PERSONAL DATA PROTECTION INSPECTOR

REPORT
THE STATE OF PERSONAL DATA PROTECTION IN GEORGIA

3/1 / 2014

FOREWORD

It is a great responsibility to present the first report regarding the state of personal data protection in Georgia to the Government and to the public.

The document reflects the results of citizens' complaints, conducted inspections and provided consultations from August 2013 to March 2014. Even though 7 months are not enough for the comprehensive analysis based on empirical data and for detecting all the facts of data breaches, the report presents major challenges and systemic problems, namely: processing of disproportionately large amount of data without the legal grounds, illegal disclosure of personal information, failure to meet legal requirements related to video surveillance, neglecting the citizens' rights during direct marketing, etc.

Deep-rooted systemic problems can only be resolved after their identification and through holistic approach. Therefore, from the moment of appointment, I started formation of the office, studying data processing practices in the country, raising public awareness on the data protection issues, analyzing the legislation and the experience of other countries in collaboration with the representatives of Parliament, the Government and non-governmental organizations.

Principles prescribed in the Law of Georgia on Personal Data Protection and functions of the supervisory body are innovation not only for citizens, but also for the data processors. Therefore, considerable time of the office was devoted to consultations and trainings. During the last six months 376 consultations were provided on the legitimacy of data processing, basic training on data protection was conducted for 58 employees of the Ministry of Internal Affairs and 163 representatives of public and private organizations got acquainted with the data protection issues relevant to the labor relations. As a result of reacting on the 8 complaints of citizens and 2 inspections, measures such as restoring the violations in the indicated form and terms, limiting the access to databases, terminating the processing, erasure or destruction of data were implemented. Public statements were issued on direct marketing, processing of biometric data, video surveillance and unlawful disclosure of the sensitive personal data.

This is just a beginning of the complicated path. Great efforts are required from the public and private entities in order to build privacy-friendly system protecting human rights and freedoms. However, empowered citizens and their active engagement are crucial for the establishment of high standards of personal data protection in Georgia.

Tamar Kaldani
Personal Data Protection Inspector

CONTENTS

INTRODUCTION ---- 3

BASIC PRINCIPLES OF THE PROCESSING OF DATA ---- 4

LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA ---- 6

CONSENT AS THE BASIS FOR THE PROCESSING OF DATA ---- 6

PROCESSING OF DATA USING ELECTRONIC TECHNOLOGIES ---- 7

COLLECTION, STORAGE, DISCLOSURE AND OTHER TYPES OF PROCESSING OF DATA RELATING TO HEALTH, POLITICAL OPINIONS, CONVICTION AND OTHER SPECIAL CATEGORIES ---- 9

PROCESSING OF BIOMETRIC DATA ---- 11

CHALLENGES IN REGARD TO SECRET EAVESDROPPING AND WIRETAPPING ---- 12

PURPOSE AND LEGALITY OF VIDEO SURVEILLANCE ---- 15

TRANSFER OF PERSONAL DATA TO ANOTHER STATE AND/OR INTERNATIONAL ORGANIZATION ---- 18

DIRECT MARKETING ---- 19

CITIZEN AWARENESS AND PROTECTION OF RIGHTS ---- 20

RECOMMENDATIONS TO THE GOVERNMENT OF GEORGIA REGARDING THE MEASURES TO BE IMPLEMENTED FOR THE PROTECTION OF PERSONAL DATA ---- 22

INTRODUCTION

In modern democracies the protection of personal data is considered as a basic human right and significant institutional and legislative reforms are underway to realize this right. In the Charter of Fundamental Rights of the European Union a separate article is devoted to the right of the protection of personal data,[1] while the European Court of Human Rights views the right to privacy as a prerequisite for autonomy, independent development and protection of dignity of the person.

The Constitution of Georgia provides for the right to privacy, personal development, protection of dignity, right of the citizen to get familiar with the information concerning him/her kept in public institutions, as well as the obligation of the state to protect the information in official records concerning health, finances or other private matters. All the above form the constitutional guarantee and basis for the personal data protection legislation.

"One of the essential aspects of the right to privacy is the interest of a person not to allow the disclosure of the information concerning private matters and to control the dissemination of such information.''[2] For the realization of the constitutionally guaranteed rights it is important that the processing of data is conducted on the legitimate grounds only. A person needs to know when the interference by the State in his/her private life shall be legitimate, what rights the person has and in what ways his/her interests can be protected.

As this is the first occasion of assessing the state of personal data protection in the county, the topics reflected in the report are analyzed within the lenses of the constitutionally guaranteed rights. The first part of the report discusses such basic issues as the principles of the processing of data, grounds and means of the processing, the processing of data using electronic technologies, specificities for processing biometric and the special category of data, secret eavesdropping and wiretapping, video surveillance, direct marketing, transferring the data to other countries and citizen awareness and protection of their rights. The final section of the report presents the Inspector's recommendations regarding the measures to be implemented for the protection of personal data.

1 Article 8, Charter of Fundamental Rights of The European Union (2000/C 364/01).

2 Decision of the Constitutional Court of Georgia dated 30 October 2008, #2/3/406.408, in the case of the Public Defender of Georgia and the Georgian Young Lawyers' Association against the Parliament of Georgia.

BASIC PRINCIPLES OF THE PROCESSING OF DATA

Legality of the processing of personal data and its compliance with high standards is essentially dependent on the observance of the principles of data processing. The principles reflected in the law, due to their sustainable character, establish the general rule of the processing of data and determine the legality of the acts of a data processor. The Law of Georgia on Personal Data Protection reinforces the principles such as fairness and lawfulness, protection of dignity of a data subject, existence of explicitly specified legitimate purpose, proportionality and adequacy, the validity and accuracy of data, and storage of data only for the period necessary to achieve the goal.

During consultations and meetings with data processors it was revealed that the most problematic issue in practice is **processing of data with explicitly specified legitimate purpose.** Majority of public, as well as private organizations cannot identify the concrete and legitimate purpose of the processing of data (e.g. collection, storage, making publicly accessible, etc.). An organization may have the purpose of collection and storage of data for a certain period, which does not necessarily imply the authorization to transfer the data to the other organization. While determining the purpose of processing of data by the public sector, often the normative acts regulating their activity are generally referred to, which is determined by the absence of explicitly specified legitimate purpose of data processing. This is in conflict with the fundamental principle of the Public Law – "everything that is not permitted by law is prohibited."

Applications by citizens confirm that in many cases they are inadequately informed, or completely uninformed about the purpose of data processing. A number of them also pointed out the **processing of data in an environment violating human dignity.**

For example, the persons who have undergone voluntary drug testing stated that the testing was carried out under the conditions of video control and without being offered any alternative means. At the same time, not only the personnel, but also other applicants of drug testing could see the image on the monitor located in the detention room.

In practice we encounter numerous cases of data processing, **which is disproportionate to the purpose, inadequately extensive and indefinite in period.** During the processing of data the assessment is not made regarding the extent of the data that is relevant for the purpose. Some data processors realize that the information requested or obtained by them is disproportionate and inadequate, however, the structure and format of an electronic program or a database does not allow for the processing of data in a smaller volume. Regretfully, during previous years expensive databases were created with the neglect of the standards of personal data protection, which is negatively reflected in the current situation.

Cases have been revealed in which the content and extent of the information requested from an individual was explicitly beyond the scope of the legitimate aim. However, lack of provision of such information would lead to the denial of considering the citizen's application.

At the same time, making the information public through internet in a manner that is disproportionate and inadequate to the purpose, is problematic. E.g. a credit organization used a public notification form, in which not only the name, last name and ID number were indicated, but also the factual and legal address, contact information, amount of debt and contract details. Through analysis of the contract concluded between the applicant and the data processor, as well as the correspondence between the parties, it was revealed that there was no need for the public notification through internet resources. Regretfully the present example does not represent an isolated case. Many financial-credit organizations use public notification forms and, as a rule, the information is not or cannot be closed even after the payment of a debt. The data is still available through internet and search resources, which damages the person's reputation, let alone the other threats related to making the data publicly available.

Mostly the data processors themselves acknowledge that the storage of data is performed **with a term inadequate to the purpose or without any term whatsoever.** Throughout the years data processors have been observing the principle: **"we keep everything that can be collected and stored.''** In practice the term of data storage depends not on the purpose of data collection, rather on the technical conditions such as server capacity or archiving capability. Data processors cannot ensure blockage, erasure or destroying of data that is collected without the legitimate basis and that is inadequate to the purpose of processing, which creates the risk of taking an incorrect decision or of inflicting harm to the subject.

Positive assessment is required for a number of organizations that created internal policy and organized special trainings for the employees in regard to the processing of data. In this regard, those steps are worth noting that are taken by such large processors as the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Finance and/or the Legal Entities of Public Law under their field of governance. Legal regulation and training of personnel is important, however, insufficient without the implementation in practice and creation of an effective internal control mechanism.

LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

The Law of Georgia on Personal Data Protection exhaustively defines the grounds and preconditions for the processing of data. Accordingly, every processor is obliged to ensure at least one of the following conditions provided by the law:

- consent of a data subject;
- consideration of an application of a data subject or provision of service to him/her;
- legal basis or carrying out a duty imposed by the law;
- under the law information is publicly accessible or data subject has made it publicly accessible;
- protection of vital interest of a person;
- protection of legitimate interest of a data processor or a third party, if their interest overrides the interest of protection of the rights and freedoms of a data subject;
- processing of data is carried out with the purpose of protecting an important public interest.

The analysis of the situation at hand shows that **the processing of data is often carried out without relevant legal basis.** Public, as well as private institutions cannot identify the legal basis for the processing of data and they define the concepts such as “important public interest”, “obligation compelled by legislation’’, or “legitimate interest of a third party’’ rather broadly and inconsistently.

Although the Law on Personal Data Protection came into force in 2012, amendments influenced by the Law have not been made in other laws and sub-legislative normative acts. Respectively, there is no explicit and clear formulation of the issues of the processing of data in the legal acts regulating such important spheres as health care, insurance, social security, education, communication, etc., which, in practice causes problems to many data processors. In this regard it is important to harmonize the legal framework, provide the reasoning in relevant decisions and develop the court practice, which will strike the balance between private and public interests.

CONSENT AS THE BASIS FOR THE PROCESSING OF DATA

Out of the grounds for the processing of data the most problematic issue is the consent of the data subject. According to the law, consent is a free consent given by a data subject, after receiving relevant information, to the processing of data for a specific purpose, expressed orally, by means of telecommunication or other relevant means, which can clearly indicate the will of a person.

Consultations provided to the citizens have revealed that mostly the consent of a subject constitutes the condition of receiving a certain service, rather than the expression of a free will. Citizens are not even aware of what they have consented to, whether or not they had the right to refuse the processing of their data and what legal consequence such refusal could entail.

Even with written consent it is difficult to establish the validity of the will of the subject. E.g. citizens are not informed that with signing service or other types of contract they have authorized the organizations to process their information with any form and purpose.

In formal terms, the service or other type of contract signed by the subject often constitutes the evidence of consent, one of the articles of which indirectly concerns the processing of data. As a rule, data processors are guided by the standard terms of the contract or the template text of consent and do not provide the citizens with relevant explanation about the purpose and basis of data processing. Unfortunately, even individuals do not pay enough attention to the content of the document. Even in the rare cases when citizens have asked for the clarifications or modification of the text, they were refused service.

PROCESSING OF DATA USING ELECTRONIC TECHNOLOGIES

In recent years automatic processing of data has obtained more and more widespread nature, which has contributed to the optimization of certain processes, simplification of service and reduction of bureaucratic steps. Despite the positive results of electronic governance, risks consecutive to the process could not be assessed in whole and minimum standards of protection and security of personal data could not be implemented either. Moving on to the new technologies was often happening without updating the relevant legislative framework. In the process of automatic processing of data **absence of legislative basis for data exchange and/or providing data access among agencies constitutes one of the major problems.** Recently the indicators of data exchange among different agencies, as well as the access of data processed by private sector by public agencies, have particularly raised, which further aggravates already not very favorable situation in regard to the processing of data and creates enabling conditions for the illegal processing of data. Data processors leave out of focus the important fact that the authority to collect and store data does not automatically give the organization the right to transfer these data to the other agency.

Another result of the large-scale processing of personal data using electronic technologies is the increase in the number of data processors, authorized persons and “authorized users’’ and their increased opportunities to access various databases. This creates the risk of illicit usage of data and makes it harder to detect the facts of their unlawful obtaining and of making them publicly accessible.

The law regulates the relationship between the data processor[3] and the authorized person[4] and imposes a number of requirements, namely: an authorized person can process data on the basis of a legal act or a written contract concluded with a data processor, which shall define in detail the goals and scope of the processing of data, the rights and obligations of parties and the issues of the security of data.

3 Data processor is a public institution, natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data, processes personal data individually or with the help of an authorized person.

4 Authorized person is any natural or legal person, which processes data for or on behalf of a data processor.

The law **prohibits the transfer of the right to process the data to another person by an authorized person without the consent of a data processor.** The authorized person is prohibited to further process the data for any other purpose, however, this very obligation is most commonly violated in practice. **Authorized persons store the data provided by the data processor and use them for other purposes even after the termination of a contractual relationship.** This problem was most clearly displayed in observing the process of massive dissemination of advertisement messages of various characters to the phone numbers of the users.

> The digital environment in which we are now all living is without any doubt an area of tremendous creativity, innovation and technical accomplishment. Make no mistake: it is neither possible nor desirable to "regulate" innovation, but the law can create the right responsibilities and allocate the right incentives.
>
> **M. Peter Hustinx**
> European Data Protection Supervisor

At the same time it is prohibited to conclude an agreement on the processing of data, if due to the activities and/or purposes of an authorized person, there is a risk of the non-target processing of data.

Authorized person is obliged to ensure the safety of data and to apply appropriate organizational and technical measures in this regard. Data processor is obliged to monitor the processing of data conducted by an authorized person and to apply relevant measures to avoid accidental or unlawful disclosure, access, alteration, destruction, or any other form of unlawful use and loss of data.

Unfortunately, during the reporting period, in the agreements and legal acts we reviewed and based on which data was processed, neither large part of the legal requirements was reflected in detail, nor the control of the authorized person by the processor was conducted on an appropriate level. In practice we encountered only one case of the monitoring of an authorized person by the agency, which ended with the imposition of a contractual sanction for the detected violation. It should be noted that the single facts of monitoring, without effective preventive measures, cannot be sufficient to ensure the appropriate quality of the protection of data.

Positive evaluation is required for the fact that as a result of the consultations with the Office of the Inspector, the Government Chancellery, the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Correction, the Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees, LEPL Civil Service Bureau, LEPL State Services Development Agency and LEPL Social Service Agency defined the specific grounds for the processing of data. In addition, a number of them refined the process of the processing of data and brought it in compliance with the law.

COLLECTION, STORAGE, DISCLOSURE AND OTHER TYPES OF PROCESSING OF DATA RELATING TO HEALTH, POLITICAL OPINIONS,CONVICTION AND OTHER SPECIAL CATEGORIES

The Law of Georgia on Personal Data Protection establishes special safeguards in regard to the data that is related to the person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, state of health, sex life or conviction. These data, as well as certain types of biometric data, belong to the special category of data due to their sensitive character, since the illegal collection, storage or distribution of this type of data might pose the risk of the violation of privacy, persecution of a person, harassment or other kind of discrimination.

The law prohibits the processing of special category of data, except in the following conditions:

- data subject has given written consent to the processing of special category of data;
- data subject has made the data regarding him/her public, without explicit prohibition of their usage;
- processing of data is necessary for carrying out the employment obligations or enjoying the related rights by a data processor;
- processing of data is necessary for the protection of vital interests of a data subject or a third person and a data subject is physically or legally incapable of giving his/her consent to the processing of data;
- data are processed for the purposes of the protection of public health, for the protection of a natural person's health by a medical institution (employee), also if this is necessary for the management or functioning of healthcare system;
- data are processed in the course of conducting legitimate activities by a political, philosophical, religious or trade-union, association or other non-commercial organization. In such cases the processing of data can be related solely to the members of this organization or to the persons who have regular contact with this organization.

In practice the processing of special category of data is mostly carried out with the written consent of a data subject. However, often the processors fail to ensure the provision of the document reflecting the consent, which would explicitly and clearly reflect the will of the subject. Moreover, **processors are not informed about the sensitive nature of the data processed by them and of the requirements established by the law,** due to which the minimum standard of data security is not ensured.

A large part of citizens expresses discontent with the disclosure of the special category of data, which mainly concerns making the data relating to health and conviction publicly accessible illegally.

During the reporting period the case of the disclosure of patient's medical history through media without his/her consent was observed. In addition, in one of the TV programs the data about drug addiction and conviction were illegally made public.

Consultations conducted by the Office of the Inspector revealed that in labor relations the processing of special category of data represents one of the prevalent problems. The processing of special category of data, such as conviction and the results of medical and drug testing, is regulated by the Law of Georgia on Public Service. Accordingly, there exists the legal basis for the processing of data. In regard to other types of special category of data the informed and written consent of a subject is required.

In August-September 2013, on the basis of the application from the Secretary of the National Security Council, in the framework of the research of one of the universities, the Inspector examined the issue of the processing of data on the political opinions of civil servants in 12 ministries in the pre-election period, coordinated by the Chancellery of the Government. It was determined that the aim of the study was to identify the factors determining the employment of citizens in the public sector. The Chancellery of the Government was coordinating the participation of the ministries in the study and did not constitute the data processor. Questionnaires provided to civil servants were anonymous and completing them was not mandatory. However, the questionnaire was not accompanied with relevant explanations and the questions asked, if taken all together, could enable identifying the servants participating in the research. The completed questionnaires were collected at the specifically designated person of each agency. Even though the study was terminated with the initiative of the Chancellery of Government during the examination of the issue, there was a risk of the violation of Article 4, 5 and 6 of the Law on Personal Data Protection. Therefore, the completed questionnaires were destroyed as a result of the application by the Personal Data Protection Inspector.

It is noteworthy that as a result of the trainings and consultations conducted during the reporting period, many public agencies started assessing the proportionality and legality of the data processed by them and bringing personal files of employees and human resources management systems in compliance with the law.

While processing the special category of data in the private sector grounds established by the law are often widely interpreted.

For example, one of the employers required the candidate selected as a result of a competition the mandatory provision of the information about the candidate's and his/her family members' health status, involvement in the criminal case under any status, ethnic origin and religious opinions, in addition to the information on education, work experience, salary history and income. The employment candidate had to submit these data, since the lack of provision thereof would result in the refusal for hiring.

As a result of trainings and consultations conducted during the reporting period, a number of companies started to make effort for the processing of special category of data in accordance with the law. However, up until 2016, due to the limited application of the Law of Georgia on Personal Data Protection in relation to the private sector, for large number of the processors the protection of personal data is not a priority.

PROCESSING OF BIOMETRIC DATA

Due to high public interest, while assessing the situation of personal data protection, separate discussion of the issue of processing of biometric data is required. Biometric data is any physical, mental or behavioral feature which is unique and permanent for each individual which can be used to identify this person (fingerprints, iris scan, DNA code, etc.). The very uniqueness of these data and the opportunity for unmistakable identification of a person using these data has resulted in the different regulation of this category of data by the Law of Georgia on Personal Data Protection.

The processing of biometric data is allowed only for the purposes of the security of a person and protection of property, as well as for avoiding the disclosure of secret information. At the same time, it has to be impossible to achieve these objectives by other means or to involve disproportionately huge efforts.

Apart from the abovementioned, public institutions can process biometric data for the purposes of issuing an identity document or for identifying the person crossing the state border, while private institutions can do so for the purposes of conducting their activities.

During the reporting period a problem emerged in regard to the processing of biometric data by public agencies, which relates to the access of a biometric photo kept in the database of one agency by another agency, while the data recipient does not have the legal grounds to obtain such type of data.

Unlike public agencies, private agencies, before using biometric data, are obliged to provide detailed information to the Personal Data Protection Inspector on the processing of such data. For the purpose of establishing a uniform standard, the Office of the Inspector has created the form to be provided by private organizations in relation to the processing of biometric data, as well as the relevant instructions. **However, up until today no official notifications have been submitted to the Office of the Inspector.**

On the basis of citizens' applications and consultations it is revealed that the processing and usage of biometric data occurs in conflict with the existing legislative requirements.

For example, as the citizens indicate, a number of organizations, including educational institutions, use fingerprints for determining payroll and recording turn up at work. The character of the organization's scope of work neither endorses the need for usage of such data, nor is the purpose of the processing of fingerprints determined in the internal regulations of the organization. Employees have not expressed their consent on the processing of biometric data and there is no other legal basis at hand either. In the present case the organization could control the payment or employees' turn up with other means, such as tabel, attendance journal or card.

CHALLENGES IN REGARD TO SECRET EAVESDROPPING AND WIRETAPPING

In terms of the right to privacy, a particularly pressing issue is the direct access of law enforcement bodies to the information in the database of telecommunication companies (including telephone communication and location of a person), secret eavesdropping and video surveillance, which is determined by their authority to conduct secret video and audio recording, photographing, eavesdropping of telephone conversation, etc. for the purposes of investigation.

The issue of secret eavesdropping and surveillance was raised particularly acutely in the spring of 2013, when the Ministry of Internal Affairs publicized the information on thousands of s**ecret audio and video recordings, created in 2005-2012, the total volume of which was 260 678 megabits and the length of the recordings exceeded 1760 hours.**

On this issue, as a result of the decision of the Government of Georgia, **Temporary Commission on the Issues of Illegal Eavesdropping and Secret Recording** was created, consisting of the Minister of Internal Affairs of Georgia (Head of the Commission), the Minister of Justice of Georgia, the Prosecutor General of Georgia, the Public Defender of Georgia, the Personal Data Protection Inspector, the Judge of the Tbilisi Court of Appeal, the Editor-in-chief of Resonansi newspaper, the Head of the Electoral and Political Technologies Research Center and the Executive Director of Transparency International Georgia.

> Even seeing up to three recordings in a non-identifiable form and fast-scroll mode for 1 minute is enough to realize how vulnerable, unprotected and rights deprived a person is when "the opinion police is able to connect to all the cables," install hidden cameras in residential homes or hotel rooms, offices or restaurants and grossly interfere with the private life of a person.
>
> **Tamar Kaldani**
> Personal Data Protection Inspector

The discovered material included recordings reflecting private life of politicians, representatives of business and civil society, audio recordings and photos. Some recordings reflected the facts of torture of prisoners. During its operation the Commission **could not find any official document confirming the legality of obtaining video and audio materials reflecting private life.** Under the recommendation of the Personal Data Protection Inspector, the Commission developed the methodology for registration, safety and destruction of the material reflecting intimate life, as a result of which **112 electronic information carriers** were destroyed, and the core material (633 electronic carriers) was handed over to the Main Prosecutor's Office for investigation purposes.

In so far as the criminal legislation in force could not provide proper guarantees for the protection of the right to privacy of a person and imposition of adequate liability in case of violations, the Commission developed and presented to the Parliament of Georgia the draft law, which provides for the restriction of sanctions envisaged in Articles 157-159[5] of the Criminal Code, as well as the review of components of the crime and criminalization of illegal obtaining, storage, usage and dissemination of personal data.

> The State is generally prohibited to become familiar with the content of conversations and messages created though telephone and other technical means, as well as to impose control on with whom and to what intensity such relationships were carried out.
>
> Constitutional Court of Georgia[6]

In the second half of 2013 the **judicial control over secret eavesdropping and recording improved,** as well as the video surveillance with technical means. According to the statistical data of the Supreme Court, in 2012 the court refused to grant only 0.25% of the motions, whereas in 2013 the number was 7.56%.[7] Under the information provided by the Ministry of Internal Affairs, **internal monitoring of the process of operational investigative actions was tightened** and refined. For the purpose of stricter control and elimination of the possibilities of unlawful obtaining of information, the Ministry of Internal Affairs carried out a number of organizational measures, in particular:

1. At various ministries decentralized secret eavesdropping systems were abolished and currently the mentioned inquiries are conducted in a centralized form and by one specific agency, which significantly limits the capability of conducting unlawful eavesdropping, making it easier to apply control mechanism at the same time;

2. Covert eavesdropping is carried out in specially protected zones with limited access, which only duly authorized persons have access to. For the purposes of control tripartite, including biometric control system is used;

3. In the limited access zones video surveillance systems were improved, the aim of which is to identify and prevent the facts of information leakage and attempts of unlawful duplication of the obtained material;

4. To prevent information leaks, in the abovementioned areas entry was restricted with the photo and video equipment, cell-phones and other means for recording and storing the information;

5. Authorized persons' electronic registration of logging to access the system was restricted.

5 Disclosure of Personal or Family Secrets (Article 157); Disclosure of Secret of Private Conversation (Article 158); Disclosure of Privacy of Personal Correspondence, Telephone Conversations or Other Massage (Article 159).

6 Decision of the Constitutional Court of Georgia dated 26 December 2007, #1/3/407, in the case of the Georgian Young Lawyers' Association and the Citizen of Georgia Ekaterine Lomtatidze against the Parliament of Georgia.

7 In 2012 the court heard 11580 motions, while in 2013 – 3699 motions.

It is important that surveillance, eavesdropping and access to the data of telecommunication companies conducted by law enforcement bodies for the purposes of investigation, is in compliance with the requirements of Article 8 of the European Court of Human Rights and international standards. According to the European Court of Human Rights, national legislation has to envisage adequate guarantees against the abuse or misuse of power by the government bodies.[8] To comply with these standards, it is appropriate to refine the legislation and create an independent control mechanism of high legitimacy, which would ensure the balance between human dignity, right to privacy and the legitimate public interests of public safety and investigation and prevention of a crime.

It is noteworthy that during the reporting period several citizens applied to the Personal Data Protection Inspector. Their main issue of interest was their right to get familiar with the information stored in the law enforcement agencies, obtained as a result of secret surveillance on them. As the Law of Georgia on Personal Data Protection does not apply to the processing of data for the purposes of public and state security (including economic security), defense, operative-investigative activities and criminal investigation, the rights of the citizens guaranteed by the Law are limited and the Inspector is incapable to react on these kinds of applications.

According to the European standards a person shall have the opportunity to receive information on operation-investigative activities conducted against him from the moment when providing such information is not likely to objectively prejudice the interests of the investigation.[9] Implementing this standard in Georgia will promote the creation of adequate safeguards for the right to privacy and the persons on whom operational-investigation activities were carried out will be able to file a complaint for the violation of the right to privacy, in case these activities were conducted illegally in relation to them.

8 Klass and Others, pp. 25 26, §§ 54 56; mutatis mutandis, Leander v. Sweden, judgment of 26 March 1987, Series A no. 116, pp. 25 27, §§ 60 67; Halford, cited above, p. 1017, § 49; Kopp, cited above, p. 541, § 64; and Weber and Saravia, cited above, § 94.

9 Principle 2.2; Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the Use of Personal Data in the Police Sector.

PURPOSE AND LEGALITY OF VIDEO SURVEILLANCE

Recently various private and public institutions have increasingly been using video control. Citizens have increasing interest in the video monitoring and recordings in the streets or public places, buildings and public transport.

The legislation in force regulates the purposes and rule of conducting video surveillance in the street, in public and private institutions and residential buildings. Conducting video surveillance is allowed only for the purposes of crime prevention, the security of persons and protection of property, secret information, public order and the protection of minors from negative influence. In addition, in case of installing a video surveillance system, public and private institutions are obliged to post a relevant warning sign in a visible place.

CCTV surveillance has become a common feature of our daily lives. We are caught on numerous CCTV cameras as we move around our towns and cities. Whilst the use of CCTV continues to enjoy general public support, it necessarily involves intrusion into the lives of ordinary individuals as they go about their day to day business. Our research has shown that the public expect it to be used responsibly with effective safeguards in place.

Richard Thomas
Information Commissioner of the United Kingdom (2002 -2009)

Only outdoor perimeter and entrance of a building can be monitored by a video surveillance system. In addition, it is prohibited to conduct video surveillance in dressing rooms and the places of hygiene.

As the study of the subject revealed, **the purpose of using video surveillance systems often transcends the scope prescribed by the law.** Organizations are unable to provide reasoning for their decisions of conducting video surveillance and cannot identify the purpose prescribed by the law.

Non-compliance with the legislative requirement that obliges private and public institutions to inform employees in writing about the video surveillance being conducted and of their rights is to be particularly noted.

E.g.: By one of the organizations video monitoring was carried out to impose disciplinary responsibility on the employees in case of their turning up late, while the employees were not informed about this.

In most of the cases, **warning signs about the video surveillance are not posted on buildings and outdoor perimeters** and data subjects are not provided the information about control in any other form either.

The Law establishes the obligation of the data processor to create **a filing system, designed for storing video recordings.** Except for recordings (photos/voice), a system should contain the information on the date, place and time of the processing of data. The practice studied by the Inspector's Office showed that most of the processors fail to establish a uniform standard of technical procedures and terms of the storage of recordings. **Often the storage of recordings is not conducted with the term proportionate to the purpose of their collection, nor are the minimum standards of their safety observed and it is unclear who might be able to access these recordings.**

In the beginning of October 2013, after the video and audio recordings of the prison cell of the accused Bachana Akhalaia were broadcasted through media,[10] the Inspector, on its own initiative, started to study the issue of conducting audio/video monitoring and record keeping in the penitentiary system.

As a result of studying the requested information and on-site inspection, the need for carrying out legal, procedural and infrastructural changes was revealed, including amending the legislative framework on conducting surveillance through technical equipment, establishing the uniform rule for surveillance using technical equipment and establishing the uniform standards for the protection and safety of personal data.

Recommendations elaborated by the Inspector concerned as follows:

- *Regulation of taking and implementing decisions concerning the usage of audio, video, electronic and other technical means, as well as of the issue of storage, erasure and destruction of confidential information and the information containing personal data;*
- *Assessment of the grounding and proportionality to the purpose of the decision on conducting control using technical means by the administration of the Penitentiary Institution;*
- *Posting a warning sign on a video/audio control in a visible place in the building of a penitentiary institution;*
- *Informing persons present at the institution about using any form of control against them;*
- *Separation of the processes of conducting video and audio monitoring;*
- *Bringing the information security policy, procedures and work instructions in compliance with internationally recognized standards;*
- *Training of Penitentiary System employees and informing them on security policies and data protection issues.*

10 Kakheti Information Center publicly released a part of the video/audio materials recorded in the cell of Bachana Akhalaia, in which the voice of Bachana Akhalaia himself and the persons having entered the cell is heard: http://www.ick.ge/articles/16000-i.html.

It should be noted that the recommendations provided in the 8 November 2013 findings of the Inspector were reflected in the amendments to the Imprisonment Code proposed by the Ministry of Corrections and Legal Assistance. Development of the special training program by the Training Center of the Ministry on the issues of protection of personal data deserves positive evaluation. However, recommendations related to information security policy require longer term and more comprehensive approach.

In the reporting period installation of video cameras in the mini-busses has taken place throughout Tbilisi. Stemming from high public interest, the Inspector issued a statement on this matter and applied to the relevant agency with the recommendation to use warning signs. Studying the issue revealed the need for legal regulation of video surveillance in public transport, as the Law on Personal Data Protection in force only regulates conducting video surveillance in the street, institutions and residential buildings.

TRANSFER OF PERSONAL DATA TO ANOTHER STATE AND/OR INTERNATIONAL ORGANIZATION

In July 2013 the Parliament of Georgia ratified the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which regulates cross-border data flows.

Transfer of personal data outside the jurisdiction of the state is associated with certain risks, therefore, the Law of Georgia on Personal Data Protection regulates the issue of the data transfer to another state and/or international organization and gives the Inspector the authority to assess the relevant guarantees of data protection in another state/international organization based on the analysis of legislation and practice.

According to the law, the transfer of data is allowed, if:

- Relevant legal grounds for the processing of data are present and adequate safeguards for the protection of data are ensured in a recipient state and/or international organization;
- This is envisaged by an international agreement of Georgia;
- Adequate safeguards are ensured under the agreement concluded between a data processor and a recipient state.

In the latter case, data shall be transferred after the permission of the Inspector. However, at present, the Office has received only one application to obtain permission for the transferring of data to Germany.

The analysis of practice demonstrates that ***the transfer of data is often conducted without relevant legal basis.*** In addition, it is problematic to reflect relevant safeguards for data protection in the agreements concluded between parties. Typically, agreements between Georgia and a data processor in a foreign country and/or founding documents do not regulate the issues relevant to information transfer and security.

Often foreign shareholders or partners of data processors have access to personal databases created in Georgia.

Because of the lack of regulation of the issue, personal data of the citizens of Georgia, in a systematic and uncontrolled manner, flows to different countries and international organizations without their consent or some other legal basis.

In order to regulate the issue of cross-border transferring of data, the Office of the Inspector is currently working on **the creation of so called “white list”,** which will allow data processors, in the presence of the grounds required by law and without special permission, to transfer data to legal entities and individuals in those countries, which provide adequate safeguards of data protection.

DIRECT MARKETING

Recently offering products or services to citizens using text messages has obtained such large-scale character that the main portion of the citizens' applications concern unwanted advertising messages and the processing of data for this purpose. Subjects cannot obtain the information about the source of their data and the means for terminating the processing of data, since it is unknown who the data processor is– mobile operator, advertising company or advertiser.

Under the law in force data obtained from publicly accessible sources, such as name, address, telephone or fax number and email address can be processed for the purposes of direct marketing. For processing other categories of data **consent of a data subject** is required. **Despite the consent, the data subject has the right to request in writing the termination of the usage of data concerning him/her at any time.** The processor is obliged to terminate the processing of data in no later than 10 working days after receiving the application from the subject and, at the same time, to explain his/her rights. As the advertiser determines the goals and means of direct marketing, it is the advertiser's obligation to inform the data subjects and to ensure the requested termination of the processing of data. Apart from this, the processor needs to make sure that the advertising company hired by him took appropriate organizational and technical measures to protect the data. The processor is also responsible to monitor the processing of data by an authorized person.

As for many years there was no legislation concerning personal data protection and various types of personal data were often made public, shared and sold. Consequently, quite voluminous markets emerged, establishing the legitimacy and source of which is related to difficulties. At the same time, the Law in force does not envisage the opportunity of inspecting and using relevant sanctions in relation to private sector until 2016, as a result of which the Inspector is unable to affectively react on the citizens' complaints. During the reporting period a number of citizens were consulted on their rights and obligations during the processing of data for the purposes of direct marketing and on the means for the realization of these rights. At the same time, with a public statement the Inspector called upon the companies conducting direct marketing to protect the existing legal requirements.

It should be noted that the provision of the Law regulating direct marketing needs to be improved, for which, with the initiative of the Office of the Inspector, a draft Law is being developed to amend the Law on Personal Data Protection.

CITIZEN AWARENESS AND PROTECTION OF RIGHTS

As it is indicated in the Annual Report N14 of the Article 29 Data Protection Working Party,[11] data of a single person are registered from 250 to 1000 databases. In fact it is impossible for a person to control the legality of processing of his/her data in each database, let alone the realization of the right of receiving information, rectification of data or request for erasure. Right to protect personal data cannot be adequately ensured, if it is only dependent on taking certain actions by citizens. Therefore, data processors have to take responsibility for the legality of the processing of data.

In Georgia even the large organizations fail to fully realize their responsibilities and obligations. Even though the Law of Georgia on Personal Data Protection came into force in May 2012, its practical implementation started only in the second half of 2013, after the creation of the supervisory institution over the personal data protection.

In the conditions of technological advances obtaining and processing of personal data acquired speedy, large-scale and voluminous character.

In everyday life people see the frequency of the collection, storage, disclosure or dissemination of their data. Certain part of the citizens has the feeling that they are under constant scrutiny. Consequently, they are interested for what purpose and term the information concerning them is collected, whether this is lawful, who can access their data and what means are at hand to redress their violated rights.

92% of Europeans are concerned about mobile apps collecting their data without their consent. 89% of people say they want to know when the data on their smartphone is being shared with a third party. Why are the figures so poor? Because citizens know that companies use their personal data in ways that they cannot control or influence. . . . Often with applications, the rule is 'take it or leave it'. That's when trust evaporates. That's when people feel forced to part with their privacy. I believe that this is a question of individuals' rights being overridden by technological change. That's why it is important to put individuals back in control by updating their rights.

Viviane Reding
Vice-President of the European Commission

Due to the low awareness level, unfortunately, citizens often make their personal data public through social networks or other means without realizing what kind of harm their action can entail. This is an acute problem not only in Georgia, but also in other more developed countries. The report issued by the European Union Agency for Fundamental Rights on the basis of the study conducted in 16 countries,[12] highlights the low level of citizen awareness and consciousness. Therefore, raising public awareness is indicated as the main recommendation.

11 „The Article 29 Data Protection Working Party" was founded on the basis of the Directive of the European Parliament and of the Council of 24 October 1995 (95/46/ EC.)

12 FRA, Access to Data Protection Remedies in EU Member States, Publications Office of the European Union, 2013, p.10

Office of the Personal Data Protection Inspector, with the purpose of informing public, released statements on the rights of citizens through media and prepared information materials. Along with the information, a few template statements needed for the realization of the rights are available on the web-page. In addition, the Office of the Inspector works on raising the education level of data processors, as ensuring the data protection in the country depends on their fulfillment of legal requirements.

Positive assessment is due for the fact a number of large processors, including public institutions, are willing to take effective steps to fulfill the obligations provided by the law, which shall be expressed in ensuring the accessibility of information for citizens and in creating an effective and simple mechanism for the rectification, erasure or destruction data.

RECOMMENDATIONS TO THE GOVERNMENT OF GEORGIA REGARDING THE MEASURES TO BE IMPLEMENTED FOR THE PROTECTION OF PERSONAL DATA

The analysis of the existing legislative framework and the situation in practice reveals the necessity for taking effective steps for the implementation of the high standards of data protection, which is also one of the pre-requisites for the simplification of the visa regime with the European Union. For this purpose the Personal Data Protection Inspector developed the following recommendations:

1. The Law of Georgia on Personal Data Protection needs to be brought in full compliance with the European standards.[13] In particular:

- To expand the list of data belonging to special category and to specify the grounds for their processing;
- To improve the existing provisions relevant to the rights of personal data subject and to increase the guarantees for protection;
- To refine the regulations relevant to direct marketing;
- To move closer the date of the enactment of the law in relation to the private sector;
- To regulate the conducting of video surveillance in public places and public transport;
- To improve the regulations for transferring the data to other states/international organizations and to bring them in compliance with the Additional Protocol of the Convention;
- To increase the accountability of the Inspector to the Parliament.

2. In so far as no comprehensive review of the legislative framework was conducted while adopting the Law on Personal Data Protection (except for the General Administrative Code of Georgia), in the first stage, for the stability of the supervisory institution, amendments should be made in the Law of Georgia on Public Service and the Law of Georgia on the Conflict of Interests and Corruption in the Public Service, as well as in a number of sub-legislative acts. At the next stage it is important to analyze the sectoral legislation (health care, insurance, banking-finance activities, education, social security, etc.) and, in case of need, to make their gradual revisions.

3. To ensure legitimate and proportional processing of data by public institutions, the rule and terms of storing, archiving and destruction of data shall be regulated. The data obtained without the legal basis in the public institutions must be immediately blocked, erased or destroyed.

13 Council of Europe Convention N108 on the Protection of Individuals with regard to Automatic Processing of Personal Data; as well as the Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) and best experiences of the European states.

4. In case of the processing of data by an authorized person, data processors shall ensure:

- Processing of data by an authorized person on the basis of a written agreement or a legal act and in compliance with relevant security measures;
- Conducting periodic monitoring for the purpose of preventing and eradicating the misuse of data.

5. In the legislative initiatives relevant to secret eavesdropping and wiretapping it is reasonable to include adequate guarantees against the abuse or misuse of power by the authorities and the mechanisms that would ensure striking the balance between human dignity and the right to privacy and the legitimate public interests of public security, crime prevention and investigation.

6. At the conclusion of international treaties and agreements, the issue of transferring information containing personal data by public institutions to other countries and international organizations shall be taken into account.

OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

www.personaldata.ge

www.pdp.ge

(+995 32) 242 1000

#15 Aphaqidze str. 0171,
Tbilisi, Georgia

office@pdp.ge