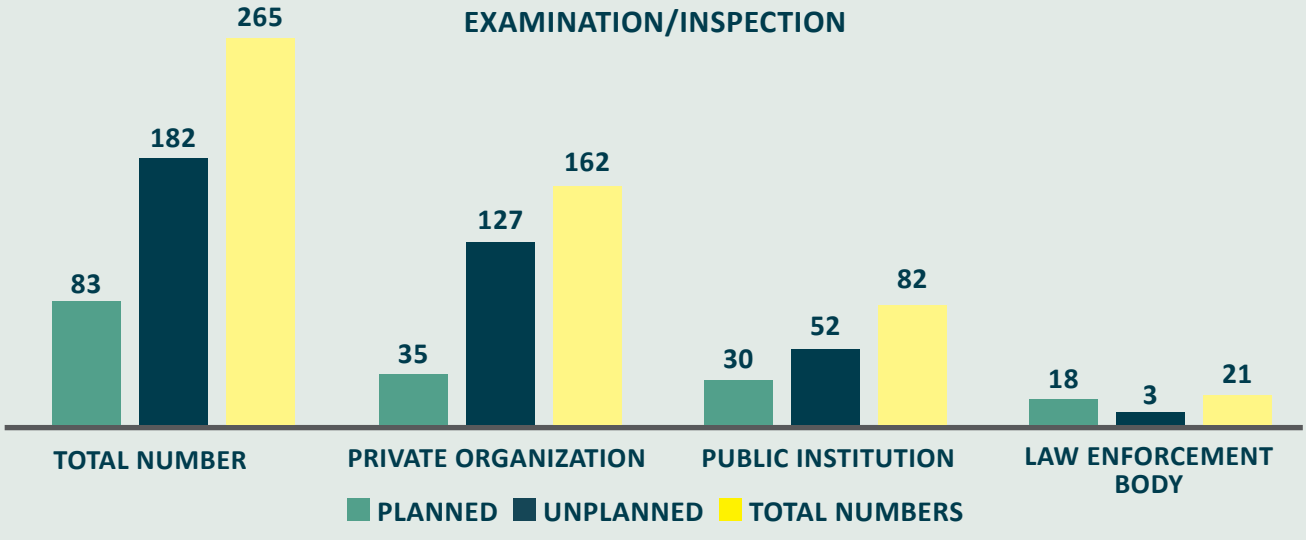
ANNEX №2: STATISTICAL DATA

1. STATISTICS ON THE MONITORING OF THE LAWFULNESS OF DATA PROCESSING



During the reporting period, the Personal Data Protection Service received a total of 1,662 applications and notifications, of which 52% (863) were applications and 48% (799) were notifications. Of the total submissions, 90% (1,486) concerned data processing by private organizations, 8% (140) by public institutions, and 2% (36) by law enforcement agencies.

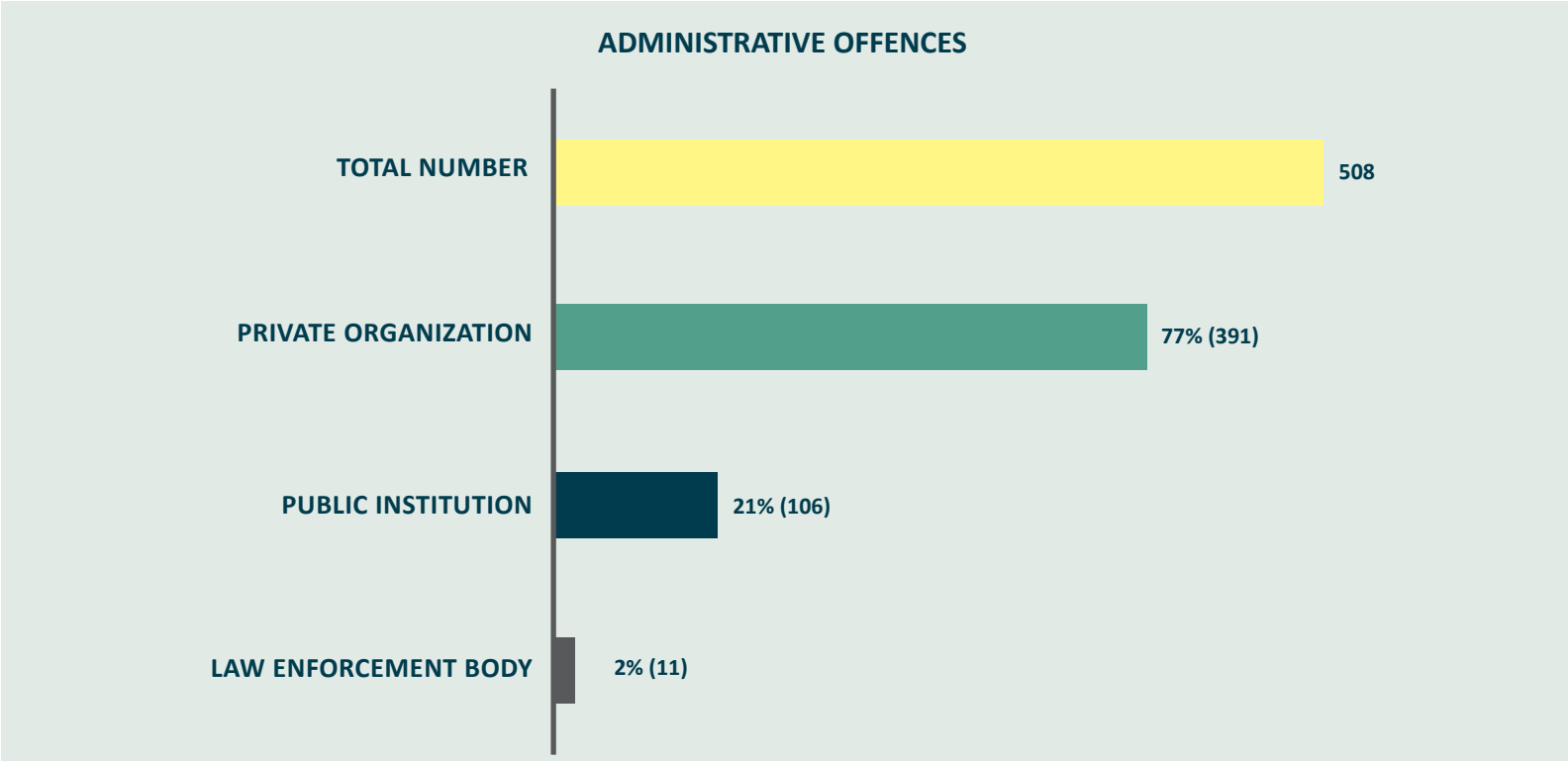
It is noteworthy that the number of applications and notifications received has increased significantly compared to 2023. In that year, the Service received a total of 526 applications/ notifications, of which 83% (436) were applications and 17% (90) were notifications. Regarding subject matter, 66% (350) of the 2023 submissions concerned data processing by private entities or individuals, 23% (120) by public institutions, and 11% (56) by law enforcement agencies.



In 2024, the Personal Data Protection Service conducted inspections on 265 instances of personal data processing to assess their lawfulness. Of these, 31% (83 inspections) were conducted on a planned basis, while 69% (182 inspections) were unplanned. Regarding the sectors involved 61% (162 inspections) concerned data processing by the private sector, 31% (82) by public institutions, and 8% (21) by law enforcement agencies.

In comparison, in 2023, the Service conducted 192 inspections, of which 59% (114) were unplanned and 41% (78) were planned. Sector-wise, 54% (103 inspections) concerned the private sector, 32% (62) public institutions, and 14% (27) law enforcement agencies.

ADMINISTRATIVE OFFENCES



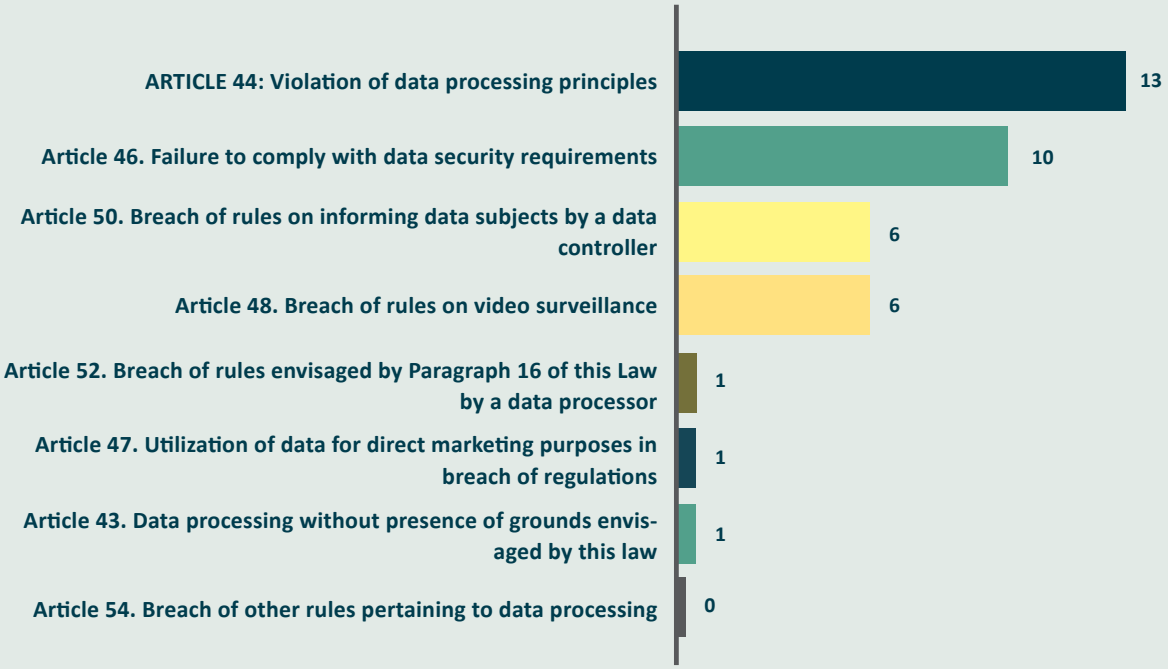
In 2024, the Personal Data Protection Service identified 508 instances of unlawful personal data processing. Of these, 29 cases were revealed through inspections initiated in 2023 and completed during the reporting period, while 479 cases were identified through inspections both initiated and completed in 2024. Sector-wise, 77% (391 cases) concerned unlawful data processing in the private sector, 21% (106 cases) in the public sector, and 2% (11 cases) in law enforcement agencies.

It is noteworthy that the number of detected violations increased significantly compared to 2023. In that year, the Service identified 267 cases of unlawful personal data processing, including 39 cases from inspections initiated in 2022 and completed in 2023, and 228 cases from inspections both initiated and completed within 2023. Of these, 63% (168 cases) involved the private sector, 26% (70 cases) the public sector, and 11% (29 cases) law enforcement agencies.

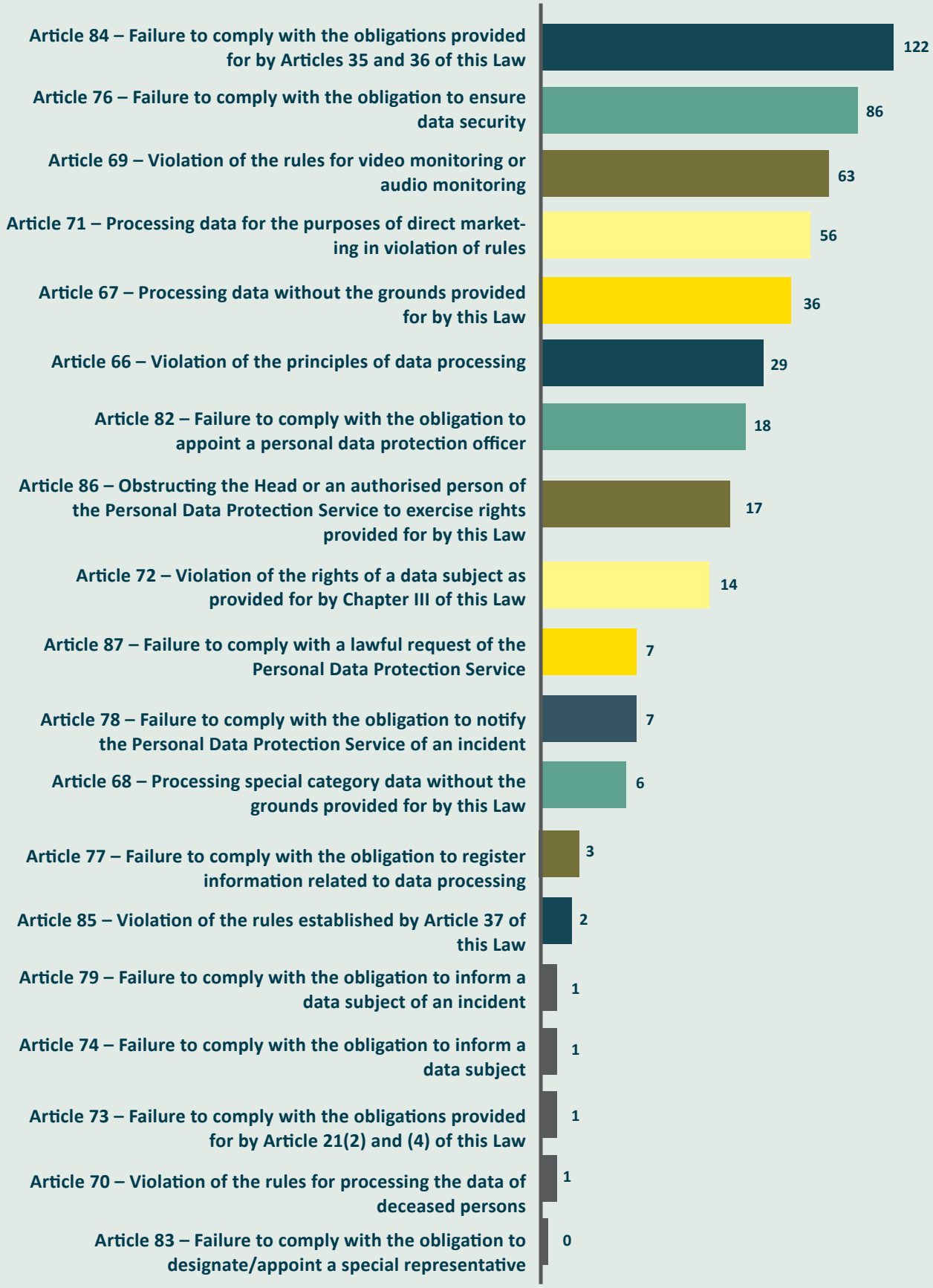
ADMINISTRATIVE OFFENCES

The Law "On Personal Data Protection" entered into force on March 1, 2024. Accordingly, statistical data for January–February 2024 is presented within the framework of the previous law, while data from March 1 through December 31, 2024, is reported in accordance with the provisions of the new law in effect from March 2024.

OFFENCES IDENTIFIED UNDER THE LAW PRIOR TO MARCH 1, 2024



OFFENCES IDENTIFIED UNDER THE LAW AFTER MARCH 1, 2024



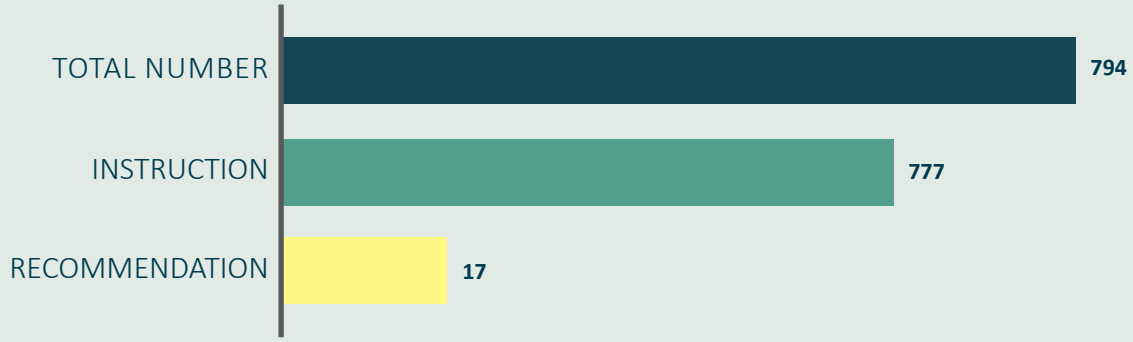
Of the 508 violations identified by the Personal Data Protection Service during the reporting period, 24% (122 cases) concerned non-fulfillment of obligations under Articles 35 and 36 of the Law of Georgia "On Personal Data Protection", relating to the obligation to inform the data subject. Seventeen percent (86 cases) involved non-compliance with data security requirements, and 12% (63 cases) related to violations of the rules governing video or audio monitoring.

In comparison, of the 267 violations identified in 2023, 33% (89 cases) involved non-fulfillment of data security obligations, 18% (49 cases) related to violations of data processing principles, and 15% (39 cases) concerned breaches of video monitoring regulations.

During the reporting period, the Service imposed administrative penalties—fines and warnings—in a total of 505 cases. Of the 312 fines issued, 9 were related to inspections initiated in 2023 and completed during the reporting period, while 303 were related to inspections both initiated and completed within the reporting period. Out of the 193 warnings issued, 17 stemmed from inspections initiated in 2023 and concluded during the reporting period, and 176 from inspections initiated and completed within the same period. In terms of distribution, 77% (390) of the administrative penalties were imposed on private institutions, 21% (104) on public institutions, and 2% (11) on law enforcement bodies.

The total number of administrative penalties imposed increased compared to 2023. Specifically, during the reporting period, 225 individuals were subject to administrative sanctions. Among them, 123 subjects (55%) received fines, while 102 (45%) were issued warnings.

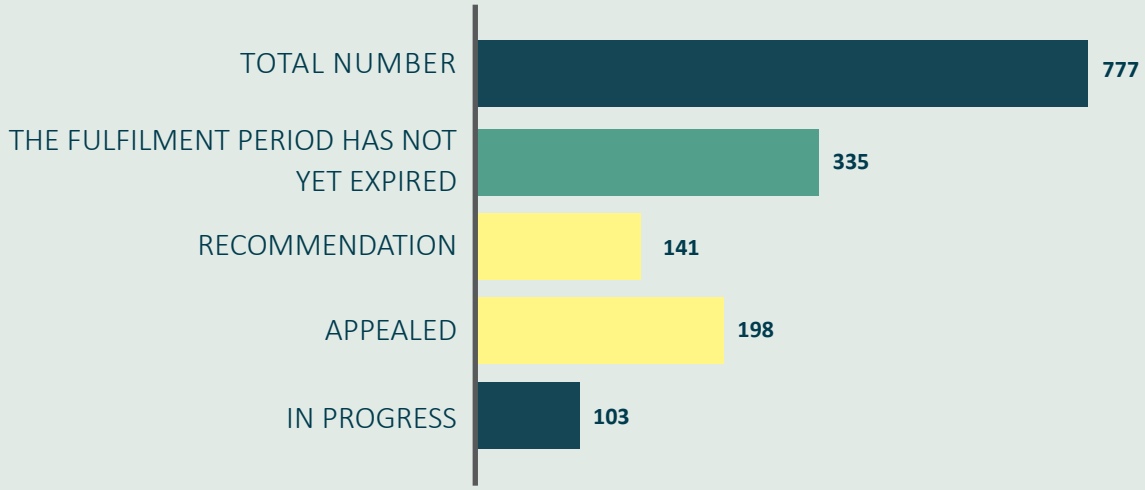
INSTRUCTIONS AND RECOMMENDATIONS



In addition to imposing administrative penalties, the Service issued a total of 794 instructions[115] and recommendations[116] to public institutions, private organizations, and law enforcement bodies to address identified shortcomings. Of the 777 instructions issued, 60 pertained to inspections initiated in 2023 and concluded during the reporting period, while 717 were related to inspections both initiated and concluded within the reporting period. As for the 17 recommendations issued, 1 was connected to an inspection that began in 2023, and 16 to inspections initiated and completed during the reporting year.

Of the total 794 instructions and recommendations, 65% (519) were directed to private institutions, 28% (220) to public institutions, and 7% (55) to law enforcement bodies. Notably, the number of issued instructions and recommendations increased significantly compared to 2023, when the Service issued a total of 472.

FULFILMENT RATE OF INSTRUCTIONS ISSUED BY THE SERVICE BY SECTOR

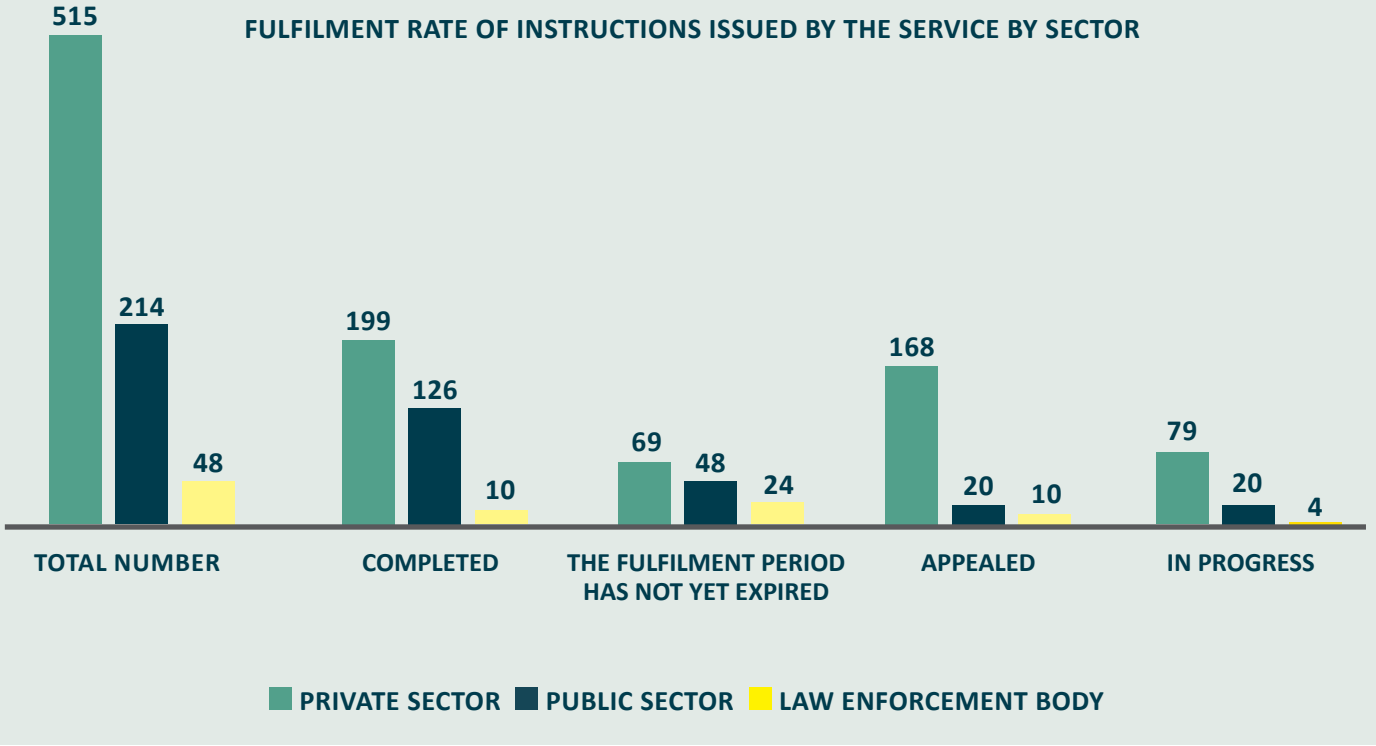


[115] **An instruction** is a written directive issued by the Service to the data controller and/or data processor, which is mandatory for implementation. It concerns the application of measures outlined in subparagraphs "a"–"d" of paragraph 1 of Article 52 of the Law of Georgia "On Personal Data Protection".

[116] **A recommendation,** on the other hand, is a written advisory issued by the Service to the data controller and/or data processor, aimed at reducing the risk of violations in the data processing process.

It is noteworthy that out of the 777 instructions issued during the reporting period, 43% (335) were fully completed, 18% (141) are still within the deadline for completion, 26% (198) have been appealed, and 13% (103) are currently in the process of being completed.

Importantly, the overall instruction completion rate has increased compared to the previous year. In 2023, 52% (239) of the issued instructions were completed.



private institutions. Of these: 39% (199) have been completed, 13% (69 orders) are within the deadline for completion, 33% (168) have been appealed, and 15% (79) are currently in the process of being implemented.

Out of 214 mandatory instructions issued to public institutions: 60% (126 orders) have been completed, 22% (48) are within the deadline for completion, 9% (20 orders) have been appealed, and 9% (20) are in progress.

Of the 48 mandatory instructions issued to law enforcement bodies: 21% (10) have been completed, 50% (24) are within the deadline for completion, 21% (10) have been appealed, and 8% (4) are in the process of being completed.

Obligation to Notify the Personal Data Protection Service of a Data Breach (Incident)

11

According to Article 3, Subparagraph "t" of the Law of Georgia "On Personal Data Protection", an "incident" is defined as a data breach that results in the unlawful or accidental damage, loss, unauthorized disclosure, destruction, alteration, access to, collection/retrieval of, or other unauthorized processing of personal data.

Pursuant to Article 29 of the Law, the data controller is obliged to document the incident, including its consequences and the measures taken, and to notify the Personal Data Protection Service of the incident either in writing or electronically, no later than 72 hours after becoming aware of it—unless the incident is unlikely to result in significant harm and/or pose a serious risk to the fundamental rights and freedoms of individuals[117].

During the reporting period, the Personal Data Protection Service received 11 notifications of data breaches (incidents) from data controllers.

- **Individuals Accessing Their Own Data**

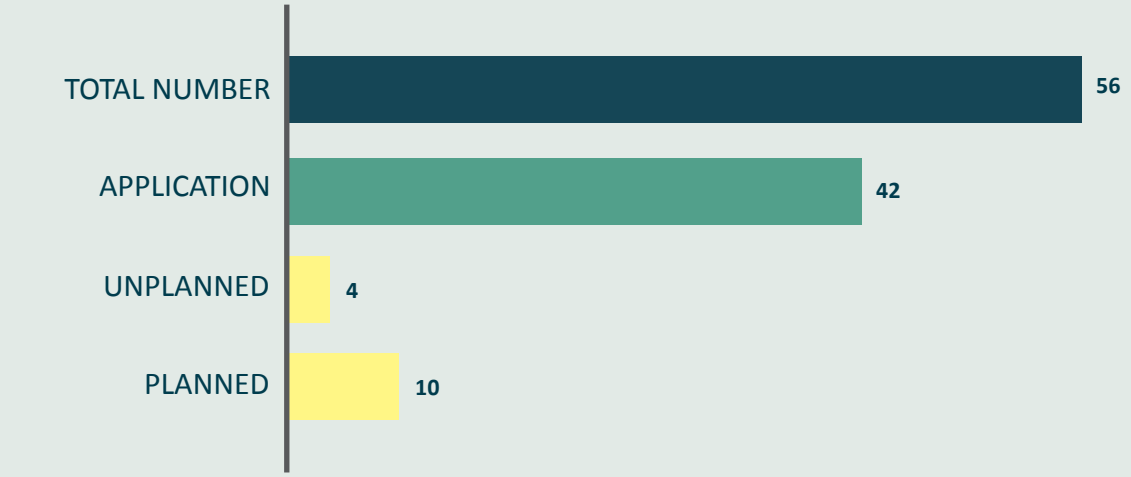
In 2024, within the framework of Chapters III and IV of the Law of Georgia "On Personal Data Protection", the Personal Data Protection Service examined 56 cases concerning the lawfulness of informing individuals by various agencies. Of these, 10 cases were initiated by the Service, 4 were unplanned inspections, and 42 were based on submitted applications.

As a result of the investigations, administrative liability was imposed on 22 individuals. Of these, 9 received a warning as a sanction, while 13 were fined. Alongside administrative measures, to improve data processing practices in both public and private institutions and to ensure compliance with the Law of Georgia "On Personal Data Protection", the Service issued 49 mandatory instructions and 4 recommendations.

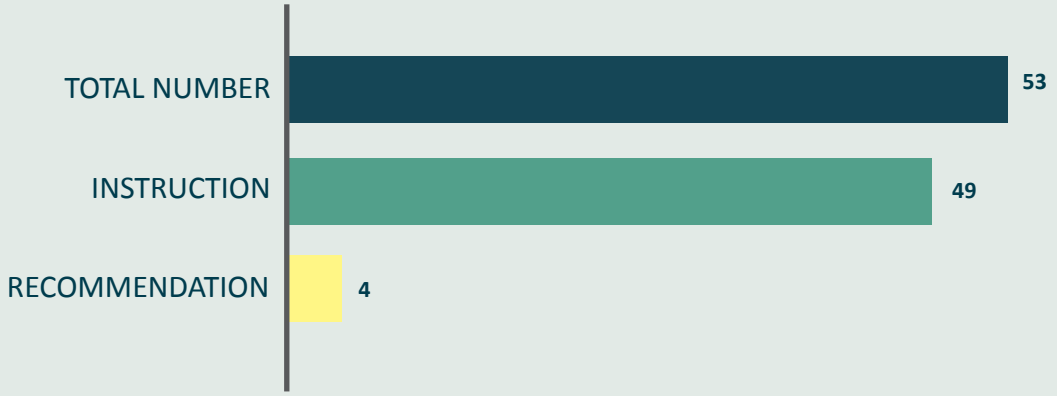
In comparison, in 2023, the Personal Data Protection Service examined 91 cases related to the lawfulness of informing individuals. Based on the findings, 36 individuals were held administratively liable. The Service issued 73 mandatory instructions and 1 recommendation.

[117] **Law of Georgia "On Personal Data Protection" Article 29, Paragraph 1.**

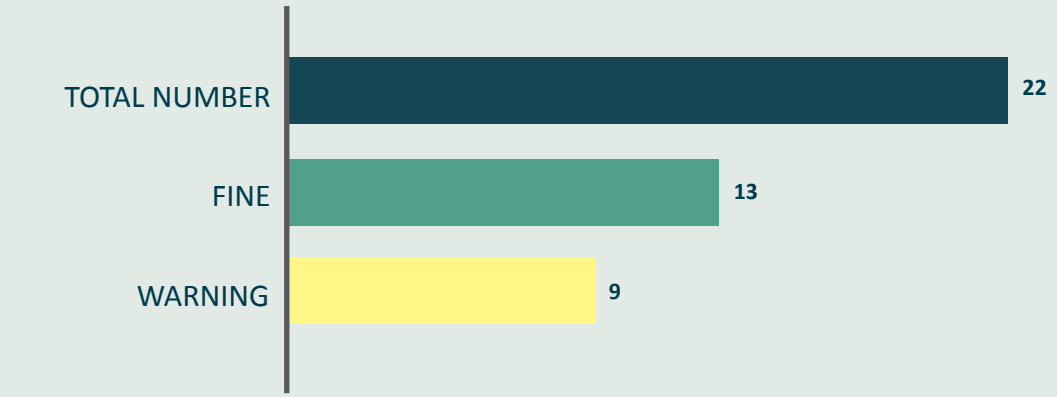
EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

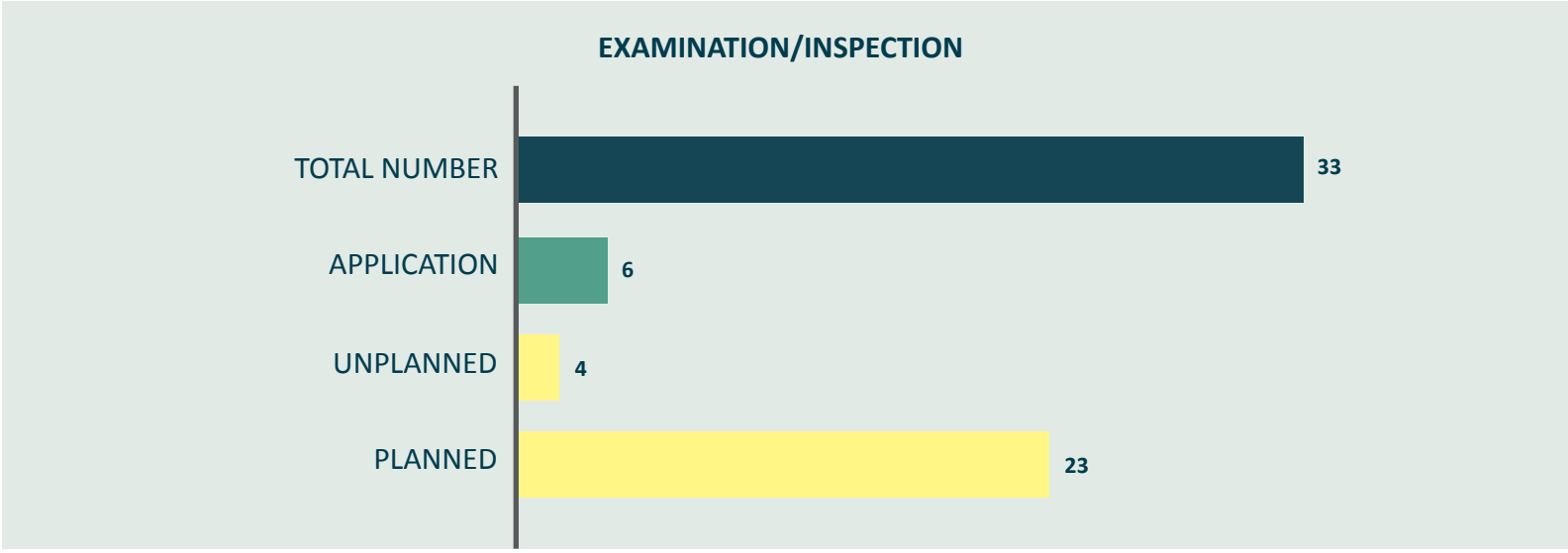


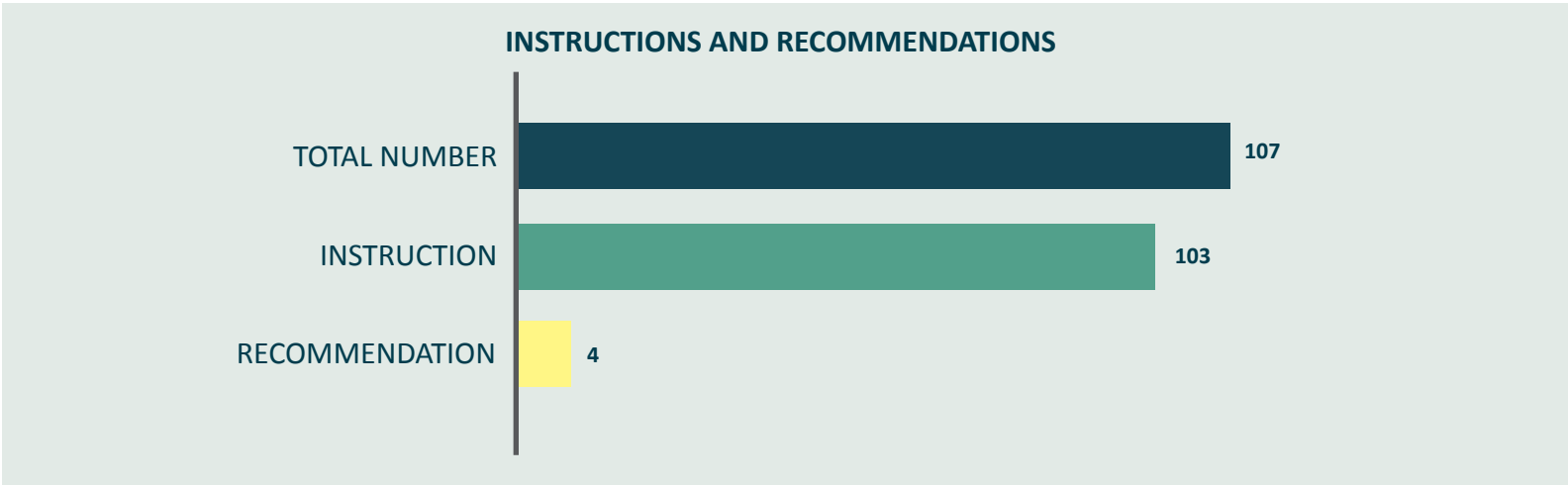
- **Protection of Minors' Personal Data**

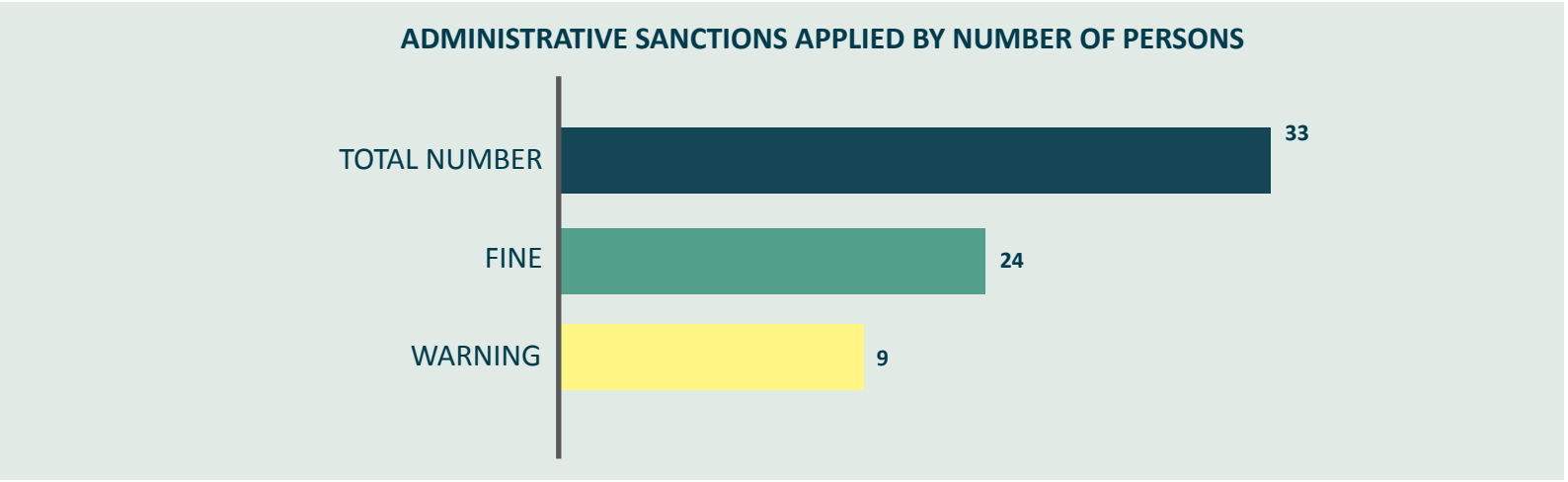
In 2024, the Personal Data Protection Service examined 33 cases concerning the processing of minors' personal data. Of these, 23 were initiated by the Service, 4 were unplanned inspections, and 6 were based on applications.

As a result of these examinations, administrative liability was imposed on 33 subjects. Of these, 9 received a warning as a sanction, while 24 were fined. In addition to administrative penalties, and with the aim of improving data processing practices in public and private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 4 recommendations and 103 mandatory instructions.

In 2023, the Service examined 34 cases related to the processing of minors' personal data. Based on these cases, administrative liability was imposed on 24 subjects. The Service issued 3 recommendations and 77 mandatory instructions.





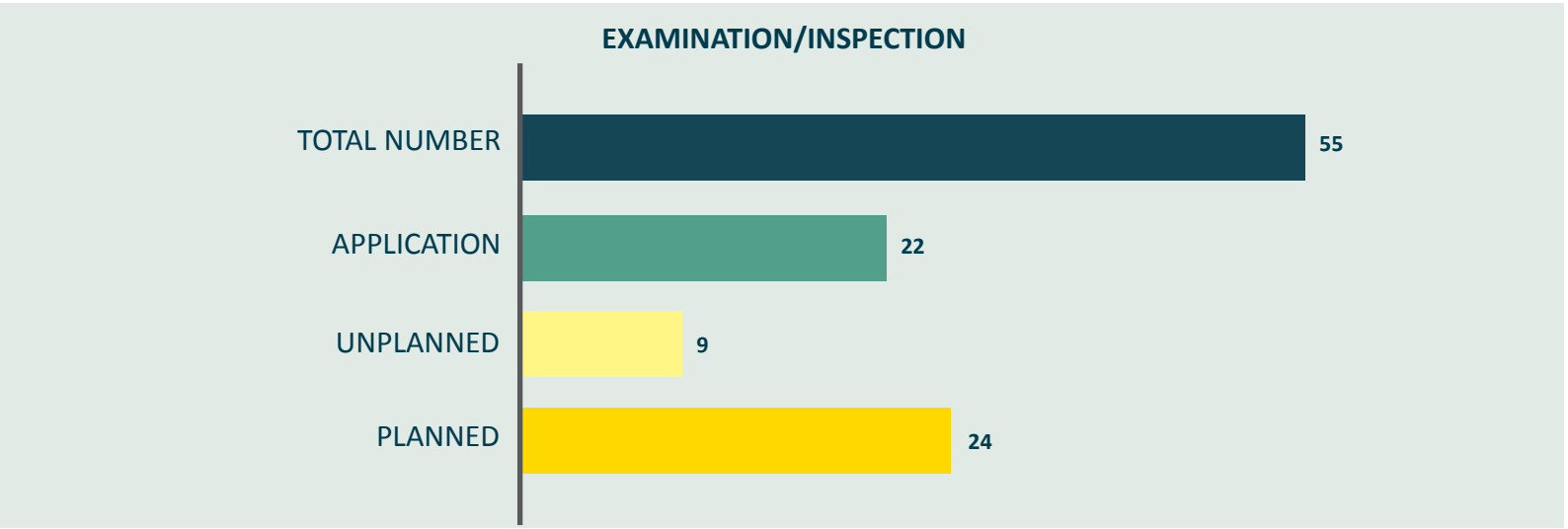


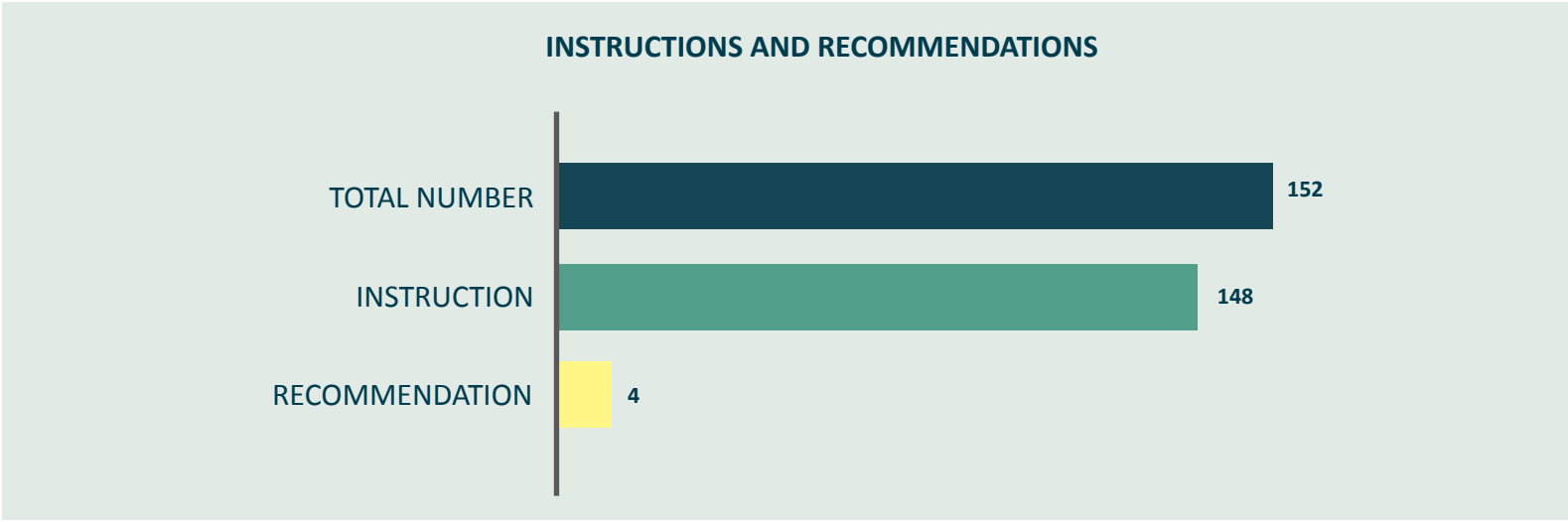
- **Protection of Personal Data in the Field of Labour Relations/Employment**

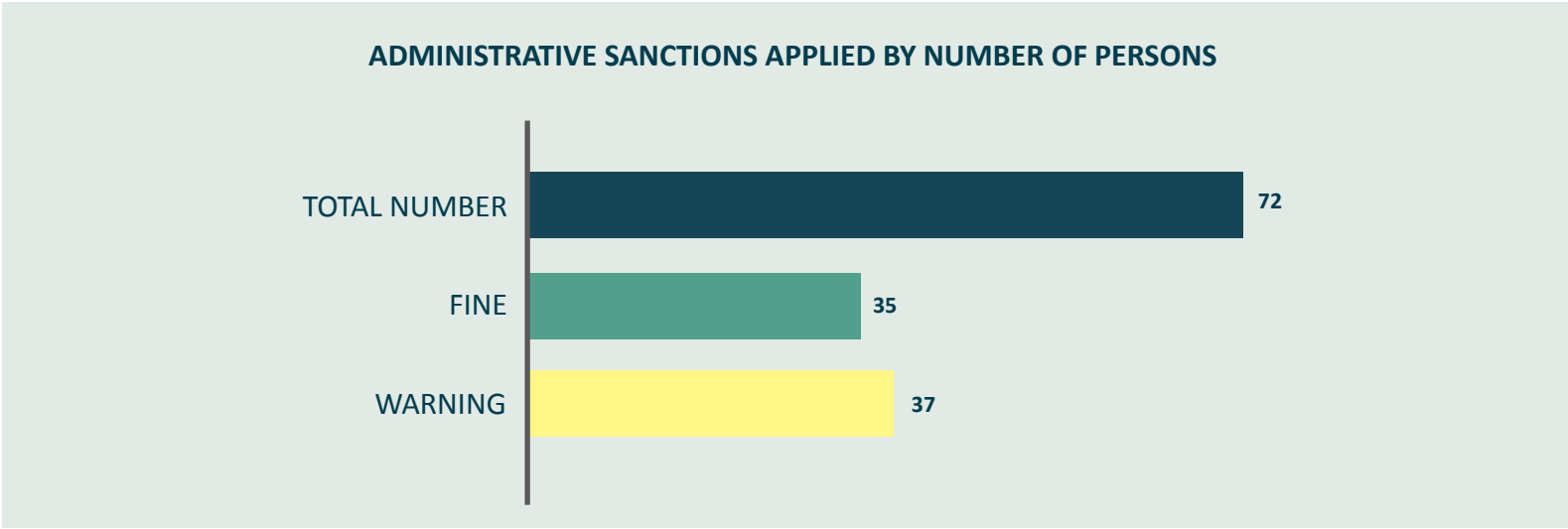
In 2024, the Personal Data Protection Service examined 55 cases of personal data processing within the framework of labor relations. Of these, 24 were initiated by the Service, 9 were unplanned inspections, and 22 were based on citizens' applications.

As a result of these examinations, administrative liability was imposed on 72 individuals. Of these, 37 received a warning as a sanction, while 35 were fined. In addition to administrative penalties, and with the aim of improving data processing practices in public and private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 4 recommendations and 148 mandatory instructions.

In 2023, the Service examined 57 cases of personal data processing in the context of labor relations. As a result, administrative liability was imposed on 26 individuals. That year, the Service issued 7 recommendations and 74 mandatory instruction.





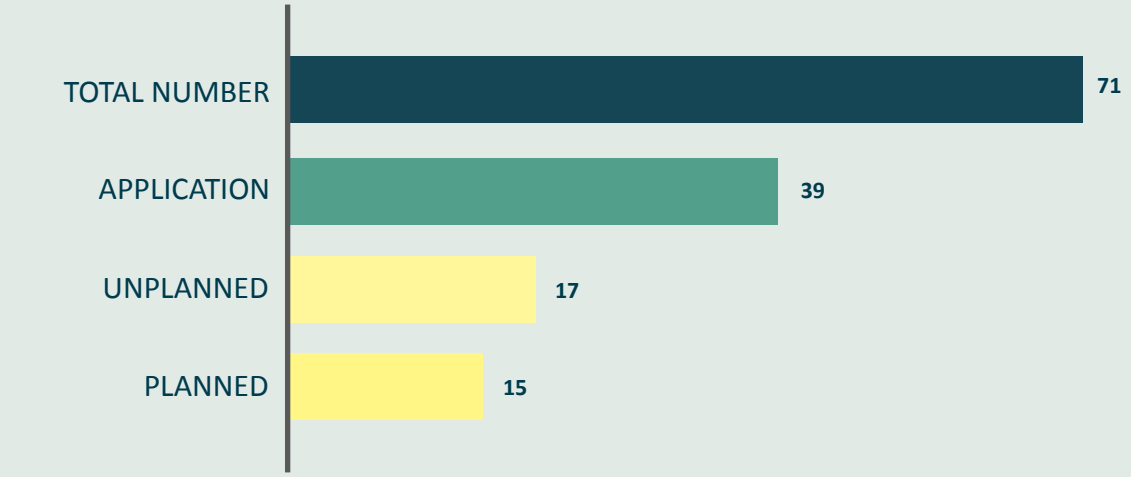


- **Video Surveillance**

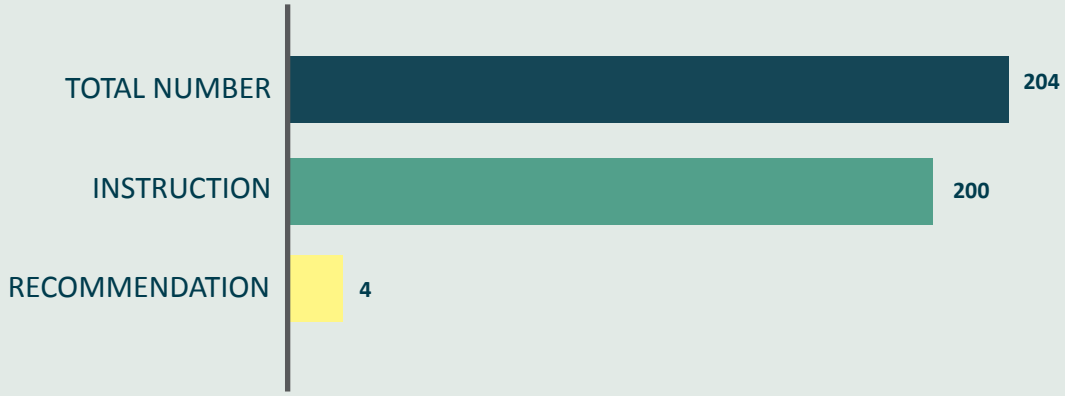
In 2024, the Personal Data Protection Service examined 71 cases of video monitoring in state structures and private institutions. Of these, 15 were initiated by the Service, 17 were unplanned inspections, and 39 were based on applications.

As a result of these examinations, administrative liability was imposed on 81 individuals. Of these, 39 received a warning as a sanction, while 42 were fined. In addition to administrative penalties, and with the aim of improving data processing practices in public and private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 4 recommendations and 200 mandatory instructions.

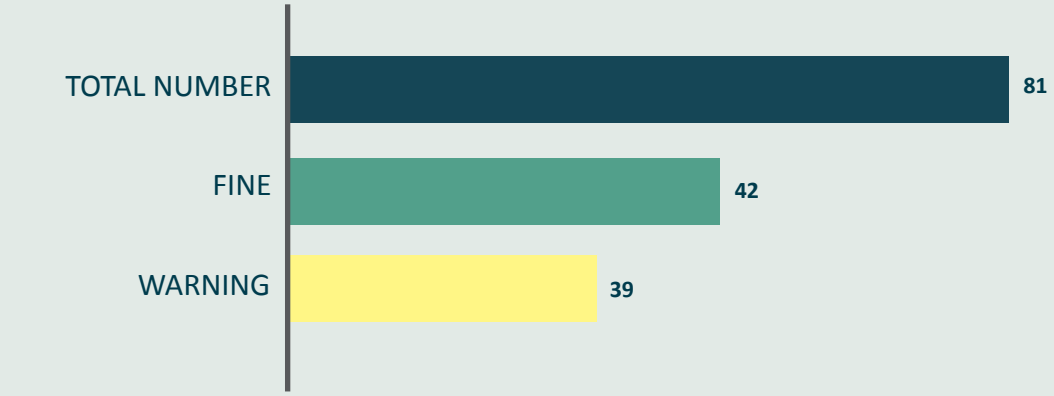
EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS

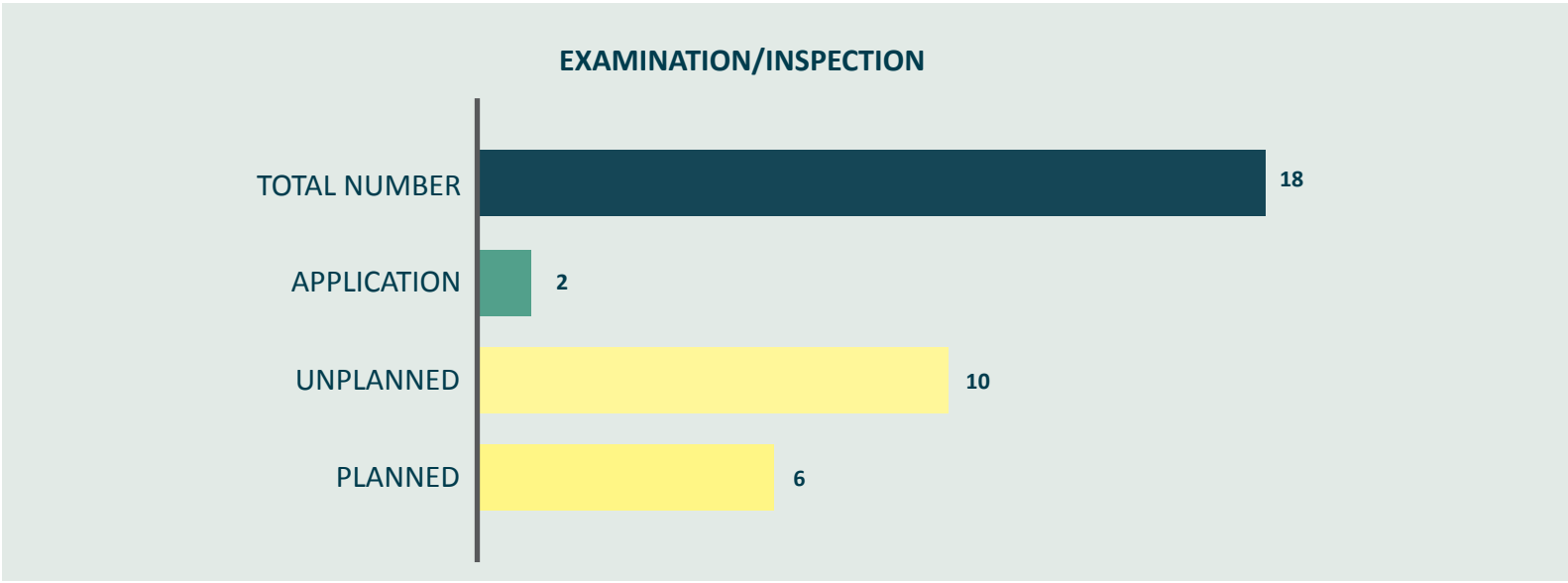


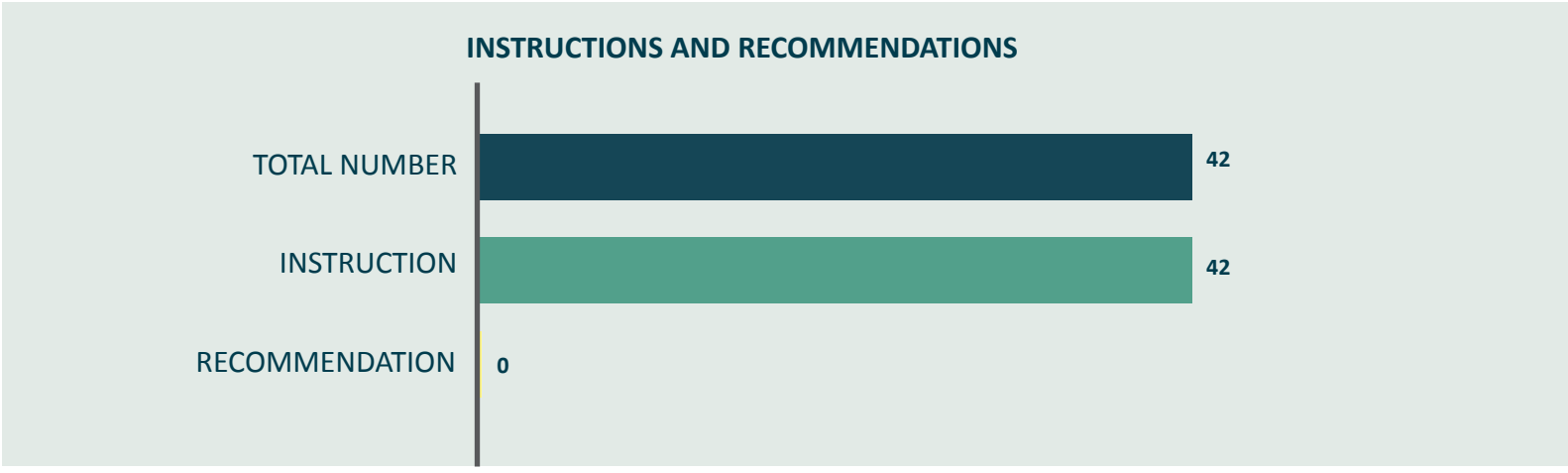
- **Processing of Personal Data in the Health Sector**

During the reporting period, the Personal Data Protection Service examined 18 cases of personal data processing in the healthcare sector. Of these, 6 were initiated by the Service, 10 were unplanned inspections, and 2 were based on citizens' applications.

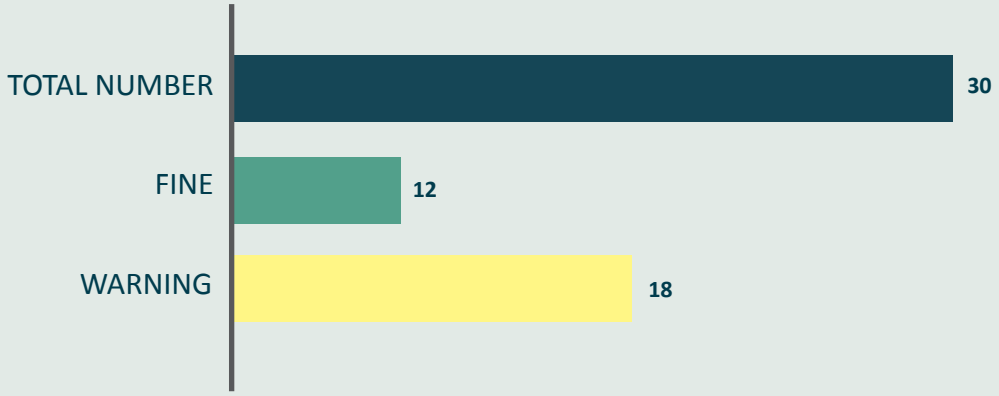
As a result of these examinations, administrative liability was imposed on 30 individuals. Of these, 18 received a warning as a sanction, while 12 were fined. In addition to administrative penalties, and with the aim of improving data processing practices in public and private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 42 mandatory instructions.

In 2023, the Service examined 15 cases of personal data processing in the healthcare sector, resulting in administrative liability for 18 individuals. That year, the Service issued 35 mandatory instructions and 1 recommendation.





ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS



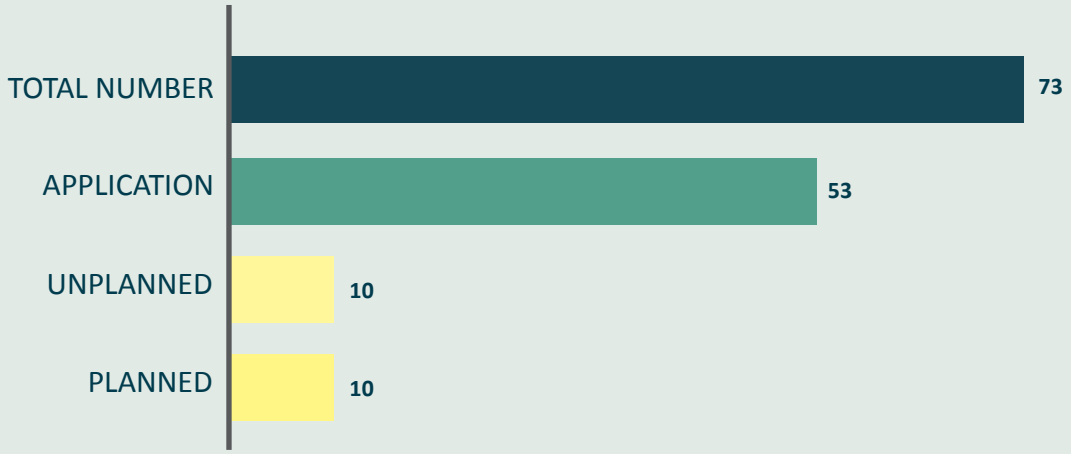
- **Processing of Personal Data in the Financial Sector**

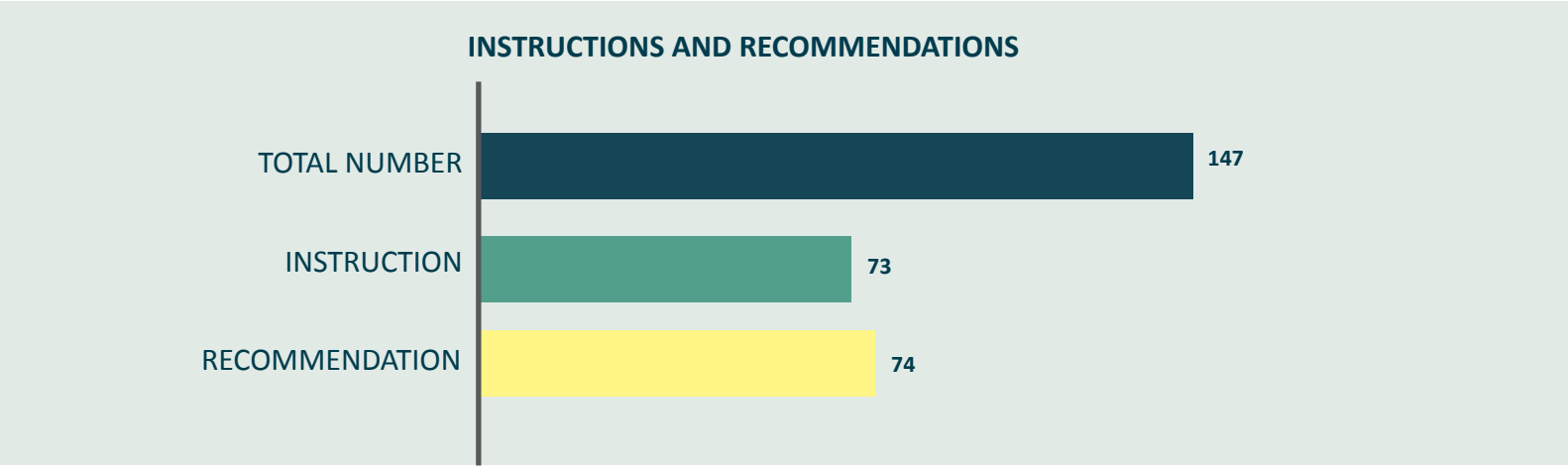
In 2024, the Personal Data Protection Service examined 73 cases of personal data processing in the financial sector. Of these, 10 were initiated by the Service, 10 were unplanned inspections, and 53 were based on citizens' applications.

As a result of these examinations, administrative liability was imposed on 62 subjects. Of these, 7 received a warning as a sanction, while 55 were fined. In addition to administrative penalties, and with the aim of improving data processing practices in private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 73 mandatory instructions and 74 recommendations.

In 2023, the Service examined 41 cases of personal data processing in the financial sector, resulting in administrative liability for 18 subjects. In that year, the Service issued 24 mandatory instructions.

EXAMINATION/INSPECTION





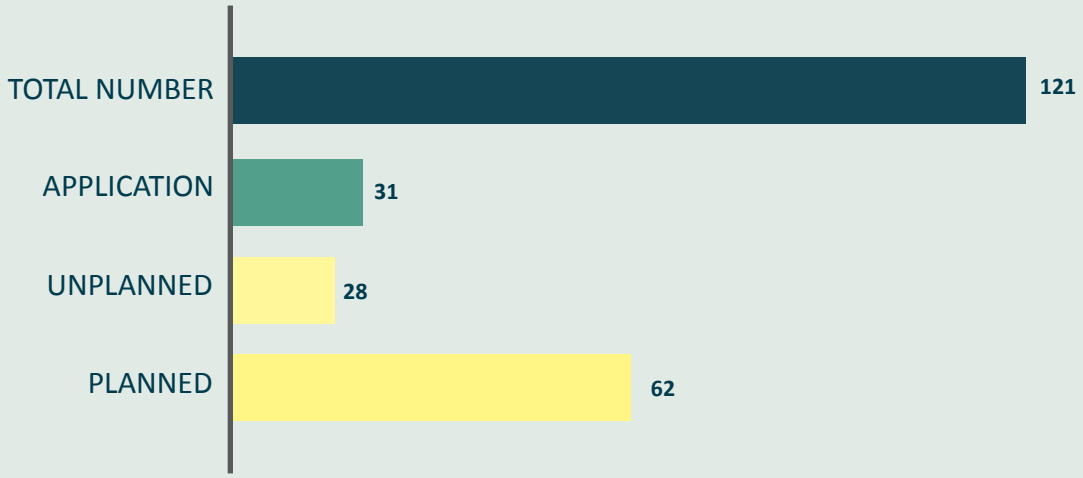
- **Data Security**

In 2024, the Personal Data Protection Service examined 121 cases related to data security. Of these, 62 were initiated by the Service, 28 were unplanned inspections, and 31 were based on citizens' applications.

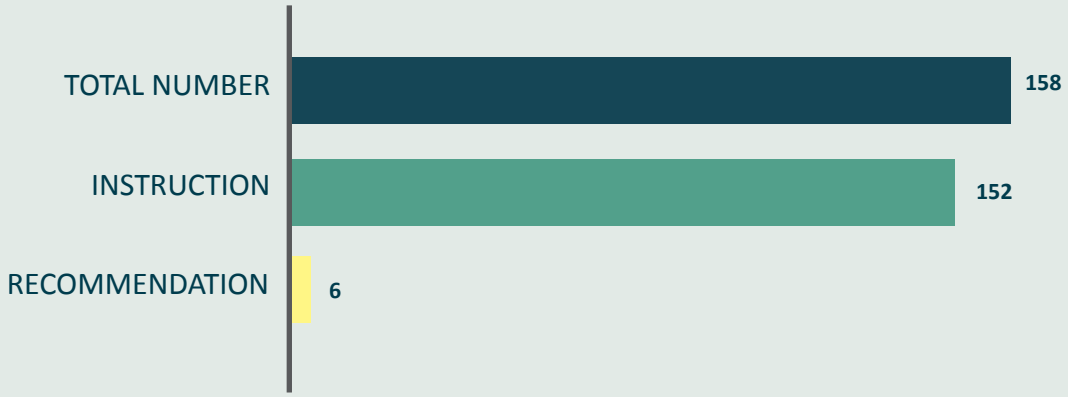
As a result of these examinations, administrative liability was imposed on 100 subjects. Of these, 57 received a warning as a sanction, while 43 were fined. In addition to administrative penalties, and with the aim of improving data processing practices in public and private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 6 recommendations and 152 mandatory instructions.

In 2023, the Service examined 90 data security cases, resulting in administrative liability for 84 subjects. In that year, the Service issued 4 recommendations and 155 mandatory instructions.

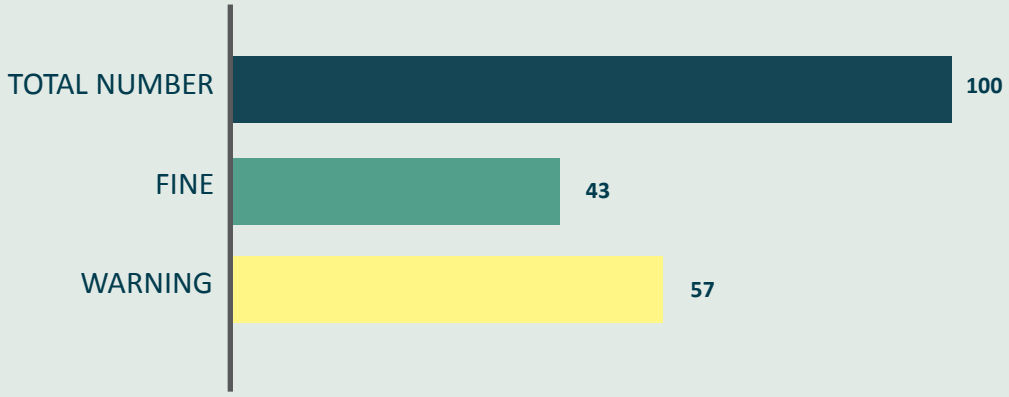
EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS



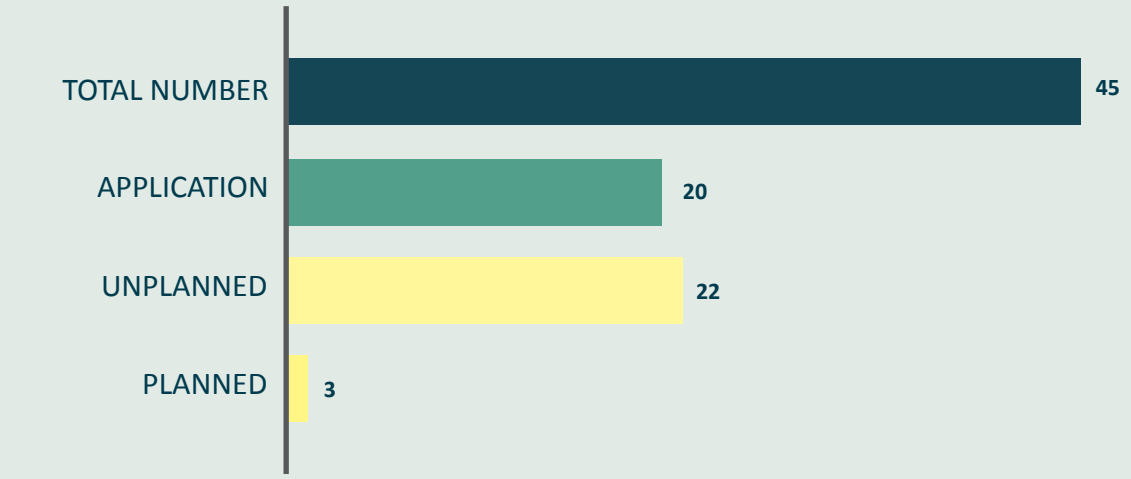
- **Processing of Personal Data for the Purpose of Direct Marketing**

During the reporting period, the Personal Data Protection Service examined 45 cases of personal data processing for direct marketing purposes. Of these, 3 were initiated by the Service, 22 were conducted as unplanned inspections, and 20 were based on citizens' applications.

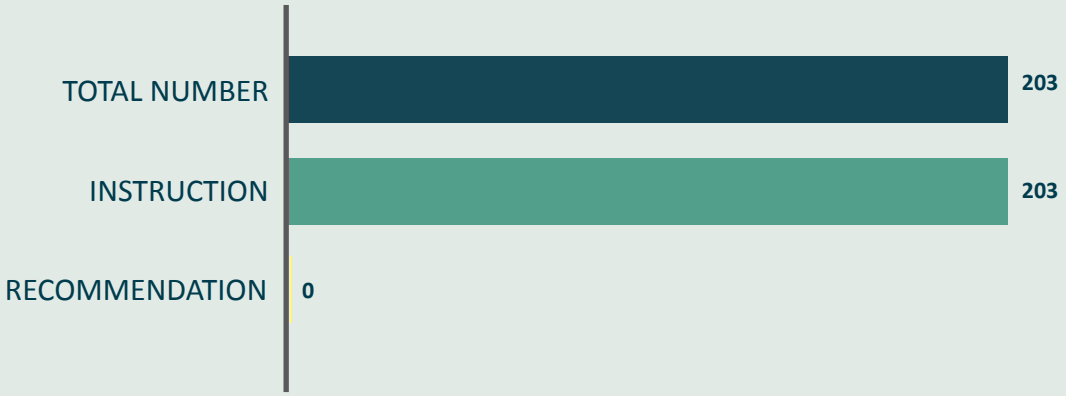
As a result of these examinations, administrative liability was imposed on 165 subjects. Of these, 11 were sanctioned with a warning, while 154 were fined.

In addition to imposing administrative penalties, and with the aim of improving data processing practices in both public and private institutions and ensuring their compliance with the Law of Georgia "On Personal Data Protection," the Service issued 203 mandatory instructions.

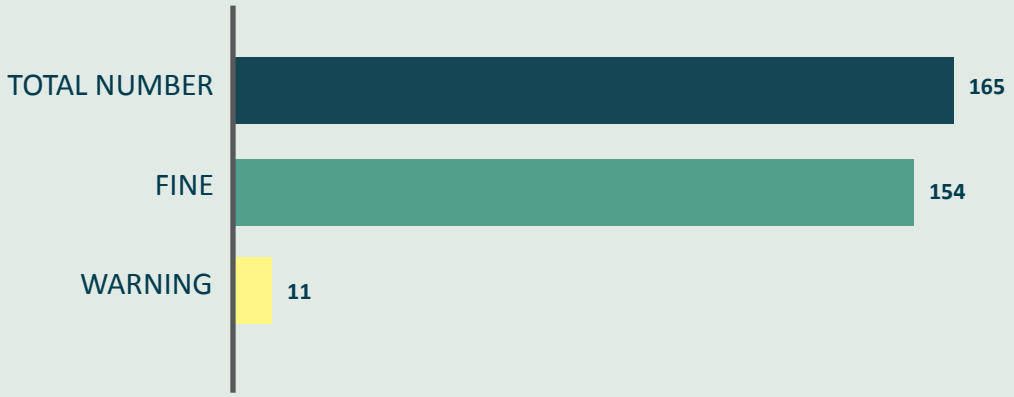
EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS



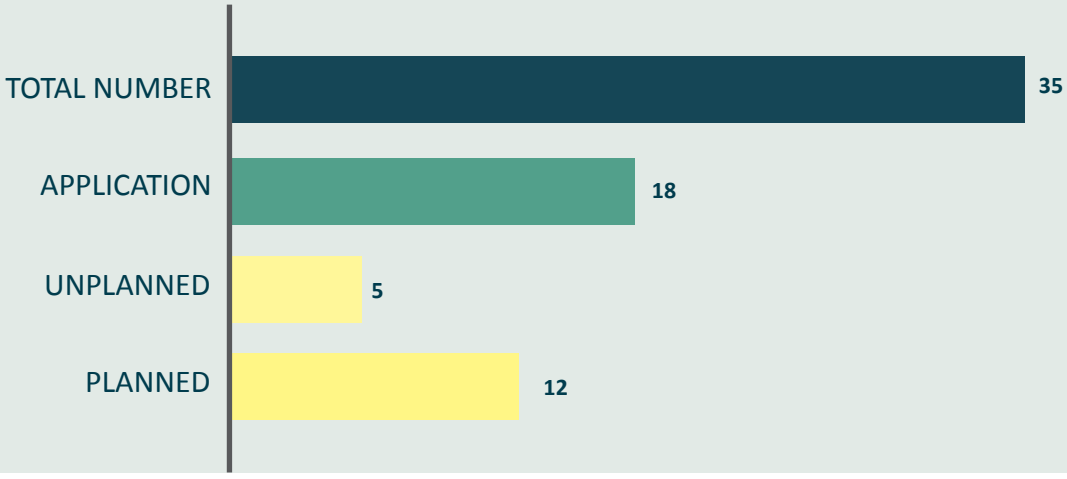
- **Implementation of Audio Monitoring**

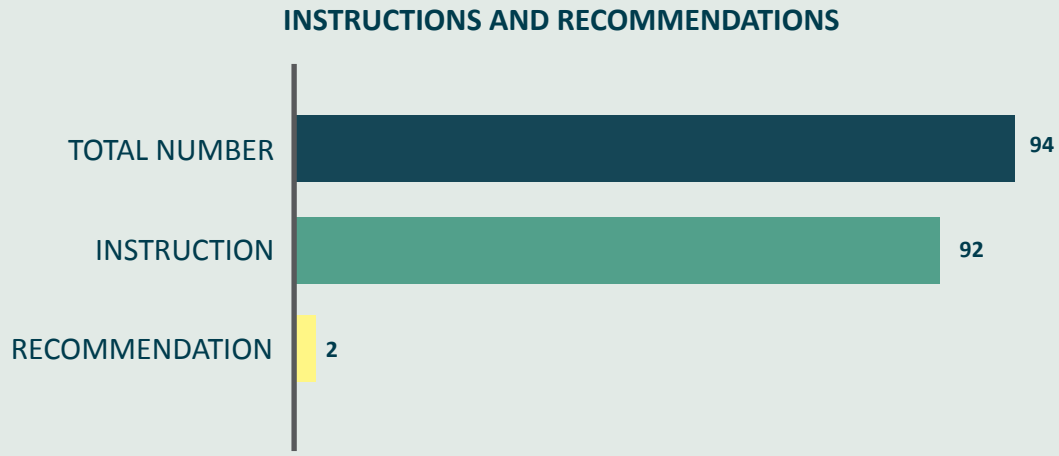
In 2024, the Personal Data Protection Service examined 35 cases of personal data processing related to the implementation of audio monitoring. Of these, 12 were initiated by the Service, 5 were conducted as unplanned inspections, and 18 were based on citizens' applications.

As a result of the examinations, administrative liability was imposed on 38 subject. Of these, 19 were sanctioned with a warning, while 19 were fined.

In addition to the administrative measures, and with the objective of enhancing data processing practices in public and private institutions and ensuring their compliance with the Law of Georgia "On Personal Data Protection," the Service issued 92 mandatory instructions and 2 recommendations.

EXAMINATION/INSPECTION



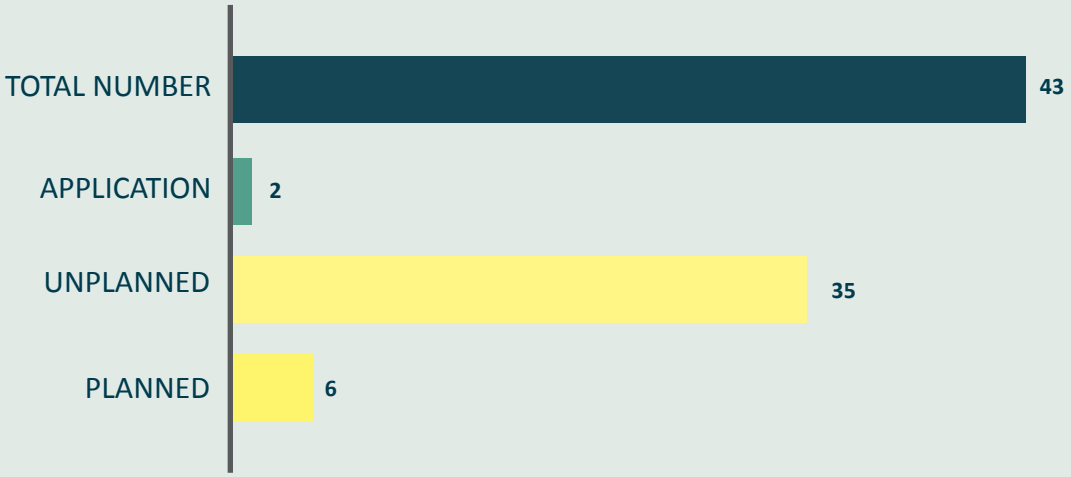


- **The Personal Data Protection Officer**

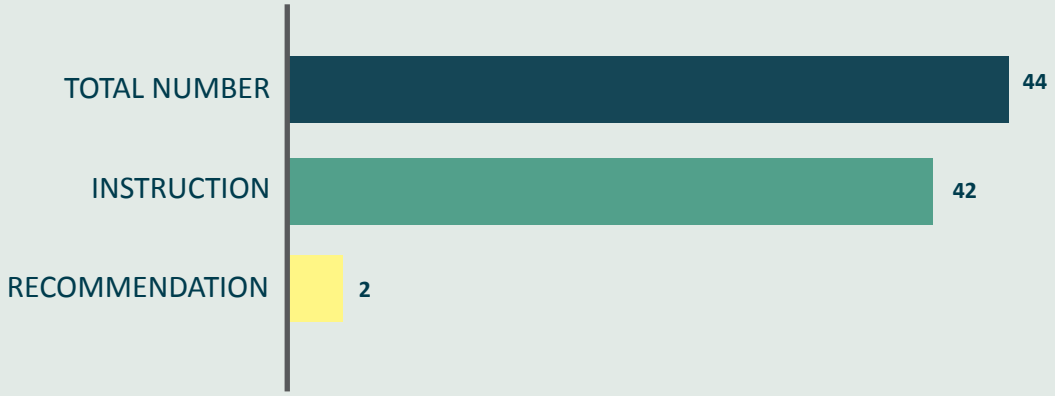
Within the framework of its obligations related to the Personal Data Protection Officer, the Personal Data Protection Service examined 43 cases of personal data processing. Of these, 6 were initiated by the Service, 35 were unplanned, and 2 were based on citizens' applications.

As a result of the cases examined, administrative liability was imposed on 22 subjects, with a warning applied as the sanction in each case. In parallel with the administrative penalties, and with the aim of improving data processing practices in both public and private institutions and ensuring compliance with the Law of Georgia "On Personal Data Protection," the Service issued 42 mandatory instructions and 2 recommendations.

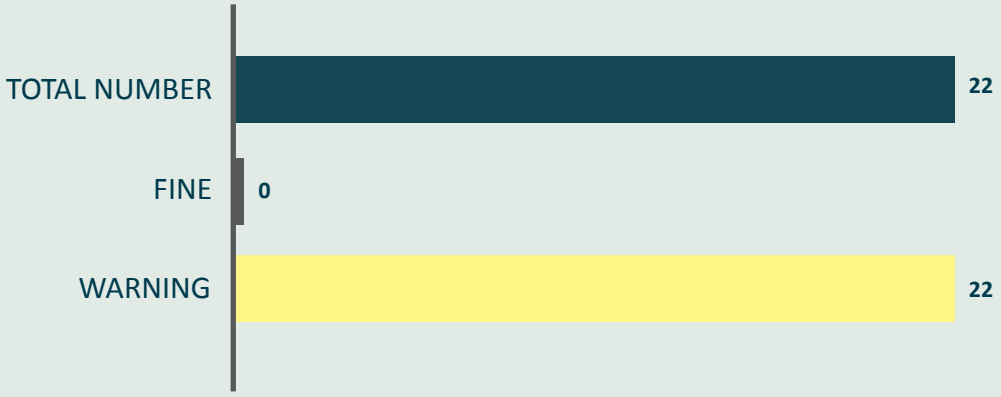
EXAMINATION/INSPECTION



INSTRUCTIONS AND RECOMMENDATIONS



ADMINISTRATIVE SANCTIONS APPLIED BY NUMBER OF PERSONS



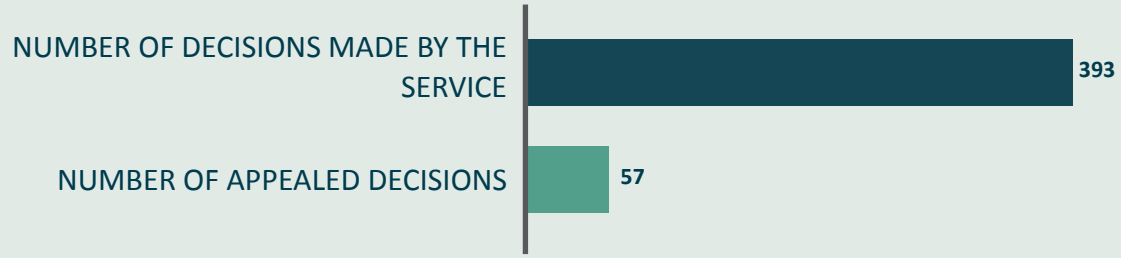
2. OTHER STATISTICAL DATA

TOTAL NUMBER OF CONSULTATIONS

16 462

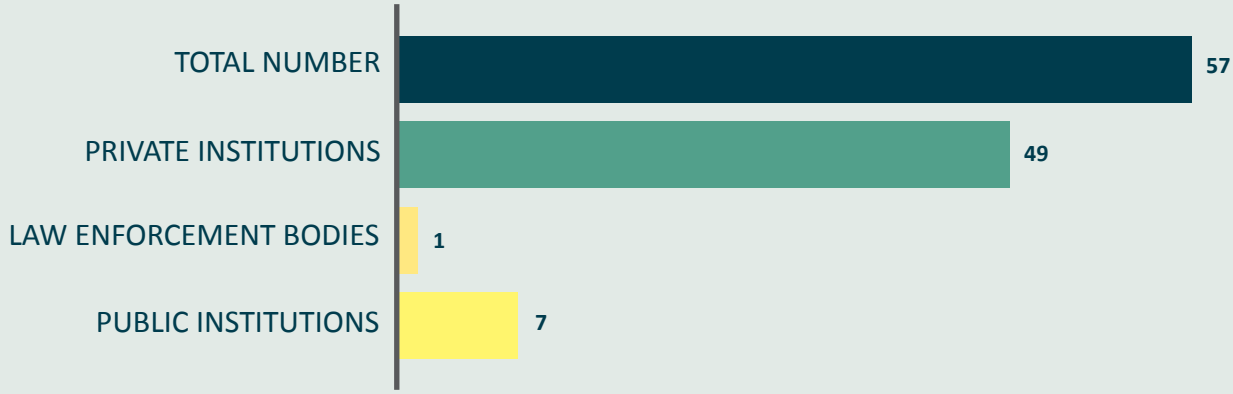
The Service provided a total of 16 462 consultations on monitoring the lawfulness of the protection of personal data and other legal issues. It should be noted that in 2023 the Personal Data Protection Service gave a total of 5106 consultations.

THE RATE OF COURT APPEALS AGAINST DECISIONS OF THE SERVICE



Of the 393 summary decisions issued during the reporting period, 15% (57) were appealed. In 2023, 17% (59) of the 338 summary decisions issued were appealed.

RATE OF DECISIONS OF THE SERVICE APPEALED BY SECTORS



Of the 57 decisions appealed during the reporting period, 86% (49) concerned decisions made against private organizations, 2% (1) against law enforcement bodies, and 12% (7) against public institutions.

Of the 59 decisions appealed in 2023, 59% (35) concerned decisions made against private institutions, 4% (2) against law enforcement bodies, and 37% (22) against public institutions.

PUBLIC AWARENESS-RAISING, INFORMATION MEETINGS AND TRAININGS

Number of Attendees

6522

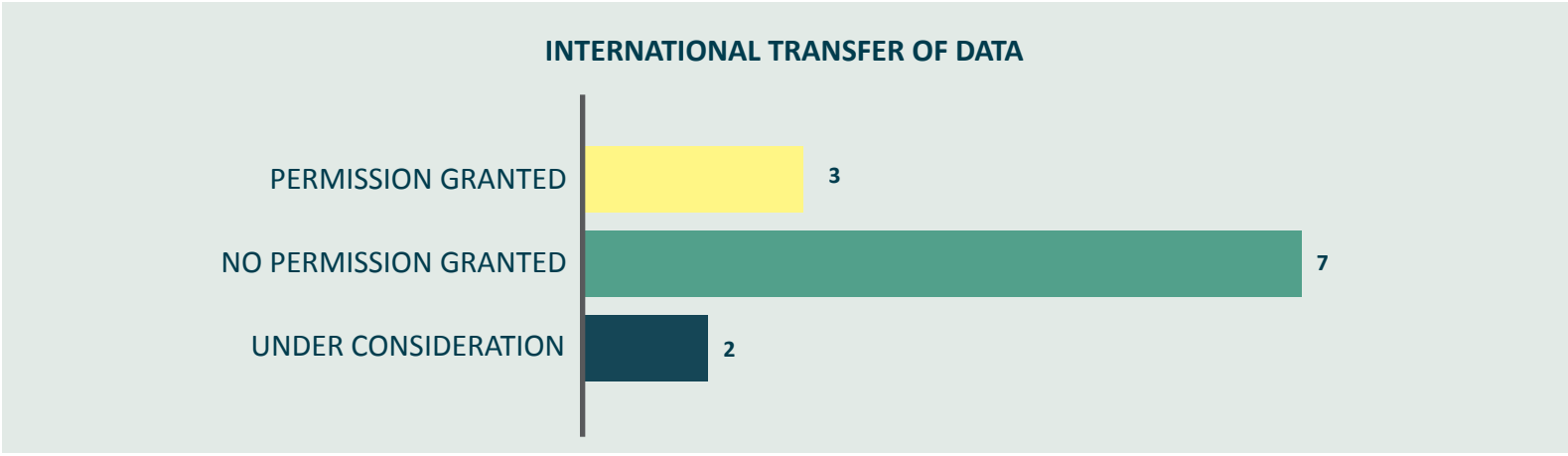
The Service actively carries out educational activities on issues related to data processing and protection. In order to raise awareness of data protection, the Service systematically organises public lectures, information meetings and training sessions for representatives of the private and public sectors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

In 2024, the Service held 108 meetings with a total of 6,522 attendees, some of whom represented both data subjects and data controllers/processors. In 2023, the Service held 62 meetings with 3,158 attendees.

NUMBER OF INFORMATIONAL MEETINGS AND TRAININGS

It is noteworthy that out of the 108 meetings held during the reporting period, 94% (101) were training sessions, and 6% (7) were regional meetings.

Out of the 62 meetings held in 2023, 90% (56) were training sessions, and 10% (6) were regional meetings.



As of December 31, 2024, proceedings were completed in relation to 10 applications for data transfer. Of these, permission was granted in 3 cases and denied in 7 cases. The Service had not completed its review of 2 additional applications.

In 2023, proceedings were completed in relation to 20 applications, all of which were granted permission to transfer data. The review of 2 applications remained pending.

LEGAL EXPERTISE OF DRAFT INTERNATIONAL TREATIES AND AGREEMENTS

LEGAL EXPERTISE OF DRAFT INTERNATIONAL TREATIES AND AGREEMENTS

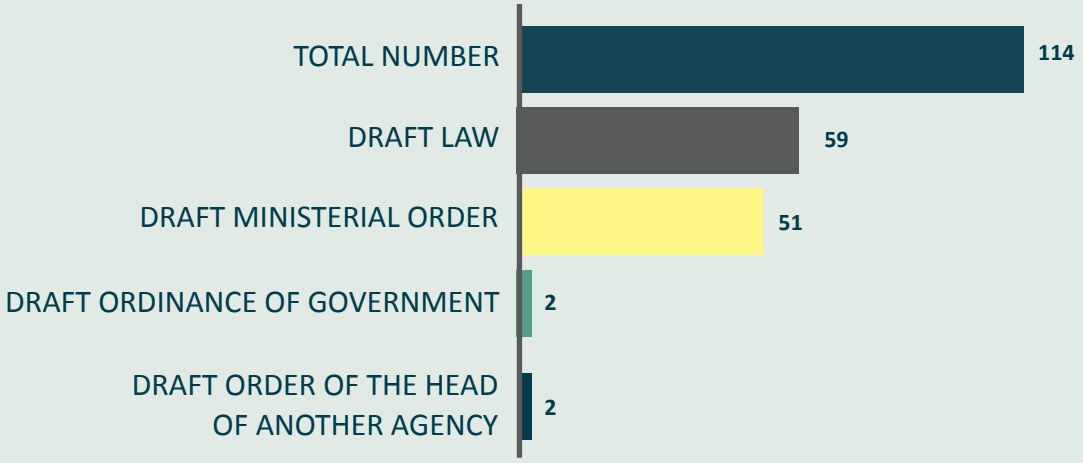
13

Within the framework of the expertise, the Service reviews the submitted draft international agreement, as well as the legislative and institutional mechanisms for the protection of personal data in the state party to the agreement, on the basis of which a recommendation for amendments to the draft agreement may be issued.

During the reporting period, the Service conducted an expertise of 13 draft international agreements, issuing a recommendation in 4 cases.

In 2023, the Service conducted a legal expertise of 12 draft international agreements and agreements to be concluded on behalf of Georgia, without issuing any recommendations.

TYPES OF ACTS ON WHICH THE SERVICE CONDUCTED LEGAL EXPERTISE

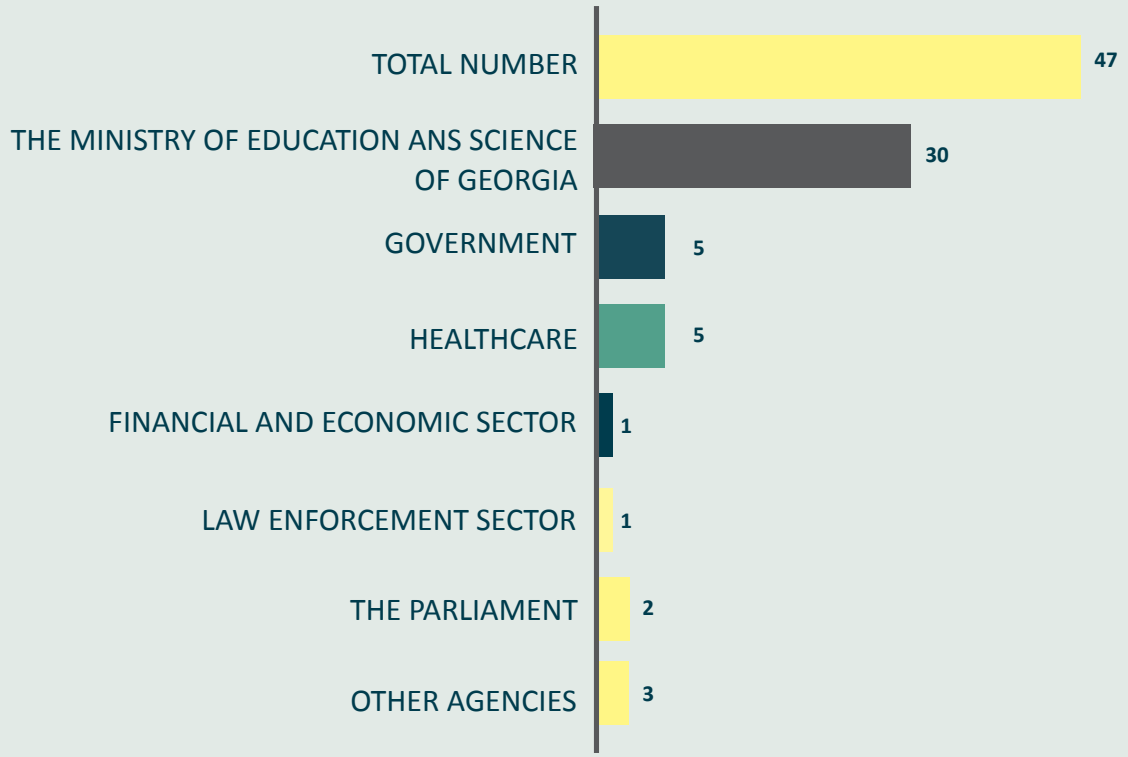


In order to ensure a high standard of personal data protection, the Personal Data Protection Service conducts legal expertise of draft legislative and subordinate acts upon the request of other agencies.

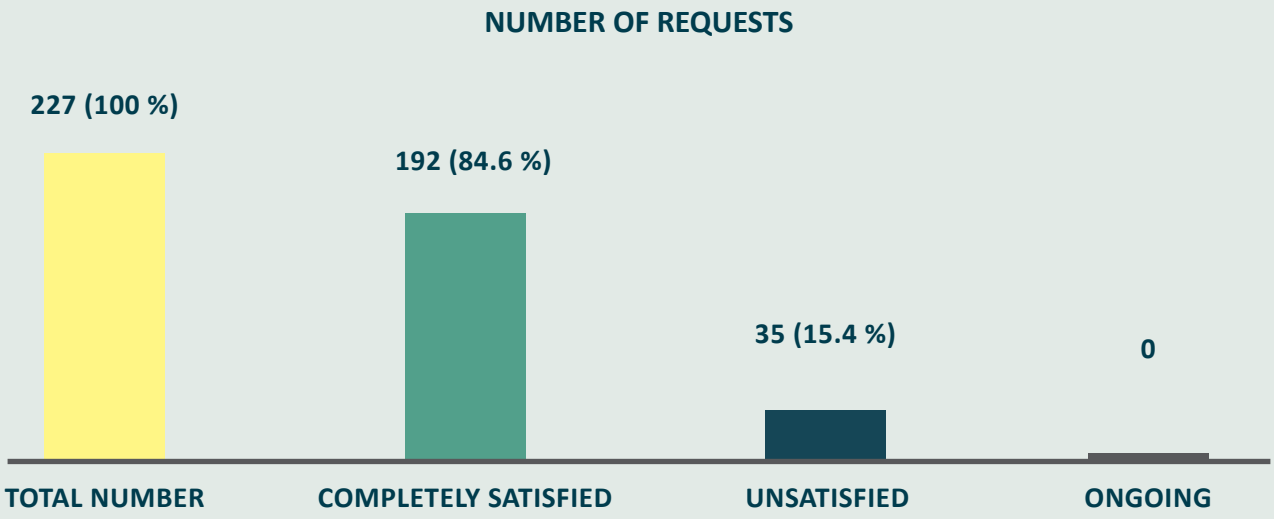
In 2024, the Service assessed the compliance of 59 draft laws, 51 draft ministerial orders, 2 draft government resolutions, and 2 draft orders issued by the heads of other agencies with the Law of Georgia "On Personal Data Protection".

In 2023, the Service assessed the compliance of 141 draft laws, 21 draft ministerial orders, 5 draft government resolutions, and 3 draft orders issued by the heads of other agencies 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



Between December 11, 2023, and December 10, 2024, a total of 227 requests for public information were submitted to the Personal Data Protection Service. Of these, 192 requests were fully approved, while 35 requests were not granted for the following reasons:

- In 15 cases, the requests were not submitted in the prescribed form, resulting in procedural deficiencies that were not rectified by the applicants. Consequently, these requests were not considered. In each case, the applicant received a reasoned response, including an explanation of the applicable appeal procedure.

- In 20 cases, the requested information was not held by the Personal Data Protection Service.

The review and processing of all requests submitted during the reporting period have been completed in full.

COMPLAINTS CONSIDERED BY THE SERVICE CONCERNING DECISIONS TO LEAVE AN APPLICATION/NOTIFICATION UNCONSIDERED OR TO TERMINATE INITIATED PROCEEDINGS

15

„According to the Order No. 34 of the President of the Personal Data Protection Service of March 1, 2024 "On Approval of the Procedure for Examining the Lawfulness of Personal Data Processing", individual legal acts of the structural unit of the Service may be appealed in the Service or in court. During the reporting period, 15 decisions made by the head of the structural unit on leaving the application/notification without consideration/terminating the initiated proceedings were appealed in the Service.

In 2023, 20 decisions of the head of the structural unit were appealed in the Service.

LAW-MAKING ACTIVITY

16

In 2024, the Personal Data Protection Service developed 16 by-laws to support its activities. In 2023, the Service developed 11 by-laws.

ANNEX №3: 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 ANDTHE YEAR OF MANUFACTURING:

№	Name of the Vehicle	The Year of Manufacture
1	KIAOPTIMA; LG917GL	2014
2	HONDACRV; 00781GG	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

In 2024, state procurement amounted to 1,508,437 GEL, including 1,448,952 GEL allocated for the full functioning of the service, and 59,485 GEL for representational expenses.

Notably, in 2023, the total amount of state procurement was 1,102,500 GEL, of which 1,042,182 GEL was used for the full functioning of the service, and 60,318 GEL was allocated for representational expenses.

7, Vachnadze Str. 0105, Tbilisi, Georgia
48, Baku Str. 6010, Batumi, Georgia

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