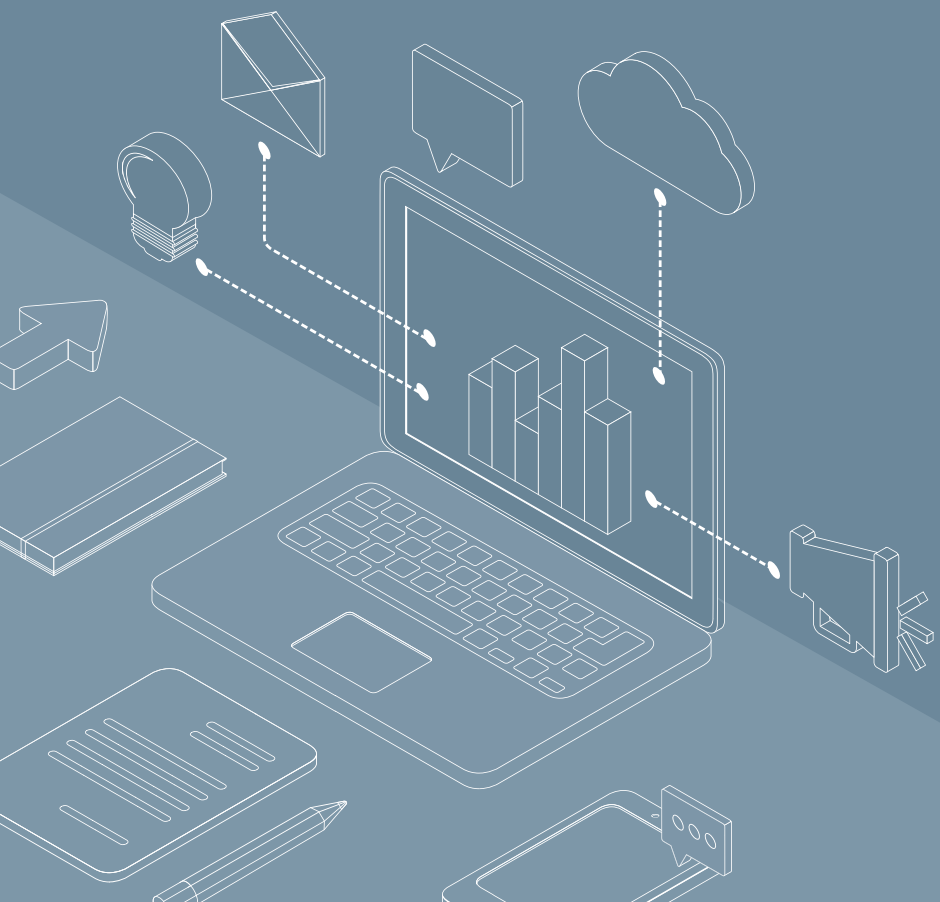
OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

STATE OF PERSONAL DATA PROTECTION IN GEORGIA

2014 REPORT



personaldata.ge

CONTENTS

Introduction 3

2014 Highlights 4

Legitimacy of Personal Data processing 7

Processing of the Personal Data by the Law Enforcement Agencies 16

Video Surveillance 19

Trans-Border Data Flows 23

Direct Marketing 27

Public Awareness and Education of Data Controllers 29

2014 Facts and Figures 31

INTRODUCTION

2014 Report of the Personal Data Protection Inspector comprises results of the applications submitted by the citizens, inspections and the consultations conducted from January to December 2014. The aim of this document is to analyse the overall situation and state of play regarding the personal data protection, as well as existing trends and challenges in this respect.

The Report reflects the issues related to the right to privacy that were the topic of the broad public discussions during last year, as well as the specific cases regarding the violation of the personal data protection legislation and responsive measures commenced by the Office, also steps undertaken by the various organisations towards implementing European data protection standards and activities of the Inspector's Office.

The Report reveals the systematic problems in relation to the data protection in a generalized way and while discussing them reference to the identity of particular organisations is minimized. In addition, applicants (data subjects) are completely anonymized.

The Report provides for such important issues as the legitimacy of data processing, processing of the data through emerging electronic technologies, processing of the personal data by the law enforcement agencies, video surveillance, and transfer of personal data to other states and/or international organisations, direct marketing, public awareness and education of the data controllers.

2014 HIGHLIGHTS

2014 was crucial in terms of data protection state policy development and its implementation, as well as for the Office of the Personal Data Protection Inspector itself as simultaneously an intensive work was carried out on amending the legislation, institutional and functional strengthening of the Office, public awareness raising and increasing the responsibility of the data controllers. The Office of the Inspector actively participated in all the important initiatives carried out to ensure the high standards of privacy and personal data protection in the country.

Positive changes and major achievements in 2014 relate not only to the qualitative and quantitative growth of the Office of the Inspector, but also to the transformation of public attitude towards the privacy related issues and the efforts made by the public and private organisations in order to implement the high standards of the data protection.

MOST IMPORTANT ACHIEVEMENTS OF 2014 ARE THE FOLLOWING:

- Two staged monitoring system over the covert investigative activities conducted by the law enforcement agencies has been established at the legislative level and currently is being implemented on the technical level.
- From November 1, 2014 the Law on Personal Data Protection became fully applicable to private sector including the supervisory powers of the Inspector (instead of January 2016 as envisaged in the previous version of the Law).
- More tangible guarantees of impartiality and independence of the Inspector were established, the level of accountability of the Inspector towards the Parliament has increased and the procedure for the election of the Inspector has been amended.

- Statutory legislation regarding direct marketing has been enhanced and all data controllers exercising direct marketing became legally obliged to create easily accessible and adequate opt-out mechanisms. From November 1, 2014 citizens actively use the new opt-out functions to reject advertising messages, while the Office of the Inspector reacts on the violations revealed.
- As a result of close cooperation between the Office of the Inspector and the data controllers the process of data processing has improved and brought in compliance with the legal requirements. The most vivid examples include placement of video surveillance warning signs, altering the photographing practice at the border check-points, limiting access to certain databases, improving the form of consent expressed by the individuals in banking and financial sectors.
- The degree of the enforcement of the Law of Georgia on Personal Data Protection and the applications of responsive measures to the violations has increased significantly. In case of an administrative offence, the Office of the Inspector applies fines and issues other binding instructions regarding terminate the future processing of the data or alteration of the processes.
- The recognisability of the Office of the Inspector and the number of consultation request from public and private organisations has increased, which in general is an indicator for the increase of public awareness.
- The Office of the Inspector is actively involved in the visa dialogue process with European Union and implementation of the Visa Liberalization Action Plan, as well as in process of implementation of the Association Agreement and Association Agenda. The EU assessment mission positively assessed the steps undertaken in Georgia for establishing data protection system in the country.

- Bilateral cooperation between the Office of the Inspector and data protection supervisory authorities of European states has been strengthened. The Office of the Inspector became a member of the Central and Eastern European Data Protection Authorities (CEEDPA) and the European Conference of Personal Data Protection Authorities (Spring Conference). The Office represents Georgia in the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) and the Bureau of the Committee. The Office has actively participated in the working group for updating the Convention N108 on personal data protection.

In order to ensure the efficient mechanisms for the protection of privacy and to establish European data protection standards efforts of all branches of government, Inspector's Office, public and private organisations and active engagement of the society is equally important.

LEGITIMACY OF PERSONAL DATA PROCESSING

The high standards of the personal data protection are determined by the legitimacy of data processing: compliance with processing principles and processing data for explicit defined purposes with respective legal basis. The consultations, meetings and inspections conducted in 2014 revealed that the processing of personal data, including sensitive data, by public or private organisations without respective legal basis still takes place. Often the data controllers are unable to identify relevant legal grounds or give improper interpretation to particular legal provisions. Violation of principles of data processing envisaged by the law still remains an issue, which includes disproportionate and inadequate processing of data and storage of such data for indefinite period of time.

Measures taken by the several ministries, public bodies and joint-stock companies to ensure the legitimacy of the data processing deserve positive assessment. These measures included not only adoption of the internal data protection policy documents, but also establishment of terms of storage and restriction of the access to data.

Unlawful disclosure and dissemination of the data can cause significant material and moral damage to individuals, especially when the information is disseminated via internet and its subsequent management and restriction is quite difficult. The vast majority of the complaints submitted by the individuals in 2014 concerned the disclosure/dissemination of the personal data without legal basis as a result of which three public agencies were imposed fines as an administrative sanction.

One of the applications submitted to the Office of the Inspector concerned the materials of criminal prosecution placed on the official web-page of the Chief Prosecutor's Office of Georgia, which included the medical diagnosis of a family member of the defendant.

In light of the inspection it was determined that the dissemination of a sensitive data took place without the legal basis envisaged in the law and the Chief Prosecutor's Office was fined with 1000 GEL in compliance with the Law of Georgia on Personal Data Protection. The Chief Prosecutor's Office appealed the decision of the Inspector in the Court. However, the Tbilisi City Court rejected the application and confirmed the fact of the administrative offence committed by the Prosecutor's Office. In addition, the Court did not support appellant's statement that the Law on Personal Data Protection did not apply to the processing and dissemination of the information for the purposes of investigation. In the given case, the Chief Prosecutor's Office exceeded the purposes provided in the Criminal Procedure Code and other normative acts regulating investigation of a crime and accordingly Law on Personal Data Protection applied to the disclosing the diagnosis for the purposes of informing public.

Violation of principles of data processing envisaged by the law still remains an issue, which includes disproportionate and inadequate processing of data and storage of such data for indefinite period of time.

In the reporting period, the Ministry of Corrections has been fined for illegal disclosure of the sensitive data. The Ministry for the purposes of informing public in order to dispel the doubts associated with the death of one of the inmates published on the web-page the name and last name, information on medical treatment administered to the inmate before death, medical diagnosis and provided medical service. The inspection found that accessibility of sensitive data without the written consent of the data subject (or statutory heirs) breached Article 6.3 of the Law of Georgia on Personal Data Protection, according to which regardless the existence of respective legal basis for data processing, it is prohibited to disclose sensitive data without the consent of the

data subject. In accordance with the Law the Ministry was imposed a fine of 1000 GEL as an administrative sanction.

In 2014, the Office of the Inspector examined the fact of disclosing the personal data of a data subject by the patrol police to a third party without the basis envisaged in the law. This was a complaint based inspection. The identity and phone number of the data subject who notified the misdemeanour on "112" hotline, was revealed to the offender from the internal protocol drawn up by the patrol crew. For negligent disclosure of personal data without the legal grounds, the Ministry of Internal Affairs was imposed a fine of 500 GEL as an administrative penalty.

Unlawful disclosure and dissemination of the data can cause significant material and moral damage to individuals, especially when the information is disseminated via internet and its subsequent management and restriction is quite difficult.

During the reporting period number of citizens addressed the Office of the Inspector with the question about the lawfulness of the accessibility of citizens' personal data on the web-pages of National Agency of Public Registry (NAPR) and Central Election Commission of Georgia. Access to personal identification number and address in the business and property registry of NAPR was of particular discomfort for citizens, together with the possibility of obtaining the photo and the information about other persons registered at the same address.

The Office of the Inspector examined the lawfulness of disclosing personal data on the web-pages by the National Agency of Public Registry and the Central Election Commission. It has been found that through the web-page of the Central Election Commission, it is possible to access the information containing personal data (including photo) in case of correct indication of two categories of data at the same

time (identification number and the last name), while photos of other persons registered at the same address are not accessible.

As for the National Agency of Public Registry, the Law on Public Registry requires making data and documents related to business and property registration available to any person.

Under the Law of Georgia on Personal Data Protection the processing of data, including disclosure is permitted if the processing is envisaged by the law, as well as if it's necessary for compliance with a legal obligation to which the data controller is subject to. Accordingly, availability of the abovementioned data on the web-page has the respective legal basis and legitimate purpose, namely, in case of Central Election Commission this is directly envisaged in the Election Code and posting the data on the official web-page of the Central Election Commission serves the purpose of forming the unified list of voters and elimination of possible inaccuracies. Disclosure of data by the National Agency of Public Registry is envisaged in the Law of Georgia on Public Registry and serves the purpose of performing duties imposed on the Agency by the legislation.

Practice proves that the collection of high volume of irrelevant data by employers causes problems to citizens.

Practice proves that the collection of high volume of irrelevant data by employers causes problems to citizens. Apart from particular consultations provided to employers, the Office of the Inspector prepared and disseminated the 13-page document on personal data protection in labour relations aiming to eliminate improper interpretation of the law, protecting the rights of employees and raising public awareness of the employers. Recommendations elaborated by the Inspector are based the Georgian legislation, Recommendations of the Committee of Ministers and the International Labour Organisation, case law of the European Court of Human Rights and the best practice of the European countries.

ERASURE OF THE PERSONAL DATA FROM INTERNET SEARCH ENGINES

In the reporting period a citizen submitted an application to the Office of the Inspector, indicating that accessibility of the information about his detention in 2007 on the mass media web-page and electronic catalogue of the National Parliamentary Library of Georgia breached his constitutionally guaranteed rights and had a negative impact on his professional reputation.

In the framework of the given case the Inspector examined the legality and proportionality of the processing of data of the data subject by the National Parliamentary Library of Georgia. It has been found that the National Library had the respective legal basis for the processing of data. In assessing the proportionality, the impact of availability such data on the individual's privacy, inflicted or possible harm and the balance between the right to privacy and the public interest were taken into account. Considering that operation of catalogue by the Library without reference to a particular person's name and last name in the search parameters was possible, the National Parliamentary Library of Georgia has been instructed to limit the access to information on the affiliation of the data subject to the crime in the search engines with name and last name parameters.

Since the Law on Personal Data Protection (except for Article 17) does not apply to the processing of data by mass media for public interest, the Personal Data Protection Inspector lacked legal opportunity to oblige mass media organisations to conduct particular activity. Despite this, on the basis of the letter of the Inspector, the media holding took into consideration the interest of the citizen and limited access to the information being sensitive to the data subject.

CONSENT AS THE LEGAL BASIS FOR THE DATA PROCESSING

In practice, the most commonly used legal basis for the processing the personal data is the consent of the data subject.

The Law of Georgia on Personal Data Protection determines the consent of a data subject as one of the legal grounds for the processing of data and establishes that consent can be expressed after receiving appropriate information on the processing of data for established purpose. It can be expressed on oral or written form, as well as through telecommunication or other relevant means.

Practice revealed that unfortunately consent expressed through signature of contracts or other types of documents has a formal nature. Often a citizen has to sign the document expressing consent without receiving any information or explanation thereon. The citizen is unaware of what type of data is used for which purpose, whether the withdrawal is possible and what legal consequences this might entail.

In 2014 the Office of the Inspector provided consultations to several organisations regarding the form of the consent. At the same time, the interest of citizens on these issues increased as well. Number of citizens applied to the Office of the Inspector with a question whether it is possible to withdraw the written consent and request termination of data processing. In addition, within the framework of the inspection of Public Service Development Agency, based on the random selection 3 851 facts of data processing with the consent of the data subject by 20 commercial banks and 6 other organisations were examined. Cases were revealed in which the organisation was given the authority to process the disproportionately high volume of data under written consent. As a result of the inspection the text of consent has become more clear and informative and the purpose of the processing of data was specified.

PROCESSING OF PERSONAL DATA THROUGH INFORMATION TECHNOLOGIES

In 2014 selling of electronic databases containing personal data of data subjects became more frequent. For example, under one of these offers, the cost of name, last name, date of birth, phone number and address of 1 400 000 individuals was 100 GEL, while the cost of email addresses of 120 000 individuals was 70 GEL.

Throughout the year the Office of the Inspector was identifying the owners of databases and examining the legality of data processing. Often these databases were formed on the basis of data illegally disclosed in the previous years. As a result of the intervention by the Office of the Inspector 7 organisations terminated the processing of data. Apart from this, with public statement the Inspector called upon all the potential buyers of the databases to verify the legality of obtaining/collecting the data and ensure the protection of individual's rights.

In the process of automatic processing of data one of the problems still is the disproportionality and lack of legitimacy of exchanging data between different organisations and access to databases. Therefore, in 2014 the Inspector with its own initiative started to inspect the largest public sector data processors.

In the consultations and legal expertise format the Office of the Inspector closely cooperated with the LEPL Social Service Agency – one of the largest data controllers in public sector.

Consultations concerned the following issues:

a) Providing information to the LEPL Public Service Development Agency to create the unified list of voters with the purpose of biometric registration of population;

b) Access of the LEPL Public Service Development Agency to the data of persons registered in the unified database of socially vulnerable families with the purpose of distributing benefits in the process of issuing electronic ID cards;

c) Access of the LEPL National Bureau of Enforcement to the database of recipients of state benefits (state pension, social package, and state compensation) with the purpose of distributing benefits.

To comply with international election standards and create accessible electoral environment for persons with disabilities, the Office of the Inspector found it relevant to provide information about persons with disabilities (using wheelchair, hearing impairments and blind) to the Central Election Commission in depersonalized form. It was assessed to be against legally defined principles to transfer the information about socially unprotected families to one of the communications companies and therefore the transmission of data was not conducted.

The Office of the Personal Data Protection Inspector together with the Administration of the Government of Georgia participated in the discussion of the issue of access to the Public Service Development Agency database by Ltd Georgian Post and L. Samkharauli National Forensics Bureau. Based on examination of respective legislative framework, the legitimate purpose which would necessitate the access to the data in a requested form was not identified. The Government of Georgia shared the views of the Inspector when taking the final decision on the issue.

INSPECTION OF THE LEPL PUBLIC SERVICE DEVELOPMENT AGENCY

In 2014 the issue of access of other organisations to the databases of the LEPL Public Service Development Agency was examined.

During the inspection it was revealed, that the information from electronic identity card program was transmitted to 73 different public institutions and private organisations, as well as to individuals on the basis of an individual request and to certain bodies to fulfil the authorities delegated by the Agency.

In the framework of the inspection it was revealed that the data was transmitted to several organisations without identifying the legal basis (often contracts/memorandums concluded between the Agency and other organisations did not include the reference to legal basis and the Agency did not possess the verified information which legal obligation necessitated receiving information from the database) and the need for receiving the data was not substantiated.

With the decision of the Inspector the Agency was instructed to take specific measures to eliminate the violations and deficiencies, as a result of which the legal grounds and purposes of transferring the data were specified, amendments were made in contracts concluded with certain organisations and access of the Administration of the Government of Georgia, the Ministry of Economy and Sustainable Development of Georgia, the LEPL Academy of the Ministry of Finance of Georgia and the Office of the Minister of Autonomous Republic of Abkhazia on Regional Governance to the database was terminated.

PROCESSING OF PERSONAL DATA BY LAW ENFORCEMENT AGENCIES

In 2014 the issue of covert surveillance was subject to specific public interest and debate. The authority of investigative and operative bodies to interfere into the private life of a person with the purpose of crime investigation or prevention or for the state security interest is an internationally recognized standard. However, this authority shall be strictly regulated and limited. Interference into the private life shall be proportionate to legitimate purpose pursued.

National legislation and practice must create adequate safeguards against the misuse of power or arbitrariness from the side of authorities. *"Article 8 of the European Convention on Human Rights (ECHR) provides for the right to private life. Interception of communication is not necessarily incompatible with that right; but it must be carried out consistently with the requirements both of the ECHR and the Council of Europe Data Protection Convention."*[1]

It is also worth of mentioning that the debate in Georgia on the access of personal data by the law enforcement bodies somehow echoed the worldwide processes, the accelerator of which was revealing the facts of large scale interception of their own citizens and citizens of other countries by security services of various countries. The current processes in the European countries is just one of the examples of the fact that violation of the right to privacy by law enforcement agencies even for the purposes of the crime investigation or the state security is still a matter of debate and reform.

One of the important events of 2014 was the decision of the European Court of Justice of April 8, 2014, in which it repealed the Directive of the European Parliament and European Council 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive). As a result of this Decision many European countries started amending not only the national legislation, but adapting the principles of international cooperation and practice to the new reality.

[1] Report of the Council of Europe experts Joseph A. CANNATACI and Graham SUTTON, Key Points Regarding Access to Personal Data by Law Enforcement and by National Security Agencies, September 2014

The Office of the Personal Data Protection Inspector, along with the Parliament of Georgia, the Government and civil society was actively involved in establishing higher standards of personal data protection in the law enforcement agencies and the work in this respect is still in progress. Clear examples for that are amendments to the laws of Georgia on Personal Data Protection, on Electronic Communications, Criminal Procedure Code of Georgia and other normative acts adopted in August and November of 2014 and related discussions.

The following legislative amendments carried out in 2014 are the most significant in terms of the work of the Inspector and its mandate:

- The concept of covert surveillance activities was created which is now subjected to higher guarantees of criminal procedure instead of operative-investigative activities and is now qualified as state secret.
- Prior control by the Inspector for the processing of data during covert surveillance activities was established. Namely, before intercepting and recording telephone conversation by the Operative-Technical Department of the Ministry of Internal Affairs of Georgia, the Inspector checks whether there is a court order/prosecutor's decision and whether the data indicated in it is in compliance with the request initiated by the Operative-Technical Department. After this, the Lawful Interception Management System is given the permission to open the requested channel and conduct interception only in case of full compliance of data. At the same time, a specific phone number is accessed by the period and to the extent which is envisaged in the court order or prosecutor's decision. Accordingly, in case of inconsistency of data the interception will not be conducted and in case of expiration of the defined period it will be terminated (will enter into force from 31 March 2015).
- The subsequent control mechanism of the Inspector was defined, which includes special electronic control system for data banks (controlling the use of already collected data), supervision of the process of destruction of collected personal data and the authority to examine the legality of the processing of personal data in the framework of interception or other investigative activities.

Despite the fact that the system of controlling legality of covert investigative activities does not provide the absolute safeguard for complete elimination of illegal surveillance (it is impossible to exclude the

possibility of direct or indirect access to communication infrastructure though illegal means), external control of the legality of covert investigative activities is a significant step forward and its successful operation will promote the implementation of further higher standards in this respect. It is logical to expect that in the process of political and legal approximation with Europe, relevant discussions and the search for efficient solutions will continue.

The Office of the Inspector examines the issues of the data processing by law enforcement agencies not only in the context of covert investigative activities. Law enforcement agencies process high volume of personal data in the process of discharging other functions under the law. While in 2013 the main task was to establish the correct grounds and procedures for collection and processing of personal data during criminal investigation and operative-search activities, the major challenge in 2014 was proportionality of data processing and its adequacy to the legitimate purpose pursued. *Article 4 of the Law of Georgia on Personal Data Protection defines that "data shall be processed only for explicitly specified legitimate purposes. It is prohibited to further process the data for other purposes inconsistent with initial purpose. Data shall be processed only to the extent necessary to achieve respective legitimate purposes. Data shall be adequate and not excessive in relation to the purposes for which they are processed."*

The major challenge in 2014 was proportionality of data processing and its adequacy to the legitimate purpose pursued.

During the reporting period the Office of the Inspector, on the basis of the citizens' complaints, conducted the inspection (examination) of several units of the Ministry of Internal Affairs, which included the processing of data in labour relations, examination of the legality of the processing of data about the citizens in the databases of the Ministry and the access to the data collected at border cross check points. As a result of the inspection the Ministry of Interior was instructed to eliminate the discrepancies revealed. The fulfilment of the instructions issued is currently under monitoring stage.

VIDEO SURVEILLANCE

Usage of video surveillance systems becomes more and more common and citizens are increasingly interested in the issues related to the legitimacy of such systems and their accessibility.

During the reporting period number of cases was identified where video surveillance system was not used for the purposes provided for by the law such as security, property and secret information, as well as the protection of minors from harmful influence. The terms of storage of recordings obtained as a result of video surveillance were not adequate and proportionate, access to the video recordings and security regulations thereto were not established.

Often public and private organisations, beyond the monitoring of the outdoor perimeter and entrance of the buildings, used video surveillance systems for the purposes of controlling employees at the work place without any justification.

Often public and private organisations, beyond the monitoring of the outdoor perimeter and entrance of the buildings, used video surveillance systems for the purposes of controlling employees at the work place without any justification, while, under the law, installation of video surveillance system at the work place is only allowed in exceptional cases and if it is impossible to achieve the legitimate purpose pursued by other means. Furthermore, the majority of employees are not informed in writing on the ongoing video surveillance and their rights.

As a result of the consultation provided, certain organisations ceased usage of data obtained through video surveillance system for the purposes of recording employees' entrees and exits from the office buildings and imposing disciplinary sanctions and notified them in writing on the ongoing video control.

One of the trade unions informed the Office of the Inspector on the photographing and audio-video surveillance system which was planned to be used for the employees control purposes. The Office addressed the organisation and asked to provide relevant justification that eventually resulted in suspended the planned activities and further consultations related to this case are currently ongoing.

The Office of the Inspector was notified that some pharmacy networks, for the purpose of the service improvement, in addition to video surveillance conduct the audio recording of conversations between customers and service personnel. Due to the fact that during the communication between customers and personnel information concerning the state of health is shared, the audio recording of such communication poses the risk of disproportionate and inadequate interference into the private life of individuals, especially when the customers are not informed on the audio recording. The Inspector requested information from pharmacies and the detailed examination of the issue is in progress.

The practice has proved the necessity of legal regulation of video surveillance in public transportation means and other public places. Legislative amendments adopted by the Parliament on August 1, 2013 eliminated the gap in the legislation.

During the reporting period several cases were revealed when video recordings from the private organisations was requested by law enforcement agencies without any proper justification and reference to the relevant legal ground (decision of investigator/prosecutor or court). The consultations have been provided to the specific organisations involved.

The practice has proved the necessity of legal regulation of video surveillance in public transportation means and other public places. Based on this needs and the best practice of the European countries the Office of Personal Data Protection Inspector developed a legislative proposal on the regulations of video surveillance in the streets, public and private organisations and residential buildings.

Legislative amendments adopted by the Parliament on August 1, 2013 eliminated the gap in the legislation. Video surveillance in parks, gardens, playgrounds, public transportation means and at the bus

stops, as well as in other public places fell within the ambit of the Data Protection Law and the obligation to place visible warning signs was established.

Given the relevance and acute character of the issue, the Office of the Inspector prepared and disseminated the recommendations[2] on the video surveillance, which aim to prevent the improper interpretations of the law and inform organisations on the principles of video surveillance, data security and respective warning signs.

RESULTS OF THE INSPECTION OF THE MINISTRY OF CORRECTIONS

revealed that in the penitentiary institutions there were no warning signs on video/audio control placed and visitors were verbally informed about video monitoring.

Considering the recommendations of the Inspector, the Penitentiary Department launched fundamental reforms in this direction. As a result of infrastructural and procedural changes the rules related to the notification of defendants/convicts, processing and storage of the video recordings were improved; the period for which data was kept was reduced. Within the framework of updated internal informational security policy the issue of access to the materials and data security was regulated.

Visible warning signs on video/audio control were placed. On the basis of the Inspector's recommendations, relevant amendments were made to the Imprisonment Code in order to ensure the compliance of the control over the defendant/convicts through electronic means with the personal data protection legislation.[3]

---

[2] *http://personaldata.ge/res/docs/recommendation/video%20surviellance-recommendation-final.pdf*

[3] *Law of 16 April 2014 №2241-IIს on the Amendments in the Imprisonment Code.*

METRO IN LIVE

During the reporting period the Office of the Inspector received information that live-streaming of video surveillance of Tbilisi Metro lobby, platform and surrounding streets was conducted through several web-pages and consequently was available to any interested person.

Examination revealed of the issue it was found that live-streaming of video surveillance of the Metro stations undoubtedly exceeded the legal margins provided for by the law. Even though video monitoring was conducted by a private company and at the time of examination the mandate of the Inspector did not apply to the private sector, considering the scale of video surveillance area and interests of thousands of citizens, the Office of the Inspector addressed the organisation and called on compliance with the legislation. As a result live-streaming was terminated.

PHOTOGRAPHING AND VIDEO CONTROL AT BORDER CHECK POINTS

In 2014 the Office of the Inspector on its own initiative examined the legitimacy of the processing of data by the Ministry of Internal Affairs of Georgia for the border control purposes. During the inspection it was revealed that while crossing the border all the passengers were photographed and the photos were reflected in the automated database. Photo was taken at each occasion of the border cross by default, even when there was no suspicion against the person and/or the database included the photo and its quality was appropriate for the identification purposes. In the process of inspection the Ministry started elaborating new standardized rules according to which photographing at the border check points will take place only in exceptional circumstances. Besides, visible warning signs on video surveillance were placed at borders and the term for storage of the data processed for border control purposes was defined.

TRANS BORDER DATA FLOWS

Due to the modern technologies very often data transfer and storage is not subject to the specific state frontiers and jurisdiction, the good example of this is the popularity of so called "cloud" technology. Sometimes there are difficulties related to identification of respective controller responsible for legitimacy of the processing and data security.

Numerous public and private institutions operating in Georgia transfer data aboard. Usually foreign shareholders and partners of private companies request personal information of employees or customers for the oversight and reporting purposes. As for the public institutions, they transfer data to foreign public agencies in the framework of mutual assistance and cooperation on the basis of international agreements.

Numerous public and private institutions operating in Georgia transfer data aboard.

Frequently public agencies are addressed with the request of submission of data from the countries without adequate level of data protection. The Office of the Inspector, upon the request of law enforcement agencies, analysed the legislation and practice of 17 states of Europe, Asia and Africa and found out that only 6 of them meet the required standards of data protection.

In addition, the Office of the Inspector examined the practice of different states, studied their personal data protection legislation, existence and functions of supervisory bodies, state of protection of human right and freedoms and the opportunities of data subjects to protect their rights. On the basis of this analysis, the Order N1 of the Personal Data Protection inspector of 16 September 2014 was issued providing the list of countries having adequate level of data protection. Accordingly, starting from September 16, 2014 public and private organisations operating under Georgian jurisdiction, in case of existence of legal grounds for data processing, are allowed to transfer data to individuals and legal entities in 47 countries without special permission. So called "white list" created the legal basis for many occasions of trans-border data flows and significantly simplified the process for public and private organisations in Georgia.

During the reporting period the Office of the Inspector became aware that financial institutions operating in Georgia planned to transfer the personal data to the competent authorities of the United States in accordance with the Foreign Account Tax Compliance Act (FATCA). Examination of the issue revealed that under the acting legislation, financial institutions neither had the legal basis for collection of this type of data and nor any of the international treaties/agreements envisaged such transfers. The Office of the Inspector issued recommendations to the financial institutions, to the National Bank of Georgia and to the Ministry of Finance of Georgia (as the body involved in the negotiations on this matter). As a result the Ministry of Finance of Georgia communicated with the American party and the deadline for fulfilling the obligation of the processing of such data by financial institutions was postponed to the period of signature of relevant international treaty between the United States and Georgia.

Throughout 2014 the Office of the Inspector examined 17 trans-border data flow permission applications from commercial, banking and financial organisations. Permission was granted on the 13 of them.

The analysis of existing practice showed that it is important for private organisations to include provisions related to trans-border data flows and data security in the contracts concluded between the parties, while public agencies shall conclude relevant international agreements with countries where adequate level of data protection is not ensured.

DIRECT MARKETING

During 2014 significant proportion of citizens' complaints, consultations and recommendations related to the direct marketing. It was not clear for the citizens how their phone numbers or emails became available to private companies. It was practically impossible to request the termination of the data processing, especially when there were difficulties related to identifying advertising companies. The existing legal regulations were not ensuring sufficient guarantees for the protection of citizens' rights.

The processing of any type of data for the purposes of direct marketing became possible only on the basis of the written consent of the data subject

The Office of the Personal Data Protection Inspector prepared the draft amendments that were adopted by the Parliament on August 1, 2014. According to the amendments, the processing of any type of data for the purposes of direct marketing became possible only on the basis of the written consent of the data subject and the legal possibility for the processing of disproportionately large amount of data without the informed consent is excluded.

In addition, the opt out mechanism was simplified and citizens were given the opportunity to request termination of the usage of their data at any time, while organisations conducting direct marketing became obliged to ensure existence of easily accessible opt-out mechanism.

The Office of the Inspector on the same day when the law fully applied to the private sector[4] received the citizens' applications and started the inspection of the companies regarding the fulfilment of their obligations (e.g. "sms off'' function, USSD code).

[4] *The Law on Personal Data Protection became fully effective for the private sector since 1 November, 2014.*

In November-December 2014 inspection of 6 companies was conducted. The sources of data, proportionality of the processing and efficiency of the opt-out mechanisms were inspected. Information was requested not only from marketing companies, but also from data processors who were sending the marketing messages on behalf of the controllers.

Once receiving citizens' applicationps the Inspector, in all the 6 cases, used the data blocking mechanism and with the final decision obliged the organisations to stop the usage of data of the applicants, to take organisational and technical measures for ensuring data security and to implement efficient opt-out mechanisms.

Notwithstanding the fact that obligation to provide easily accessible opt-out mechanisms exist only for several months, according to the information of one of the advertising companies, rejection mean (USSD code) was used by 113 000 subscribers, part of whom requested the complete opt-out from of all forms of advertising messages, while the other part chose the product/service segmentation principle.

Considering the number of companies conducting direct marketing and the interests of the citizens, the Office of the Inspector prepared specific recommendation for organisations and the information paper for citizens.

PUBLIC AWARENESS AND EDUCATION OF DATA CONTROLLERS

For implementing high standards of personal data protection in the county it is important to raise awareness of data controllers and citizens, especially considering the large scale of data processing and the risk of illegal, including criminal, usage of data.

Besides the consultations the Office of the Inspector regularly conducted information meetings with various data controllers whose daily activities are linked with the processing of personal data.

In 2014 the interest of citizens towards personal data protection increased significantly.

Meetings were held with mobile operators, internet service providers, banking and financial institutions and public agencies. The Office participated in the events organized by government, international and non-governmental organisations.

Within the framework of its activities in 2014 the Office of the Inspector provided trainings on personal data protection related issues for approximately 1300 public servants and over 100 representatives of private organisations. The Office of the Inspector cooperated with the Training Centre of Justice, Police Academy of the Ministry of Internal Affairs, Training Centre of the Ministry of Foreign Affairs, Academy of the Ministry of Finance, HR Guild and other organisations.

From October 2014, during 4 months, the Office of the Personal Data Protection Inspector conducted a course of trainings for 700 employees of Public Service Development Agency in Tbilisi, as well as in Kutaisi, Batumi, Gori, Telavi and other cities.

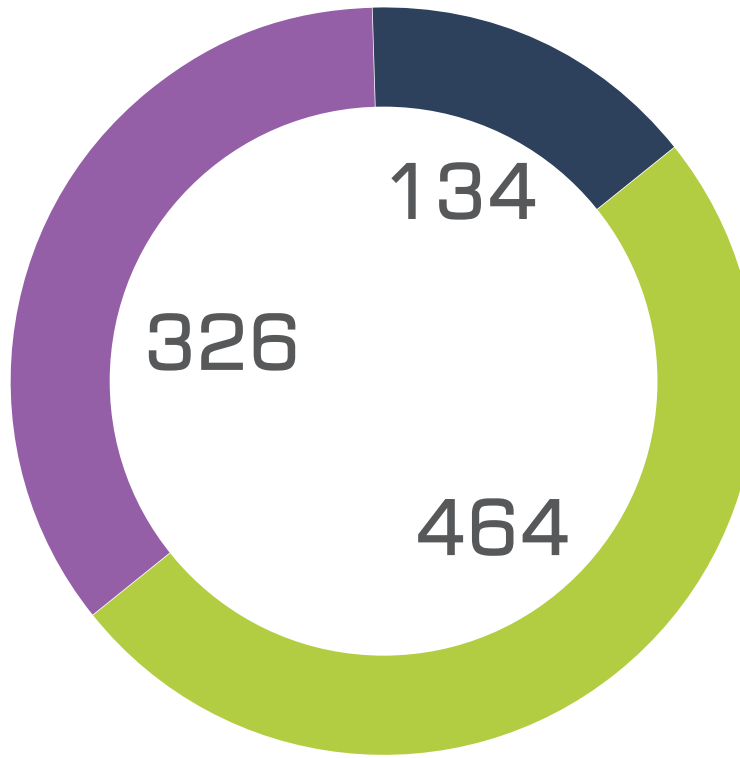
Two types of training modules adjusted to the activities of the Agency were prepared: 7 hour module for those who are directly involved in the formation of databases and providing services to citizens and 3 hour basic module for the Agency administration.

In 2014 the interest of citizens towards personal data protection increased significantly. More and more individuals are interested in their right to personal data protection. The Office of the Inspector prepared informational papers including bilingual ones on personal data protection during border-cross and on the rights of the data subjects. Guidelines were developed for citizens on the issues of direct marketing and safe usage of mobile applications. Information meetings were held in the regions and public lectures were conducted for students. In order to inform public on the work of the Office of the Inspector, its employees and the Inspector herself took part in various TV and radio programs.

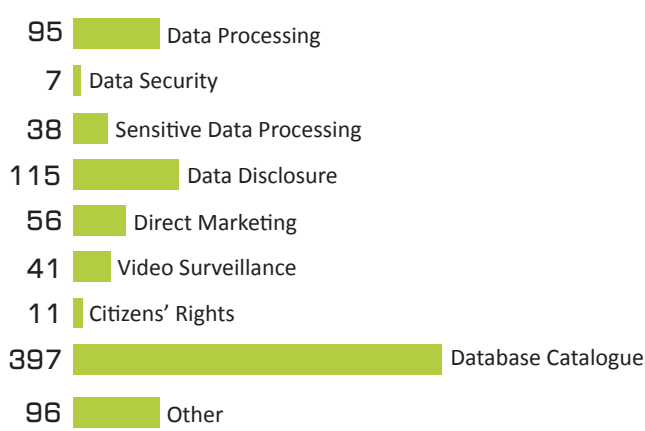
The web-page of the Office of the Inspector – www.personaldata.ge is operating since January 28, 2014. It brings together the information about ongoing activities of the Office, news, legislation, best practices and other interesting topics. During 2014 the web-page had more than 11 000 unique users. The number of users is increasing and its average daily number constitutes 150. The Office of the Inspector actively uses social networks to disseminate information and to provide consultations to citizens.

2014 FACTS AND FIGURES

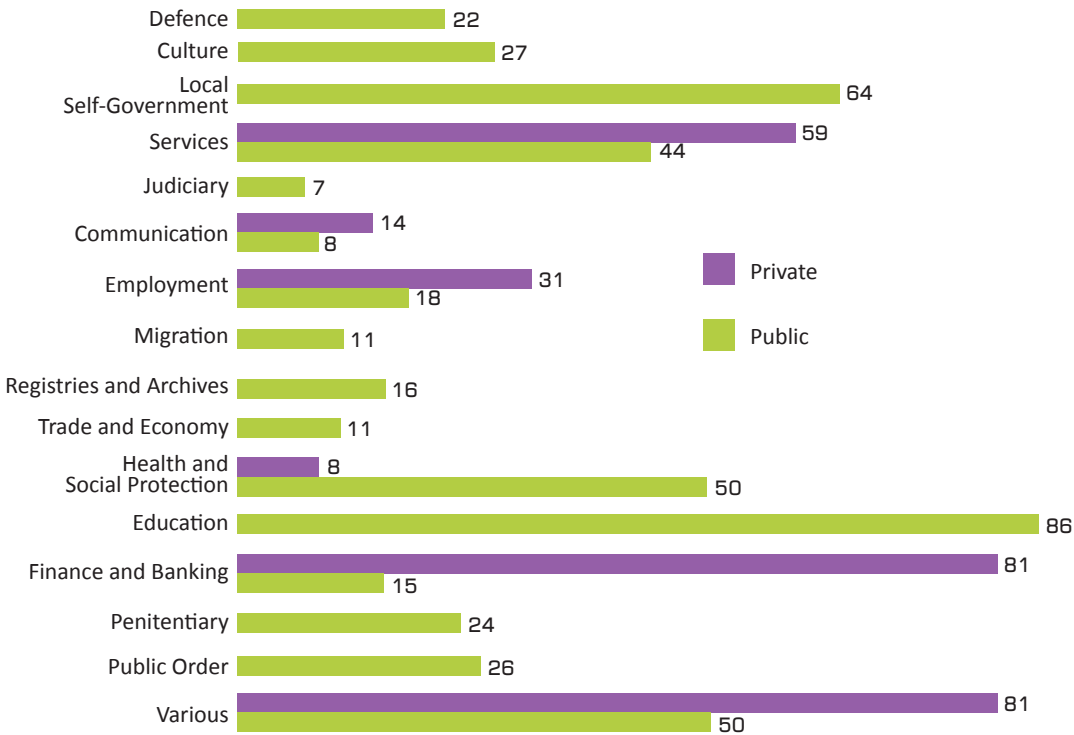
IN 2014 924 CONSULTATIONS WERE PROVIDED INCLUDING:



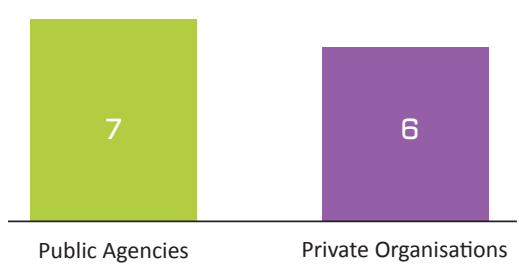
TOPICS OF CONSULTATIONS



CONSULTATIONS BY SECTORS

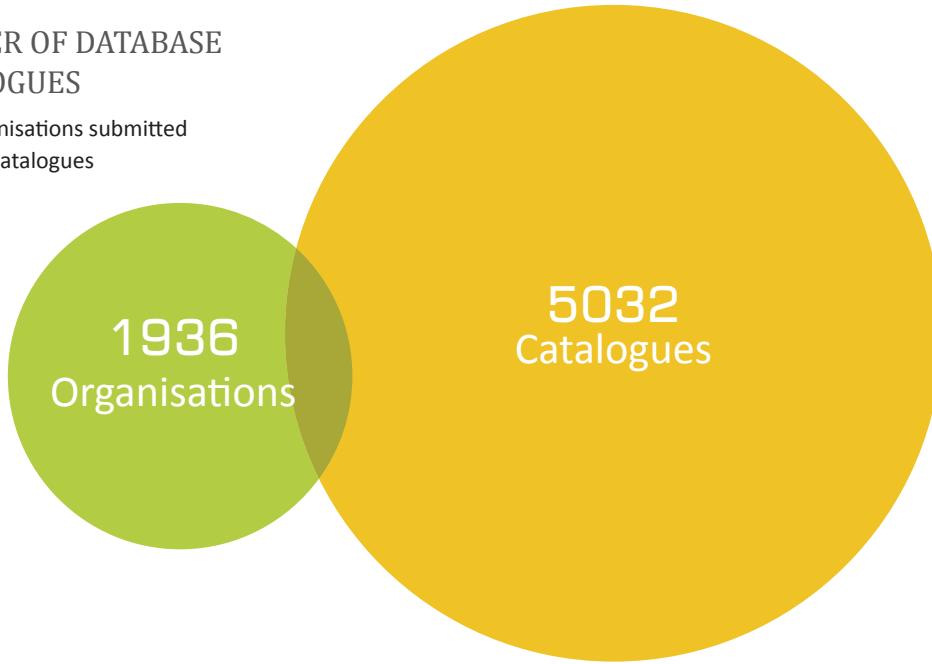


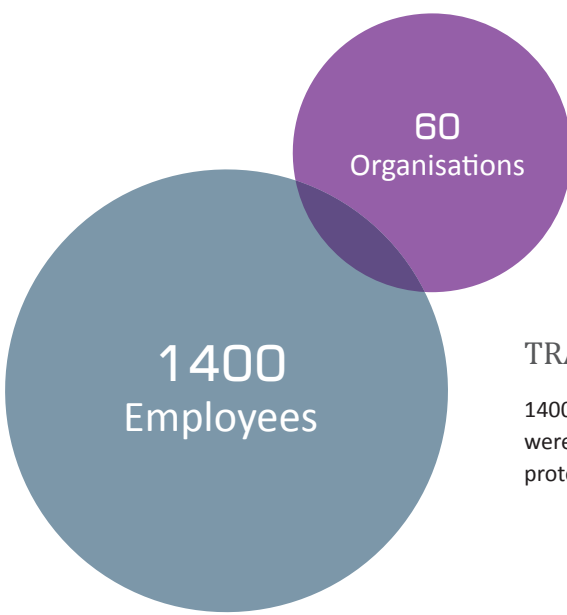
13 INSPECTIONS CONDUCTED



NUMBER OF DATABASE CATALOGUES

1936 Organisations submitted database catalogues





TRAININGS

1400 employees of 60 organisations were trained on personal data protection

OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

(+995 32) 242 1000
office@pdp.ge
www.personaldata.ge
FB/DPAGeorgiaOfficial