STUDY ON THE STATE OF PERSONAL DATA PROTECTION OF THE LGBT+ COMMUNITY MEMBERS IN GEORGIA

2022

"RULE OF LAW CENTRE"

The study was carried out by the non-govermental organization Rule of Law Centre.

Authors of the report: Londa Toloraia, Tamar Daushvili, Tamar Zubashvili.

This study has been prepared with the assistance of the European Union (EU) and the United Nations Development Programme (UNDP). Its contents are the sole responsibility of the Rule of Law Centre and do not necessarily reflect the views of the European Union and the United Nations Development Programme.

The Rule of Law Centre thanks the non-governmental organizations Women's Initiatives Supporting Group (WISG), Equality Movement and Identoba Youth for their assistance in the process of the study.

TABLE OF CONTENTS

I. INTRODUCTION

The right to private life and personal data protection are fundamental rights guaranteed by both international and national legislation. Protecting these rights is equally important for everyone, but the right to private life and protection of personal data of the LGBT+ community members is even more important, as they often become victims of abuse, discrimination, degrading treatment, verbal and physical violence when disclosing information about their sexual orientation or gender identity.

Personal data of the LGBT+ community members, especially special category of data (which includes information such as: sexual life, state of health, granting a person victim status and/or recognition as a victim, etc.) are processed in various areas: in healthcare sector, law enforcement agencies, courts, etc. Illegal collection, use, exchange or other processing of such sensitive data may cause irreparable physical, moral or property damage to the community members and affect their relationships with family members, friends, acquaintances, colleagues or other members of society.

It is clear that processing of personal data of LGBT+ persons is necessary for provision of services or planning correct (socio-economic, educational, employment, physical and mental health management and development of opportunities) policies in relation to them. However, public and private institutions that process personal data of the LGBT+ community members have a special responsibility for data protection when processing this data, since lack of protection leads to weakening or disappearance of the trust of the community members in the institution in question, which negatively affects not only the right to data protection, but also other rights, for the exercise of which members of the community must apply to various private or public institutions. LGBT+ community members, due to the fear of disclosing information about their sexual orientation, gender identity, HIV status or other data, may refrain from contacting, for example, medical institutions, law enforcement agencies, which threatens their vital rights (the right to life, the right to health, etc.). Thus, protecting the data of LGBT+ persons is important both for their right to privacy and protection of personal data, as well as for the exercise of other fundamental rights.

The purpose of this study is to examine the state of personal data protection of the LGBT+ community members in Georgia, identify problems existing in the process of data processing and develop recommendations in various areas to raise the standard of protecting personal data of the community members.

The present study provides an analysis of legislation regulating personal data, results of interviews with representatives of LGBT+ persons and NGOs involved in the protection of the rights of the LGBT+ community members, problems they see in the data processing process, current practice of the Data Protection Authority in relation to processing data of the LGBT+ community members, including decisions delivered and recommendations in various areas, the implementation of which shall promote improving the state of personal data protection of the LGBT+ community members in Georgia.

II. METHODOLOGY OF THE STUDY

Within the framework of the study, interviews were conducted with 20 people, 10 of whom were members of the LGBT+ community and 10 were representatives of the non-governmental organizations working on the rights of the LGBT+ community members. Some of the interviews were conducted online, and some through in-person meetings.

Transgenders, gays and lesbians were among the interviewed LGBT+ community representatives. Therefore, the study covered all the challenges faced by representatives of different groups of the community in different areas.

As for the organizations, representatives of non-governmental organizations were involved in the process of the study - Women's Initiatives Supporting Group (WISG), Equality Movement, Identoba Youth, heads of the organizations, lawyers, social workers.

The interviews were preceded by the development of a questionnaire that addressed the issues of processing personal data of the LGBT+ community members in various areas: grounds for data processing, data processing principles, various forms of data processing (collection, use, disclosure, publicizing, video recording, etc.) and the rights of the data subject. The questions also related to the processing of data by the media outlets for the purpose of informing the public and issues of disclosure of data by the community members for personal purposes. Also, as part of the study, interviewees were asked about the level of awareness of the community members on data protection issues and the protection mechanisms they use regarding the facts of illegal data processing. In addition, the object of the study was the needs of the organizations that protect the rights of representatives of the LGBT+ community in terms of data protection.

In parallel with the information obtained as a result of the interviews, information and decisions related to the processing of personal data of the LGBT+ community members were requested from the Data Protection Authority and analyzed (five decisions were provided by th Authority).

Within the framework of the study, international regulations and national legal acts related to personal data were analyzed.

III. INTERNATIONAL ACTS AND NATIONAL LEGISLATION

According to Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, a person's right to personal data protection forms the part of the right to respect for private and family life, home and correspondence. [1]

According to Article 2(a) of the amended Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called 108+ Convention), personal data is any information relating to an identified or identifiable person ("data subject"). [2]

Pursuant to Article 4(1) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[3]

Pursuant to paragraph "a" of Article 2 of the Law of Georgia on Personal Data Protection, personal data is any information connected to an identified or identifiable natural person. A person shall be identifiable

1 *Handbook on European Data Protection Law, 2018 Edition, European Union Agency for Fundamental Rights and Council of Europe p. 20. see: https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf*

2 *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, see: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1*

3 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), see: https://gdpr-info.eu/*

when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural or social features specific to this person. [4]

Modernized Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the so-called 108+ Convention) and the Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), which are important international instruments for the protection of personal data, separately list special category of data (so-called "sensitive data"). The definition of a special category of data is also given in the Law of Georgia on Personal Data Protection.

Article 6 of the modernized Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (the so-called 108+ Convention) lists special categories of data, which include: genetic data; personal data relating to offenses, criminal proceedings and convictions and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health or **sexual life.**

Article 9 of the Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), assigns the following to special categories of data: racial or ethnic origin of a person; political opinions; religious or philosophical beliefs; trade union membership; genetic data, biometric data for the purpose of uniquely identifying a natural person, **data concerning health or data concerning a natural person's sex life or sexual orientation.**

Therefore, the modernized Council of Europe Convention for the Protection of Persons with regard to Automatic Processing of Personal Data (the so-called 108+ Convention) does not explicitly refer to sexual orientation and gender identity as a special category of data, however, sex life is considered as special category of data. According to the Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), sexual orientation, together with sex life, is considered a special category of data, but does not explicitly refer to gender identity.

According to subparagraph "b" of Article 2 of the Law of Georgia on Personal Data Protection, a special category of data is data related to a person's racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership, state of health, **sex life,** criminal record, administrative detention, application of a restraint measure, plea bargain, diversion, granting a person victim status, as well as biometric and genetic data that allow to identify a natural person by the above features. Therefore, there is no explicit reference in the Georgian legislation to sexual orientation and gender identity as a special category of data, although sex life is considered as such data.

The Modernized Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called 108+ Convention) and the Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), as well as the Law of Georgia on Personal Data Protection do not give the definition of the term "sex life".

In order to determine whether sexual orientation and gender identity are (or should be) a special category of data and whether the term "sex life" includes "sexual orientation" and "gender identity" in itself, it is necessary to determine necessity of special protection of this type of data and give detailed definition of these terms.

4 *Law of Georgia on Personal Data Protection, see: https://matsne.gov.ge/en/document/view/1561437*

The special nature of data is determined by the need for their special protection. The Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) states that personal data, which by their nature are particularly sensitive in relation to fundamental rights and freedoms, require special protection as the context of their processing may involve significant risk to fundamental rights and freedoms. [5] The explanatory report to the Modernized Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the so-called 108+ Convention) states that sensitive data should be protected to a greater extent, since their processing "may lead to encroachments on interests, rights and freedoms". This can be the case for example, "where there is a potential risk of discrimination", when the interference takes place in the most intimate area of the data subject, such as the person's sex life or sexual orientation. Accordingly, in order to avoid adverse consequences for the data subject, such processing "should only be permitted where appropriate safeguards which complement the other protective provisions of the Convention, are provided for by law".[6]

It is a fact that the processing of data about both sexual orientation and gender identity can pose a significant risk to the rights of the LGBT+ community members, as disclosure of this data may expose them to abuse, discrimination, degrading treatment, verbal and physical violence (there were many examples of this in Georgia). Therefore, this data really needs special protection compared to regular data.

As to whether "sex life" includes "sexual orientation" and "gender identity", it is necessary to understand their meaning.

"Sexual orientation" is a person's ability to experience deep emotional, romantic or sexual attraction as well as intimate/sexual connection with persons of the opposite sex (heterosexual), the same sex (homosexual, lesbian, gay) or more than one sex (bisexual).[7] It is worth noting that "sexual orientation" is closest to the "sex life" category, and therefore most international data protection laws recognize "sexual orientation" as part of "sex life" and a special category of data. And, as mentioned above, the Regulation of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) recognizes data on "sex life" and "sexual orientation" as special categories. Accordingly, "sex life" as provided for by the Law of Georgia on Personal Data Protection should be interpreted broadly, and "sexual orientation" should be considered as part of "sex life".

As for "gender identity", this is an individual internal perception by a person of his belonging to a man, woman or another sex. [8] Unlike "sexual orientation", most international data protection laws do not explicitly assign so-called "gender identity" to "sensitive data",[9] however, due to the nature of data on gender identity and the fact that in practice in most cases the processing of information on gender identity is also associated with the processing of information on sexual orientation, and at the same time, Georgian legislation allows for a broad definition of "sex life", "gender identity" should be considered as part of "sex life" and therefore a special category of data.

---

5 *Paragraph 51 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), see: https://personaldata.ge/cdn/2018/11/GDPR-%E1%83%97%E1%83%90%E1%83%A0%E1%83%92%E1%83%9B%E1%83%90%E1%83%9C%E1%83%98.pdf*

6 *The Difficulty of Defining Sensitive Data - The Concept of Sensitive Data in the EU Data Protection Framework, Paul Quinn and Gianclaudio Malgieri, p. 1585. See: https://www.cambridge.org/core/journals/german-law-journal/article/difficulty-of-defining-sensitive-datathe-concept-of-sensitive-data-in-the-eu-data-protection-framework/5EC5932AAC5703E31D2C90045813F6C6*

7 *Policing Hate Crime against LGBTI Persons: Training for a Professional Police Response, see: https://rm.coe.int/hate-crimes-against-lgbti/168073dd37*

8 *Ibid.*

9 *See article, https://iapp.org/news/a/does-brazils-lgpd-recognize-gender-identity-and-sexual-orientation-as-sensitive-personal-data/*

The Law of Georgia on Personal Data Protection regulates the protection and processing of personal data in Georgia, establishes mandatory rules for organizations and individuals involved in data processing and defines administrative liability for violation of these rules.

The Law of Georgia on Personal Data Protection exhaustively lists the grounds for processing the so-called "ordinary", as well as special category of data. In particular, Article 5 of the law defines the grounds for processing the data of the "ordinary" category, and Article 6 - the processing a special category of data.

According to Article 5 of the law, processing of personal data is allowed if: a) there is a data subject's consent;[10] b) data processing is provided for by Law; c) data processing is necessary for a data controller to perform his/her statutory duties; d) data processing is necessary to protect vital interests of a data subject; e) data processing is necessary to protect legitimate interests of a data controller or a third person, except when there is a prevalent interest to protect the rights and freedoms of the data subject; f) according to the Law, data are publicly available or a data subject has made them publicly available; g) data processing is necessary to protect a significant public interest under the Law; h) data processing is necessary to deal with the application of a data subject (to provide services to him/her).

Pursuant to paragraph 2 of Article 6 of the above law, special category of data can be processed with the written consent of the data subject[11] or in case when a) processing of the data related to previous convictions and state of health is necessary for labour obligations and labour relations, including making a decision regarding employment; b) data processing is necessary to protect the vital interests of a data subject or a third person and when the data subject is physically or legally unable to give his/her consent to data processing; c) the data are processed for public health protection, health care or protection of health of a natural person by an institution (employee), and if it is necessary to manage or operate the health care system; d) a data subject has made his/her data publicly available without an explicit prohibition of their use; e) data are processed by a political, philosophical, religious or professional union or a non-commercial organisation when implementing legitimate activities; In this case, the data processing may only be connected with the members of this union/organisation or persons who have regular contacts with this union/organisation; f) data are processed to consider the issues related to the maintenance of personal files and registers of the accused/convicted persons; to the individual planning for a convicted person to serve his/her sentence, and/or the release of a convicted person on parole and the change of an unserved term of his/her sentence with a lighter punishment; g) data are processed for the purpose of enforcing legal acts under Article 2 of the Law of Georgia on Enforcement Procedure of Non-custodial Sentences and Probation; g[1]) data are processed for the purpose of re-socialization and rehabilitation of convicts and ex-prisoners, implementation of crime prevention measures and coordination of juvenile referral process; h) data are processed in the cases directly provided for by the Law of Georgia on International Protection; i) data are processed for the functioning of the unified analytical system of migration data; j) data are processed for the purpose of realization of the right to education of persons with special educational needs; k) data are processed in order to consider the issue provided for in Paragraph 2 of Article 11 of the Law of Georgia on Prevention of Violence Against Women and/or Domestic Violence, Protection and Assistance to Victims of Violence. According to paragraph 3 of Article 6 of the Law of Georgia on Personal Data Protection, in case of the above ground(s) of the processing of special category data, a separate ground for making public and

10 *Pursuant to subparagraph "g" of Article 2 of the Law of Georgia on Personal Data Protection, consent is defined as a voluntary consent of a data subject, after receipt of the respective information, on his/her personal data processing for specific purposes expressed orally, through telecommunication or other appropriate means, which enables clearly establishing the will of the data subject.*

11 *Pursuant to subparagraph "h" of Article 2 of the Law of Georgia on Personal Data Protection, written consent of the data subject is a voluntary consent expressed by a data subject, after receipt of the respective information on his/her personal data processing for specific purposes, which was signed or otherwise acknowledged by the data subject in writing or in any other equivalent form.*

disclosing this data to a third party - the consent of the data subject - is required.

Pursuant to the Law of Georgia on Personal Data Protection, in order for the processing of personal data to be considered lawful, it is necessary not only to have the grounds for data processing, but also to comply with the principles of data processing. Article 4 of the law lists the following principles: a) data must be processed fairly and lawfully, without insulting the dignity of a data subject; b) data may be processed only for specific, clearly defined and legitimate purposes. Further processing of data for purposes that are incompatible with the original purpose shall be inadmissible; c) data may be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which they are processed; d) data must be valid and accurate, and must be updated, if necessary. Data that are collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed; e) data may be kept only for the period necessary to achieve the purpose of data processing. After the purpose of data processing is achieved, the data must be blocked, deleted or destroyed, or stored in a form that excludes identification of a person, unless otherwise determined by Law.

Public and private institutions processing personal data must ensure data security. In particular, pursuant to paragraphs 1 and 3 of Article 17 of the Law of Georgia on Personal Data Protection, A data controller is obliged to take appropriate organisational and technical measures to ensure protection of data against accidental or unlawful destruction, alteration, disclosure, collection or any other form of unlawful use, and accidental or unlawful loss. Measures taken to ensure data security must be adequate to the risks related to processing of data. According to paragraph 4 of the same Article, any employee of the data processor involved in the processing of data is obliged not to exceed the scope of the powers granted to him and is obliged to protect the confidentiality of the data, including after the termination of his official powers.

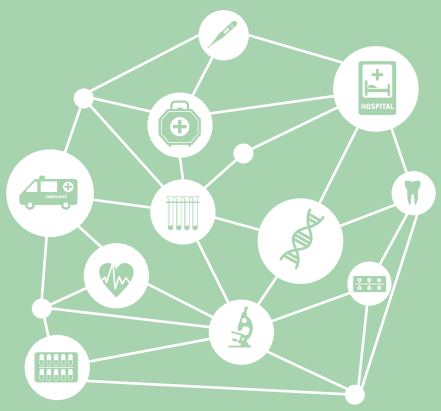
At the same time, the Law of Georgia on Personal Data Protection lists the rights of the data subject.[12] Pursuant to Article 15 of the Law, if data are collected directly from a data subject, a data controller or a data processor shall be obliged to provide the data subject with the following information: a) identities and registered addresses of the data controller and the data processor (if applicable); b) purpose of data processing; c) whether provision of data is mandatory or voluntary; if mandatory – the legal consequences of refusal to submit them; d) the right of the data subject to obtain information on his/her personal data processed, request their correction, updating, addition, blocking, deletion and destruction. According to Articles 21-16, the data subject has: the right to request information from data controller concerning processing of his/her personal data, the right to request correction, update, addition, blocking, deletion and destruction of data, the right to withdraw their consent to the processing of data and request the termination of the processing of their data and/or the destruction of the processed data, as well as the right to file a complaint with the Personal Data Protection Service or a court in case of illegal processing of their data.

It should also be noted that illegally obtaining, storing, using, disseminating or otherwise providing access to personal information that caused significant damage is a crime under Article 157 of the Code of Law of Georgia, [13] which from March 2022 falls under the investigative jurisdiction of the Special Investigation Service. [14]

12 *Pursuant to paragraph "f" of Article 2 of the Law of Georgia on Personal Data Protection, data subject is any natural person whose data is being processed.*

13 *Criminal Code of Georgia. See: https://matsne.gov.ge/en/document/view/16426?publication=235*

14 *Article 19 of the Law of Georgia on Special Investigation Service. See: https://matsne.gov.ge/en/document/view/4276790?-publication=4*



IV. PERSONAL DATA PROCESSING IN HEALTHCARE SECTOR

INTRODUCTION

Data relating to a person's physical or mental health, including information about medical complaints, diagnoses, treatment, examinations, recoverable diseases, referrals to health facilities, is health-related data.

In order to protect human health and provide medical care, the above personal data are processed daily in a number of institutions: in multidisciplinary hospitals, clinics, specialized centers, dental clinics, laboratories, as well as by individuals engaged in independent medical activities and others.

Human health information is a special category of data and a high standard of protection is applied to such data under both national and international law.

The Law of Georgia on Personal Data Protection and the legislation regulating healthcare (Laws of Georgia on Patient's Rights, Health Protection, HIV Infection/AIDS) exhaustively determine the permissible cases of disclosure of patient information to third parties. In addition, it strictly defines the obligation of the person providing medical services to protect the confidentiality of the information available about the patient, while the medical worker and all employees of the medical institution are obliged to protect medical secrecy.

When providing medical services to the LGBT+ community members, medical institutions often process information not only about their health, but also about their sexual orientation and gender identity, the

unlawful disclosure and/or illegal processing of which sometimes leads to very serious consequences - from stigmatization and discrimination to violence.

Given the above, the issue of protecting the personal data of community members in the healthcare sector becomes even more important. The collection, disclosure and other use of data by medical institutions and their medical workers, other personnel must be carried out in accordance with the rules established by the Law of Georgia on Personal Data Protection and the legislation regulating the healthcare sector.

IDENTIFIED SHORTCOMINGS

Interviewed members of the LGBT+ community and representatives of organizations protecting the rights of the LGBT+ community members pointed out a number of shortcomings in the protection of personal data in the healthcare sector: facts of violations of both the grounds of data processing and the principles of data processing, improper informing of data subjects when obtaining written consent for the processing of their data. They also spoke about the insufficient measures taken by medical institutions for the purpose of data security.

The study also identified healthcare facilities that are frequently used by the community members who face multiple breaches of their data privacy: First of all JSC Scientific-Practical Center of Infectious Pathology, AIDS and Clinical Immunology was named as such an institution; also LLC Aladashvili Clinic, LLC Maternity Hospital of the Patriarchate named after Saints Joachim and Anna, Tbilisi Balneological Spa Resort, Center for Mental Health and Drug Abuse Prevention (including regional centers), New Hospitals, David Tatishvili Medical Center, National Research Center for Dermatology and Venereal Diseases (Health Rooms), Evex Clinics, Medcenter, Tbilisi Marine Hospital.

WRITTEN CONSENT TO THE PROCESSING OF PERSONAL DATA

Representatives of the LGBT+ community interviewed within the framework of the study noted that they give their written consent to the processing of personal data in medical institutions without realizing it: no one explains the meaning of this consent, the procedure and rules for processing their data and their rights in the data processing process. While medical institutions process a special category of data of the LGBT+ community members (including sexual orientation, gender identity), providing these patients with full information about the processing of their personal data can be of utmost importance in the process of avoiding the consequences that sometimes accompany the accessing this data by others.

DISCLOSURE OF DATA DURING THE REGISTRATION PROCESS

The persons interviewed within the framework of the study indicated the processing of their data in the presence of third parties in the reception of a medical institution as one of the problems. In particular, one transgender woman mentioned in an interview that when registering, the health facility registrar often refers to the transgender woman/man loudly, in the presence of others, by the name indicated on the identity card, despite the fact that s/he is well aware of the patient's gender identity. Accordingly, by addressing in this manner, information about the patient's gender identity becomes known to others regardless of the patient's desire not to disclose this information.

"When registering with a medical institution, being called by a name that doesn't match your appearance is a huge stress for transgender people," - a member of the LGBT+ community.

KEEPING A MEDICAL RECORD

Improper storage of medical records was identified as a problem.

It was noted that the medical records in medical clinic (where all data related to the collection of anamnesis are entered) are kept open and any person working in the clinic has access to these documents.

In addition, in certain clinics, including Evex sometimes these documents are placed in a place accessible to other patients. In particular, they are placed on the doctor's desk, and accordingly, information about the visits and examinations of the patients specified in the document is available to anyone entering this room.

MEDICAL CONSULTATION IN THE PRESENCE OF OTHER PERSONS

Within the framework of the study, one of the problems indicated by individuals interviewed, was the provision of consultations in the presence of other individuals (other doctors, assistants, other patients).

It was indicated that there are cases when interns are in the doctor's office upon arrival, about whom the patient is not informed in advance. Nor does the doctor obtain permission for their presence later during the medical procedure.

In addition, it was noted that the infrastructure of some medical institutions is arranged in such a way that it is impossible to maintain confidentiality. In particular, there is more than one doctor in one office, who simultaneously receives patients. Accordingly, information provided to the doctor by an LGBT+ person is heard by another doctor in the same room (in best case), as well as by a patient who is in the same room with another doctor for consultation.

MEDICAL CONSULTATION IN A ROOM WITH AN OPEN DOOR

One of the problems identified by the LGBT+ community members and organizations protecting the rights of the LGBT+ community members is that doctors consult patients in a room with an open door. In this way, the information provided to the doctor by members of the LGBT+ community (about health status, sexual orientation, gender identity) becomes available to other patients awaiting the same doctor, who are usually constantly near the doctor's room.

> "The psychiatrist received patients in the room where the door was open. Waiting chairs were also located near the door and all citizens (patients, third parties) being there could hear the information that the LGBT + person gave during the consultation. This seemed to be a common practice in this clinic,"– a representative of the organization Women's Initiatives Supporting Group (WISG).

It was also noted that other doctors and citizens enter the open door without hindrance, which is also a serious problem for the community members in terms of protecting their data.

COLLECTING EXCESSIVE AMOUNTS OF INFORMATION

One of the problems indicated by members of the LGBT+ community and organizations working on the rights of the LGBT+ community is that doctors ask questions about details that are not needed for providing medical services.

"Sometimes the medical staff asks patients questions about their sex life: "Tell me, who is your partner?" etc. All this is sometimes heard by surrounding people and therefore, special category of data of these patients becomes available to them. Due to such cases, it is even unbearable for representatives of the LGBT+ community to go to a medical institution,"– a representative of the organization Equality Movement.

VIDEO RECORDING

Within the framework of the study videotaping by medical workers was also mentioned. In particular, one of the interviewees stated that a beaten transgender woman, taken to the New Hospital by an ambulance, was harassed by the clinic staff and filmed on a mobile phone.

DISCLOSURE OF INFORMATION

Most of the persons interviewed in the framework of the study noted that representatives of the LGBT+ community often express their concern about the disclosure of information about patients' health by doctors of various medical institutions, laboratories, consciously or unconsciously.

One form of information disclosure by doctors is the transfer of patients' special category of data to other doctors/clinic staff and voicing in their presence.

One of the interviewed lesbians mentioned that about 2 years ago she was examined by a gynecologist in Batumi, in a multidisciplinary medical institution - "Med Center". The examination room was a single space in which the so-called gynecological examinations were located behind a "screen" (moving curtain), however, the door of the examination room was open and many people (medical personnel, patients) entered and left the room. During a conversation with a doctor, a lesbian had to provide information about her sexual orientation and relationship, listening to which, the doctor got angry and started speaking loudly that s/he had never heard of such a sexual relationship (with an emphasis on details) before. By doing so, the doctor made available the information about the lesbian woman to the persons present in the same room, beyond the curtain. The same gynecologist performed the "coming out" of the lesbian woman in the presence of other doctors and patients in another room, namely the ultrasound room, during the ultrasound examination of the lesbian woman, where there were many employees of the clinic and patients were moving around.

A transgender woman mentioned that she was undergoing hormone therapy, so she went to the David Tatishvili Medical Center to get a prescription. On a subsequent visit to the same clinic, all the reception staff asked her about starting hormone therapy ("what are you doing with hormones, did you buy them?") when they should not have known about it.

The problem of data disclosure was also mentioned in relation to a dentist. In particular, one of the representatives of the LGBT+ community, who was in the dental clinic for services, informed the dentist about his/her HIV-positive status (since, in this case, the clinic should take appropriate measures - use special tools, disinfect them). After leaving the clinic, the community representative had to return to the clinic as s/he left the document in the dentist's office. When s/he returned, s/he witnessed a dentist talking on the phone saying to the interlocutor (colleague) that he had an HIV positive patient on a visit indicating the relevant personal data. The interviewee mentioned that the representative of the community applied on this issue to the Professional Development Council of the Ministry Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs, which after about 2 years found the violation and issued an oral warning to the doctor.

Disclosing a special category the data of patients in the presence of other patients (in the corridor, in the hospital reception, in the ward) was named as one of the forms of disclosure of information by doctors.

"It is a very common practice for medical staff to voice personal information from the room to the corridor. I heard, for example, about the fact that a doctor publicly, in the presence of others, said: "A man with AIDS has come," – a member of the LGBT+ community.

"In one of the psychiatric hospitals, there was a case when a doctor publicly, in the hospital's reception, in the presence of third parties, disclosed information about previous visits of a member of the LGBT+ community who was on the verge of suicide to the same medical facility," – a member of the LGBT + community.

"The doctor disclosed information about my gender identity to other patients. In particular, the doctor spoke about my gender identity in the ward where other patients were present," – a member of the LGBT+ community.

"There was such a case in one of the clinics, when a lesbian who was awaiting abortion was called in the corridor to enter the doctor's room in such a form - "abortion, come in,"– a member of the LGBT + community.

According to one of the interviewees, cases of disclosure of personal data by doctors are frequent at the LLC Alexander Aladashvili Clinic. For example, there were cases when an ambulance brought a representative of the LGBT+ community to the clinic and a doctor on the outer perimeter used to call down that there was nothing serious with him, at this stage he needed to have an injection and continue taking medications for HIV infection. According to the same interviewee, because of such cases, transgender people avoid this clinic and refuse that the ambulance brigade transfer them to the aforementioned clinic.

Disclosure of information about the gender identity of transgender people who changed their first and last name, but did not change gender, was indicated as one of the problems.

"I have changed my first and last name. The ID shows woman's name, but I didn't change the gender. Thus, the entry about the gender in the identity card is male. There was a case, when I was transferred to the Tbilisi Marine Hospital by an ambulance team where the doctor addressed me "Mr...." during an X-ray. This form of address made my belonging to a trans group recognizable to others," – a member of the LGBT + community.

One transgender woman noted that her doctor ignored her request to be called by a name that matched her appearance and revealed information about her gender identity.

"I was attacked on the street, so I called an ambulance. At that time, I had not officially changed my first and last name. Therefore, I had a man's name on my ID card, but I actually had a woman's name. The emergency medical doctor asked my real name. I told him/her quietly so the others wouldn't hear. The doctor deliberately announced my real name and family name and informed everyone being there about me. I lodged a complaint against the emergency doctor and s/he was dismissed because of it," – a member of the LGBT+ community.

Disclosure of health data through social networks was indicated as ane of the challenges.

LLC Alexander Aladashvili Clinic published on its official Facebook page the personal data of a transgender woman: her first and last name (which were indicated on her identity card and by which her relatives knew her), as well as information about her state of health (medical complaints, examination results, doctors' conclusions). The transgender woman filed a complaint about the above violation with the Personal Data Protection Inspector, whereby she challenged two violations: so-called "coming out" by the medical institution (since the post published by the medical institution contained the name and

family name used as the pseudonym by the transgender woman, as well as the name and family name indicated on the identity card) and disclosure of health-related information. Also, since there was a risk that the relatives of the transgender woman could access the statement (so-called post) disseminated by the medical institution in social media and the information contained in it, the transgender woman immediately applied to the medical institution with a request to delete it. The Personal Data Protection Inspector found the medical institution to be liable in the part of the disclosure of health data and instructed it to delete the post.

There was also a case when a doctor of the clinic made the information about the treatment of a transgender woman public in response to the criticism expressed against the clinic in a social network (which was about the conditions created against the transgender woman in this clinic).

DATA PROCESSING IN JSC SCIENTIFIC-PRACTICAL CENTER FOR INFECTIOUS PATHOLOGY, AIDS AND CLINICAL IMMUNOLOGY

The majority of interviewees within the framework of the study indicated that the most problematic medical institution in terms of data protection is the Scientific-Practical Center for Infectious Pathology, AIDS and Clinical Immunology (hereinafter referred to as the Center), while this center has the highest number of referrals from the LGBT+ community members, both for medications and various medical services, and this center processes the most sensitive data related to HIV infection/AIDS.

The persons who participated in the study identified a number of data protection concerns regarding the Center.

"The Center is the most problematic for representatives of the LGBT+ community in the medical field. This Center has many bad practices. Here, on the one hand, the so-called "coming out" and on the other hand, disclosing the diagnosis of HIV infection is problematic,"– a representative of the organization Women's Initiatives Supporting Group (WISG).

"Medical workers of the Center do not care about personal data and do not feel that it is necessary to protect this data,"– a member of the LGBT+ community.

First of all, complaints made about the infrastructural arrangement of the Center should be mentioned.

Persons interviewed within the framework of the study stated that the form of separation of spaces in the Center leads to the automatic disclosure of a special category of personal data: for HIV-infected people and beneficiaries participating in the HIV prevention program, a separate space/room is allocated from which medicines are taken out. Therefore, everyone knows that a person coming out of a certain room has taken particular medicines. According to the community members, this leads to the disclosure of information about their disease ("If you take drugs, then you use them").

"Medication information is also personal information (what medications you take) that a community member may not want to share with others. Therefore, it violates the confidentiality of information about an LGBT+ person,"– a member of the LGBT+ community.

"If you are standing/waiting in this space and someone sees you, it already means that you are HIV positive and are waiting for a medication. There was a request that both categories of beneficiaries be served in one space in order that the"space for the infected" disappear and there were no cases of "coming out", but this practice has not changed to this day,"– a member of the LGBT+ community.

"Since the medicines are given only to beneficiaries, it is clear to me that people standing in the respective line are HIV positive. I saw my co-worker in line and that's when I found out that he had HIV/AIDS,"– a member of the LGBT+ community.

Regarding the infrastructure of the Center, it was also noted that there are not sufficient rooms for doctors and several doctors can be accommodated in one room. During a consultation with one doctor, the entire medical history of an LGBT+ community member, test results, etc. becomes available to at least one more doctor who is constantly present. There are also cases when several patients are simultaneously in the same room and hear about each other almost everything that is being said in this room.

"Announcement of the test results in the presence of other persons is frequent. There were cases when several people were tested at the same time. Also, sometimes the medical staff asks the patient questions about his sexual life. All this is heard by the surrounding people, and, accordingly, a special category of data of these patients become available to them,"– a representative of the Equality Movement.

Complaints were also made about patients being received in a space with the door open; there is always a queue outside the room, and the conversation between the doctor and the patient is usually accessible to people standing in line.

Disclosure of data by the Center's medical staff to third parties was also mentioned as a problem. It has been noted that it is frequent for doctors to publicly talk about personal data of the LGBT+ community members, as well as calling out names names, family names of patients, information about HIV status in the corridor (for example: "do you remember that this is Givi is positive?", Etc. .), and there is always a queue in the corridor. Accordingly, the information voiced by the doctors becomes available to the people present there.

"Any person who is interested in the HIV status of other people, will receive a large amount of information about people suffering from this infection by coming to the Center,"– a member of the LGBT+ community.

"While accompanying a beneficiary, I often had a case when a medical worker of the Center called a patient from the ward who was standing in line or went out into the corridor and, in the presence of others, announced information about the HIV status along with the name and family name (that s/he is HIV positive or suspected of being HIV positive and needs to be re-tested),"– a representative of the organization Equality Movement.

"I was standing in the waiting room of the Center when one of the doctors called the patient's name and mentioned the result of the CD4 analysis. The CD4 test is usually taken by an HIV-positive person," – a member of the LGBT+ community.

It was noted that it is also problematic to disclose the diagnosis of HIV infection/AIDS, including to the patient's family members by the Center's medical staff.

"There was one case when a representative of the LGBT+ community came to the Center for HIV/AIDS testing. A clinic representative (doctor or nurse) who knew the community member's mother, contacted her by phone and informed her about her son/daughter's visit to the Center and HIV/AIDS testing," – a member of the LGBT+ community.

The issues of protecting the confidentiality of health records were also revealed.

"I applied to the AIDS Center after the results of the test. The medical worker had a list with the names of the patients and information about their HIV status (who was positive and who was negative) in front of her/him. Therefore, anyone could easily read the identity of a particular person on the list and information about their status," – a member of the LGBT+ community.

The interviewees also noted that when dispensing medicines to beneficiaries diagnosed with HIV/AIDS, the Center kept a journal where all persons receiving medicines put their signatures next to their names. Data on other beneficiaries who signed the journal was available to the recipient of medicine, who came before the latter for medicine and signed the journal on the same page. Sometimes a staff member of the Center would cover the paper and no data other than the signature box could be seen, but the names and family names of some beneficiaries were fully/clearly written in the signature box. Therefore, the recipient of medicine became aware of the data of other beneficiaries infected with AIDS. This practice was changed a few months ago, and now the signature is recorded electronically on the monitor, where other people's data is no longer visible. It should be noted that most community members do not have information about the cancellation of the journal (which can be one of the obstacles for community members to refer to the Center, since this issue has been identified as one of the serious problems).

CONCLUSION

The study showed that medical institutions process data of the LGBT+ community members in violation of the Law of Georgia on Personal Data Protection.

In particular, in some cases, data is processed in violation of the principles of data processing, as a result of which their dignity is impinged (publicly emphasizing the patient's gender identity, announcing the patient's diagnosis in the corridor, discussing the details of his/her intimate life with others); also, excessive amount of data is processed, which is not needed to receive medical services (request for information about the identity of the partner).

In some cases, data is processed without legal grounds (photography of LGBT+ people with mobile phones, disclosure of data through social networks, disclosure of information to third parties, including family members, other doctors/clinic employees, patients).

In most cases, proper organizational and technical measures to protect data security are not taken - data is not protected from unauthorized or accidental disclosure and use (case stories and medical records of patients are available to third parties, dialogue with a doctor is conducted in an open door and/or in a room in the presence of other doctors and patients, medical services are provided in such premises, which in many cases leads to the disclosure of information regarding the health status of members of the LGBT+ community and/or so-called "coming out").

In addition, often when receiving written consent from a medical institution, LGBT+ people are not properly informed about the processing of their data, whereas for the consent to be valid, the consent must also be based on familiarization and understanding of the facts and the consequences that will arise as a result of the consent of the data subject in respect of data processing.

Individuals interviewed within the framework of the study noted that the lack of protection of personal data by medical institutions and medical workers, among many other problems, leads to the refusal of the LGBT+ community members to receive necessary medical services and participate in specific programs, which ultimately has a negative impact on the health of LGBT+ person and the normal functioning and efficiency of the system.

Representatives of the organizations working on protecting the rights of the LGBT+ community members noted that due to numerous cases of disclosure of data and distrust towards medical workers,

representatives of the LGBT+ community often clarify information with the organizations protecting their rights: how information about their consultation with a doctor will be protected, whether a doctor has the right to disclose the information about the consultation to the patient's mother or other relative. And, due to fear of disclosure of information, in the absence of appropriate trust, they may not turn to a specialist at all or turn to a specialist on time.

It was also mentioned that in order to avoid 'coming out", transgender people often avoid going to medical institutions and resort to self-treatment, which sometimes ends in negative consequences for their health.

Based on the foregoing, medical institutions and healthcare professionals should approach the processing of personal data of LGBT+ persons with particular care. It is necessary to protect the confidentiality of the information provided by the patient to them and disclose it only when there are grounds provided for by law; process data in compliance with the principles of data processing, including only to the extent necessary for the provision of specific medical services. It is important, when obtaining written consent, to inform the community members about the processing of their data. At the same time, they must fully understand and assess the risks associated with the processing of special categories of data and take adequate and effective measures to protect them.

V. PERSONAL DATA PROCESSING BY PSYCHOLOGISTS

INTRODUCTION

It should be noted that the LGBT+ community members, given their vulnerability and needs, often have to resort to the services of a psychologist. The information voiced by LGBT+ persons during a visit/session with a psychologist mainly concerns such details of personal life as perception of one's own body, sexual orientation, intimate details of sex life, isolation from society, discrimination at work, violence, course of treatment, etc. Illegal/accidental use or disclosure of the data, given its sensitivity, may cause particular harm to LGBT+ people.

Thus, the psychologist is obliged to take into account the rules provided for by the Law of Georgia on Personal Data Protection and process the data of LGBT+ persons if there are relevant legal grounds and in compliance with the principles. The psychologist is also required to protect data confidentiality and take data security measures into account when processing the data.

IDENTIFIED SHORTCOMINGS

Members of the LGBT+ community and representatives of the organizations that protect the rights of the LGBT+ community members, interviewed within the framework of the study, indicated that psychologists, in the course of their professional activities, have certain problems in protecting the confidentiality of data of LGBT+ people.

It has been noted that sometimes psychologists directly or indirectly disclose information about their patients and stories told by patients.

"Quite often, psychologists in interviews, social networks (so-called posts) and in their articles/ books tell stories of patients where the names and family names of patients are not indicated, however they tell stories in such detail that patients can be indirectly identified. Sometimes psychologists get the consent of the patients, but even with their consent, it is not justified to publicize such stories, " – a representative of the Women's Initiatives Supporting Group (WISG).

There have also been references to cases in which the psychologist shared information disclosed by the patient with another person, for personal gain or personal acquaintance.

"One of the psychologists who worked with representatives of the LGBT+ community tdisclosed information voiced during the session other people. S/he used these stories to her/his own advantage. By the way, this person now works as a psychologist in one of the government agencies and continues to work in this direction," – a representative of the organization Women's Initiatives Supporting Group (WISG).

"Mother brought an LGBT+ person to a psychologist she knew. After the sessions, this psychologist told the patient's mother about the news of her son/daughter," - a representative of the organization Women's Initiatives Supporting Group (WISG).

One of the interviewees recalled a case when a psychologist was attending a NGO meeting with a member of the LGBT+ community whom s/he had previously counseled. The psychologist, in the presence of others, started speaking with the community member about the issues discussed during the consultation, thereby disclosing his/her personal information.

CONCLUSION

The above facts indicate that psychologists tend to violate confidentiality of the LGBT+ community members, including in a way that degrades their dignity. This is contrary to applicable law and constitutes a gross interference within a person's private life. Members of the LGBT+ community who disclosed intimate details of their personal lives to a psychologist, had a legitimate expectation that the information they disclosed would be protected from disclosure to third parties.

Facts like the above lead to a weakening of trust in psychologists. LGBT+ people may no longer turn to them for services when needed.

Interviewees noted that there are already obstacles for representatives of the LGBT+ community to contact a psychologist as homophobic attitudes on the part of psychologists are widespread. Thus, the fear of disclosure/publicity of data creates additional barriers for the community members to use the services of a psychologist.

That is why psychologists must comply with the Law of Georgia on Personal Data Protection, including, in case of reasonable necessity, assess the risks associated with the processing of data of the LGBT+ community members and make a decision to disclose data only in full compliance with the requirements of the law.

VI. PERSONAL DATA PROCESSING BY LAW ENFORCEMENT AGENCIES

INTRODUCTION

The activities of the law enforcement agency - the Ministry of Internal Affairs of Georgia (hereinafter referred to as the Ministry) are related to carrying out of various police activities and investigation of crimes. When performing these functions, the Ministry processes voluminous information of the participants in the process, including personal identification data, contact data, fingerprints, as well as information about sexual orientation, gender identity, criminal record, victim status, state of health, which belong to a special category of data. When processing personal data by the Ministry, there is often an interference with the privacy of a person. In addition, within the framework of the powers assigned by law, the Ministry has the ability to receive, use, transfer and otherwise process data from both open and hidden sources, which, in turn, increases the risk of illegal, improper and excessive processing of data.

Illegal processing of such data can significantly infringe on the rights of the LGBT+ community members: degrade their dignity and damage their reputation and/or stigmatize them, result in discrimination against them, violence, etc.

The Law of Georgia on Personal Data Protection applies to the processing of data by law enforcement agencies, except for the exceptions provided for by law. [15] Therefore, the law enforcement agency is

15 *Pursuant to paragraph 6 of Article 3 of the Law of Georgia on Personal Data Protection, Article 6 of this Law does not apply to the processing of data for the purposes of public security, operative-investigative activities and investigation of crimes if the issue is directly and specifically regulated by the Criminal Procedure Code of Georgia or the Law of Georgia on Operative-Investigative Activities or other special law.*

obliged, including during the investigation, to carry out relevant investigative and procedural actions, taking into account the legislation on personal data protection and to process the data of LGBT+ persons only in cases of a specific need, in case of necessity, in compliance with the principles of data processing and security measures. Law enforcement officials granted access to personal data, in order to perform their duties, are required to process such data only for these purposes and to protect their confidentiality.

IDENTIFIED SHORTCOMINGS

Members of the LGBT+ community, interviewed within the framework of the study and the representatives of the organizations protecting the rights of the LGBT+ community members pointed out a number of shortcomings in the processing of personal data in the Ministry: violations of both the grounds and the principles of data processing. In addition, they spoke about the lack of measures taken by the Ministry for the purpose of data security and about the violation of security rules by employees of the Ministry. The lack of use of the mechanism provided for by Article 104 of the Criminal Procedure Code (inadmissibility of disclosure of investigation data) in criminal cases containing sensitive data was indicated as a problem.

INTERVIEW IN THE PRESENCE OF OTHERS

Conducting the interviews in the presence of others was cited as one of the challenges. In particular, it was noted that in police stations, as a rule, LGBT+ representatives are interrogated in a common space where other investigators and citizens are present. A number of cases of breach of confidentiality and disclosure of personal data are related exactly to the interview process in the common room of police stations.

During the interviews, members of the LGBT+ community disclose information about their first name, last name, sexual orientation, gender identity, and the community members do not want this information to be heard by anyone other than the investigator. It was also noted that interviews are conducted in such spaces with representatives of the LGBT+ community who have become victims of sexual violence. Thus, they have to talk about the details of the case in front of other people. In addition to the fact that this is a violation of the law, it is associated with a lot of stress for the community members.

> "In the Ministry of Internal Affairs, it is common for other investigators to attend the interview of the LGBT+ community member. This issue is especially problematic and sensitive for people who haven't "come out" – a member of the LGBT+ community.

It was also noted that sometimes the process of interviewing could take place in a secluded (rather than shared) room, but still other police officers were present and the entrance and exit of others into the interrogation room was not restricted.

> "A friend of mine who is a member of the community was the victim of sexual abuse. I was a witness in this case. We were taken to the interrogation room, although there were too many people present. Questions were asked during the interrogation, including about the details of the rape. I objected to the interrogation in the presence of other persons. Because of this, my friend (the victim) felt unwell and we postponed the interrogation. During the subsequent interrogation, the victim was already accompanied by a lawyer and the process took place in a more adequate environment," – a representative of the NGO Identoba Youth.

The presence of other investigators during the interview process makes the data available to unauthorized persons, who, in turn, may use the information for non-official purposes.

"There used to be a case when a police officer (who was not involved in the case of an LGBT+ person, although worked in the same department where s/he was interviewed) wrote to the community representative on his/her mobile phone number and reminded of the fact that s/he was in the police station ("hey ok, I know everything, aren't you the one who was beaten and who was with us the other day?" Because of such facts, community representatives often do not address the police," – a member of the LGBT+ community.

Cases when, in addition to other police officers, citizens are also present during the interview process was identified as an additional problem by the LGBT+ community members.

"It is one thing when other police officers are present during the interview, another thing is when citizens are also present in this space. This problem exists in almost all district police departments, with the exception of the building of the Ministry of Internal Affairs on the Kakheti highway where it is possible to use an isolated room upon request," – a representative of the organization Women's Initiatives Supporting Group (WISG).

"In the 2nd department of the Batumi police, the investigator asked a minor in a crowded room if s/he was a representative of the LGBT+ community and demanded an explanation," – a representative of the NGO Identoba Youth.

"In one case, three representatives of the LGBT+ community were interviewed at the police station (one of them had not"come out"and one of them was a minor) in connection with a homophobic threat. Next to them in the same space, in parallel to their interview, a minor girl who was a victim of domestic violence was being interviewed. Their personal data became available to one another. The Organization contacted the Human Rights Protection Department of the Ministry of Internal Affairs and provided information about the police station and the time of the interview, however the response provided is unknown to the Organization," – a representative of the organization Equality Movement.

"In one of the cases, when the investigator was questioning and an LGBT+ person was speaking about the sexual violence against him/her (s/he had not "come out"), another woman was being interviewed at the same time in the same space in a fraud case to whom the information became available about the details of the LGBT+ person's case," – a representative of the organization Equality Movement.

According to the interviewees, a huge problem is faced by transgender people, voicing the name of whom as per identity card in front of many people identifies them as transgender people (due to the inconsistency of the visual/external expression with the official name. For example, a person has a man's name and looks like a woman).

"There was a case when two transgender women approached the police department with a request to start an investigation into theft. Since their external appearance did not match the names on the ID card, one police officer pointed this out to another police officer with the following words - "look at their names and what they look like" and started mocking them. Due to this, the entire department heard information about their gender identity. Had the police officers refrained from disclosing the names indicated on the identity card, no one would have realized that they were transgender women, " – a representative of the organization Equality Movement.

It was also noted that sometimes during the interview, police officers check all the information about this person in the databases, and the data indicated in the database (for example, on the imposition of an administrative penalty) are announced aloud in the presence of citizens present.

"I was often told at the police station that my old administrative offenses appeared in the database. Special emphasis is made on May 17 to emphasize my gender identity or sexual orientation. The information is given out loud, for example, with the following remark: "Oh, you have an administrative offense." You were arrested on May 17. Were you painting a flag on the wall?..." Moreover, this sometimes happens in the presence of others, including persons accompanying me, who sometimes do not know about my old administrative offenses at all," – a member of the LGBT+ community.

The persons interviewed in the framework of the study indicated that they sometimes request the interview process to be held in a separate room, especially in relation to cases where information about health status, sexual orientation, gender identity or other sensitive details of personal life should be disclosed, however, in some police departments, there is no possibility to separate such rooms.

"In one case, an additional questioning of a transgender woman involved in sex work in a case of sexual violence took place in the police station, in a common room where the TV was turned on and 50 people were present. The lawyer of the transgender woman suggested to the investigator that the interview take place in the room of the head or the deputy head of the department but was told that there was no free room," – a representative of the organization Equality Movement.

INVOLVEMENT OF SEVERAL INVESTIGATORS IN THE INVESTIGATIVE PROCESS

One of the problems indicated is the informal participation of several police officers in the investigation process, including before the start of the investigation - at the stage of receipt of the complaint.

"In the police station, I was interviewed by different people regarding the same fact: first, the district inspector, then the head of the department, as the district police officer explained to me that in order to receive this complaint, the permission of the head was needed. Also, people unknown to me attended the interview (the head of the department told me that they were his deputies), which is an additional problem in terms of data protection. The main reason why the community members do not apply to the police is that they "come out under duress", not only the case investigator, but also other persons are involved and/or attend the interview, so that the community members do not know who they are and why they should disclose the case details to every person" - a member of the LGBT+ community.

It was noted that if the interview takes place in a common space, usually all the investigators present participate in the interview process and ask questions. There are cases when an interview with a representative of the LGBT+ community is not conducted in a common space, s/he is taken to another separate room, although other people still participate in his/her interview.

"A representative of the LGBT+ community, who came from the region and had not "come out", applied to the police about the fact of extortion and sexual violence. Before receiving his statement, the mentioned person was first interviewed by the head of police, then by his deputy and then by two investigators who were to be involved in the case. All of them inquired about the details. It turned out that these two investigators were no longer available to investigate the case and another investigator was involved in the case. Thus, it turned out that at least five people participated in the interview of the LGBT+ person and had detailed information about his/her personal data while the investigation had not even started," – a representative of the organization Equality Movement.

"There were frequent cases in the Kutaisi police when the case investigator called another employee during the interview of a community member (allegedly for help, but in fact - with the motive of listening to the testimony), while the representative of the LGBT+ community testified about personal and sensitive issues (violence, threats. Repeating this and especially telling to several people is even more difficult for them," – a member of the LGBT+ community.

The frequent change of investigators in a criminal case, as well as the conduct of investigative actions by different investigators, was indicated as a problem. By this, the story of a LGBT+ community member, including information about his/her sexual orientation, gender identity, becomes known to several people, which increases the risk of illegal processing of this data and violation of privacy. It was noted that this is especially problematic in regions where everyone knows each other. Accordingly, in view of the interviewees, in order to avoid cases of data disclosure, the number of investigators in specific criminal cases should be kept to a minimum.

"The number of investigators in specific criminal cases should be reduced to a minimum. This does not imply complex cases where several investigative actions have to be carried out. For example, in a case related to Article 126 (violence) of the Criminal Code of Georgia, there is no need to involve five investigators and conduct different investigative actions by different investigators," – a representative of the organization Equality Movement.

"There was one case where the case of an LGBT+ community member involved sensitive details (s/he had HIV status, was involved in sex work and relatives did not know about his/her sexual orientation). When the community member came to the first interview, s/he was interviewed by one investigator and at the second interview, there was another investigator. This caused outrage in him/her because s/he did not want another person to get to know the details of his/her case. The female investigator sitting nearby told him/her as a reply that they all were investigators and everyone knew everything about each other's cases," – a representative of the organization Equality Movement.

AVAILABILITY OF PROTOCOLS OF INVESTIGATIVE ACTIONS TO THIRD PARTIES

Placing interview protocols on the investigator's desk, in a visible place, in a form accessible to third parties was indicated as one of the challenges in terms of data protection.

"Protocols are placed on the investigator's desk in such a way that in many cases you can easily read what a particular person testified with his/her personal number, name, family name, date of birth. A similar problem exists in all police departments. During the interview in the past days, the interview protocol was placed on the investigator's desk in which not only the demographic data of the participant in the process, but also the entire content of the testimony was available," – a representative of the organization Equality Movement.

INFORMATION DISCLOSURE

Shouting to one another about the arrival of the community members to the police among police officers (from room to room, from floor to floor) was indicated as one of the problems. One of the community members noted that such a situation exists in almost all police stations in Kutaisi. This echo leads to the so-called "coming out", especially when the visual side of the community member does not match his/her official name. It was also noted that during such a conversation between police officers, the circumstances of the criminal case are frequently mentioned (for example, "s/he came from "Identoba", the one who was hit on the head").

"I have witnessed many times shouting among police officers when they inform each other about the arrival of LGBT+ persons to the police. A few months ago, I witnessed an attack on LGBT+ people and when I went to the police station with other members of the community for the interview, the police officers announced - the LGBT+ community members have come," – a member of the LGBT+ community.

Also, asking the LGBT+ community members and the organizations protecting their rights questions about other members of the community by the investigators of the Ministry (for example, mentioning specific names and family names and asking if they know them as members of the community or as partners) was identified as a problem. It was also noted that sometimes police officers, publicly, in the presence of the member of the community, other citizens or investigators, ask a lawyer accompanying the community member about other members of the community whose interests they represent in the same department (for example: "will you bring him/her (name and surname?").

Disclosure of information about the circumstances of a criminal case by police officers to other persons was also highlighted as one of the problems. A reference was made to the case when a transgender woman was interviewed by an investigator who told the details of a criminal case of another transgender woman. A case was also mentioned about providing information on a victim to a medical worker.

"A member of the community who became a victim of violence on homophobic ground, was brought to the clinic. The police came to the clinic to interrogate this person and told the medical staff why s/he had been beaten," – a member of the LGBT+ community.

It was also mentioned that sometimes police officers when meeting LGBT+ persons in another place mention such details in the presence of third parties, that lead to their so-called "forced coming out" and disclosure of other personal data.

"There were cases where a police officer met a member of the community in a public place, greeted (introduced) him/her in the presence of others and reminded them in what circumstances they had met," – a member of the LGBT+ community.

Access to the unified data bank of the Ministry of Internal Affairs for non-official purposes and the disclosure of information about sexual orientation and gender identity and its use for personal purposes was indicated as one of the problems.

"The transgender woman's brother had a fiancée who was the daughter of a police officer. This police officer checked the information about her (transgender woman's) gender identity and sexual orientation in the database of the Ministry for non-official purposes (he searched the information electronically in the criminal case) and later disclosed this information (sent the so-called "screenshots" of the database) to the transgender woman's mother. This case was studied both by the Personal Data Protection Inspector and by the General Inspection of the Ministry of Internal Affairs. According to the decision of the Personal Data Protection Inspector, a certain offense was detected, however, due to the expiration of the statute of limitations, administrative liability could not be imposed on the offender. As for the official inspection conducted by the General Inspection, the action of the police officer was considered a disciplinary offense and he was dismissed from his post,"– a member of the LGBT+ community.

A case was also mentioned when a brother received information about his sister's sexual orientation from the Ministry of Internal Affairs (a lesbian was interrogated in a criminal case involving her friends from the LGBT+ community), which later became the cause of domestic violence.

There was also a case when an investigator (who was not the investigator of this criminal case, he only worked in the same department where a transgender woman was interviewed) called his relative and provided information about the gender identity and sexual orientation of an LGBT+ person and other information provided in the course of the investigation.

"I ended up at the police station due to a certain incident. The investigator questioned me in a common area where other investigators were sitting, including the investigator (three tables away) who the next day contacted an acquaintance on the phone and disclosed my gender identity and the information I had provided to the investigation. In particular, he told her that the previous night, a transgender woman with the same family name and living in the same village was in the police station. This person had an incident with a client as she was involved in sex work. The acquaintance whom the investigator called turned out to be my sister," – a member of the LGBT+ community.

Within the framework of the study, a case was mentioned when an investigator disclosed information about the gender identity and sexual orientation of one of the interviewed LGBT+ persons to his/her relative.

"Two transgender women were raped and beaten. An investigation was launched and these persons were questioned at the police station. The case investigator knew a relative of one of the transgender women. The investigator contacted the relative and told him that a relative of his, who was a transgender woman, was involved in a rape case at the police station, and it turned out that he was involved in sex work. The family of this person did not know this information until then," – a member of the LGBT+ community.

According to Article 104 of the Criminal Procedure Code of Georgia, the prosecutor/investigator is obliged to ensure that information about the progress of an investigation is not made public. For these purposes, he has the right to oblige a participant in criminal proceedings not to disclose data on the case without his permission and to warn about criminal liability. If, despite the warning, a participant in the process discloses information about a criminal case, s/he may be held criminally liable under Article 374 of the Criminal Code (disclosure of investigation data).

Within the framework of the study, it was mentioned that although participants in the process can be held criminally liable for disclosing investigation data, disclosure by investigators of the details of a criminal case in many cases is left without response.

The persons interviewed within the framework of the study also noted that in criminal cases in where sensitive data appear, it is important for the investigator to use Article 104 of the Criminal Procedure Code of Georgia and warn the participant of the process about non-disclosure of information in the case. The practice of applying this article to cases of this category is not introduced, whereas a legal basis for its application is present quite often.

INDICATING EXCESSIVE PERSONAL DATA IN A RESTRAINING ORDER

In terms of data protection, interviewees criticized the form of a restraining order. For example, one case was cited where a police officer provided the victim's address in a restraining order. A copy of the decision was handed to the abuser against the background that the victim had requested in the interview protocol and in the complaint that, despite the presence of such a field (until July 2018 the Order №491, dated July 2, 2014 of the Minister of Internal Affairs of Georgia on approval of the forms of the restraining orders and those of protocols of the restraining orders, and on determination of the persons authorized to compile the said forms, included a field on the actual address of the victim's residence), the information about her actual address not to be indicated in order to prevent further violence.

The mentioned fact was also discussed by the Personal Data Protection Inspector, who did not find a violation (on the grounds that the form of the protocol provided for such a field), but pointed out the

importance of having such a mechanism that would ensure that legitimate interests of the data subject be taken into account in the process of filling out the protocol, as the relevant legislation did not provide for the mandatory filling out of the address field in the protocol.

It should be positively noted that on July 13, 2018, by order No. 81 of the Minister of Internal Affairs of Georgia, the forms of the restraining order and the protocol on the restraining order were updated and no longer include the field of information about the actual address of the victim.

VIDEO RECORDING

Within the framework of the study, it was also noted that sometimes police officers film LGBT+ people on mobile phones.

> A member of the LGBT+ community came to one of the police stations to file a statement with a request to start an investigation into the fact of disclosing his/her personal data. S/he was summoned to the head of police where s/he met three people, about whom the head of police told him/her that they were his deputies. In addition to transphobic and various comments, during the conversation, one of the deputies took a video of the applicant with his phone and laughed with the others. The community member applied to the General Inspection of the Ministry of Internal Affairs which informed the applicant that no violation was found, but a warning was issued," – a representative of the organization Equality Movement.

CONCLUSION

The above facts indicate significant problems in the process of processing data of LGBT+ persons in the Ministry.

On the part of Ministry/Ministry employees, data on LGBT+ persons is often processed for unofficial (personal) purposes without legal grounds (checking data in databases for non-official purposes; disclosing the information obtained during an interview of an LGBT+ person and/or other information from a criminal case to members of his/her family, relatives, community members, medical workers and other persons; public disclosure of information about an administrative offense of an LGBT+ person, photographing an LGBT+ person with a mobile phone).

In a number of cases, the processing of data of the LGBT+ community members is carried out in violation of the principles of data processing, including without a legitimate purpose and in a degrading manner (participation of unauthorized persons in the process of interviewing an LGBT+ person; publicly emphasizing gender identity or sexual orientation; inquiries about the details of intimate life of an LGBT+ person who came for an interview in the presence of others).

In addition, in most cases, proper organizational and technical measures to protect data security are not taken: data is not protected from illegal or accidental disclosure and use (before the investigation, as well as during the investigation, several investigators informally participate in the case; in a criminal case, the investigator is often replaced and/or investigative actions are carried out by different investigators); interview of the witness and the victim is carried out in a common room in the presence of other investigators and citizens; interview protocols are placed openly on the investigator's desk and are available to third parties).

This is contrary to the requirements of the legislation on the protection of personal data and is a gross interference in the private life of a person, degrading human honor and dignity.

The failure to use the mechanism provided for in Article 104 of the Criminal Procedure Code to warn participants in the process about non-disclosure of information in criminal cases containing sensitive data was also indicated as a problem.

The interviewees within the framework of the study noted that representatives of the LGBT+ community in the region have constant fear of leaking information from the police and informing their relatives and/or family members about their sexual orientation and gender identity. Therefore, in order to avoid publicity/ disclosure of information about sexual orientation and gender identity, in many cases they refuse to contact the police, especially those representatives of the LGBT+ community who do not have "come out". This fear, which is real in most cases (especially in the regions), is an obstacle in the process of restoring their rights.

Representatives of the organizations protecting the rights of the LGBT+ community members noted that if a representative of the LGBT+ community living in the region decides to contact the police on a specific fact, in order to avoid disclosure of data, the organization applies to the Department of Human Rights Protection and Investigation Quality Monitoring of the Ministry of Internal Affairs in advance requesting that appropriate environment in the police station be set and his/her personal data not be publicized. Sometimes the involvement of mentioned department is enough to convince members of the community to apply to the police, but sometimes even this intervention does not work given that the fear of disclosure of data is high.

Such facts have negative impact on the implementation of the rights of LGBT+ persons and the effectiveness of investigation carried out by law enforcement agencies, as well as reduce the trust of the LGBT+ community and society in law enforcement agencies.

Therefore, the Ministry and employees of the Ministry should treat the processing of LGBT+ data with special care and attention and collect, use, disclose and otherwise process data only if there is an appropriate legal basis and legitimate purpose, in accordance with other data processing principles determined by the Law of Georgia on Personal Data Protection. In addition, the Ministry should assess the risks associated with the processing of personal data of LGBT+ persons and take adequate security measures to protect the data.

VII. PERSONAL DATA PROCESSING BY LAWYERS

INTRODUCTION

In the process of protecting the rights of a defendant or other person, the lawyer contacts with various participants in the process, including victims, witnesses, psychologists and social workers. They also have access to the materials of the criminal case. Accordingly, lawyers have access to the personal data of the participants in the process, including details of their personal lives.

According to paragraph "a" of Article 3 of the Law of Georgia on Lawyers, one of the main principles of a lawyer's activity is to act lawfully, in compliance with the current legislation. According to the second paragraph of Article 1 and the first paragraph of Article 6 of the same Law, a lawyer in his activities abides only by the law and the norms of professional ethics; to protect interests of the client, the lawyer has the right to use all means not prohibited by law or the norms of professional ethics.

Thus, a lawyer who processes data in connection with his professional activities is obliged to comply with the current legislation, including the requirements of the Law of Georgia on Personal Data Protection and process the personal data of a person only if there are grounds provided for by law and in accordance with the principles.

IDENTIFIED SHORTCOMINGS

Interviewed representatives of the LGBT+ community and representatives of organizations protecting the rights of members of the LGBT+ community, indicated that in terms of protecting confidentiality of data of LGBT+ people, certain problems are identified on the part of lawyers in the course of their professional activities.

One of the problems was the disclosure by defense lawyers of personal data about sexual orientation and gender identity. In particular, it was noted that both during the court hearing and in public, lawyers appeal to sexual orientation and/or gender identity of the participant in the process, while this circumstance does not matter for qualification and punishment in a criminal case (a crime is not committed on the grounds of intolerance) and disclosure by the lawyer of the specified information serves only one purpose - to discredit the participant in the process.

Among them, during court hearings, lawyers ask questions about details of personal life that are not related to the criminal case.

"During the court hearing, lawyers often ask questions that are not related to the case. Questions emphasize the witnesses' sexual orientation or gender identity (eg: "Do you have a wife or a husband?", "What is your orientation?"). Unfortunately, the victim and the witness do not have the right to divert such questions. Nor are the lawyers of the victim and the witness equipped with such powers. The role of the judge in this process is passive and therefore it is completely up to the parties to divert irrelevant questions. We warn the witnesses in advance that when asking such questions, they should ask the judge to divert the question and tell them that this is their personal information which has nothing to do with the case," – a representative of the organization Women's Initiatives Supporting Group (WISG).

"In December last year, a victim had been interviewed in court about the events of July 5-6. Many people attended the process (journalists, family members of the defendants, lawyers, others). The defendants were charged with violence (committed under aggravating circumstances), however, the question "whether the victim was a lesbian for a long time" was not relevant to the case. It is welcomed that both the prosecutor and the judge responded to this question - the judge indicated to the lawyer that the question was irrelevant and asked the lawyer not to ask such question again, " - a representative organization Equality Movement.

"In one of the cases, the lawyer disclosed information about the sexual orientation of the witnesses directly during the trial, publicly while this issue had nothing to do with the case. Despite the protests of the witnesses, the judge did not divert questions related to sexual orientation, while the lawyer used this fact to discredit the witnesses," – a member of the LGBT+ community.

A representative of the organization Equality Movement noted that in 2020, in one of the high-profile cases (premeditated murder under aggravated circumstances), the defendant's lawyer publicly informed the media about sexual orientation of the deceased. The organization applied to the Ethics Commission of the Georgian Bar Association with a request to impose disciplinary liability for disclosure of a special category of data by the lawyer. Two and a half years later, the Ethics Commission delivered a decision founding that the lawyer was protecting the client's interests and there was no violation (a complaint to the Data Protection Authority had not been lodged).

The disclosure of data of LGBT+ persons by lawyers through social networks was also indicated as a challenge. In particular, a representative of the NGO Identoba Youth named one of the criminal cases that was considered in the Kutaisi City Court as an example of illegal disclosure of data by a lawyer. The defendant in this case was acquitted, after which his lawyer posted on Facebook and indicated sexual orientation of the victim and his/her sister. In the case of the victim, the name and family name were indicated in the form of initials, however, given that the city is small, and the status mentioned social worker and psychologist, who were witnesses in this case, by their names (it was also indicated that the victim was assisted by an organization that protects the rights of the LGBT+ community members) It became known to everyone who the post was about.

"It is one thing for participants in a process to talk about their sexual orientation in a courtroom, but this does not mean consent or desire to make this information available to the wider public," – a member of the LGBT+ community.

Also, one of the members of the LGBT+ community noted that during the trial, the lawyer provided information stored in a law enforcement agency, to which he did not have access and failed to provide documents on its legal acquisition.

"During the trial, the lawyer presented information on the criminal case started 9-10 years ago (which was discontinued), one of the witnesses in which was a main figure and to which the lawyer should not have had access under any circumstances. The lawyer could obtain this information only from the law enforcement agencies," – a member of the LGBT+ community.

CONCLUSION

The above facts of the disclosure of information by lawyers through the social network and the media indicate that they disclosed information about sexual orientation in an unethical, degrading manner, without the consent of the persons concerned. At the same time, other legal grounds for data processing defined by the Law of Georgia on Personal Data Protection were missing as well.

In addition, it should be taken into account that when giving interviews to the media and/or disclosing information through a social network, this information becomes available to a wide range of people, while, for example, during the trial of a case, it is announced in the courtroom, in the presence of a limited circle of people. The wide availability of information, especially the dissemination of sensitive information such as a person's sexual orientation and/or gender identity, increases the risk of irreparable harm to the data subject.

Based on the foregoing, it is necessary that a lawyer strictly comply with the requirements of the law and disclose a special category of data of LGBT+ people only in exceptional cases provided for by law.

With regard to the disclosure by lawyers of information about the sexual orientation and gender identity of witnesses and victims at open court hearings and the raising of questions aimed at disclosing this information, it should be noted that, according to paragraph 3 (b) of Article 3 of the Law of Georgia on Personal Data Protection, this Law does not apply to the processing of data for the purposes of legal proceedings, as this may prejudice legal proceedings before the final decision of the court. However, in order to ensure respect for private life and dignity, as defined by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Article 15 of the Constitution of Georgia and Article 4 of the Criminal Procedure Code of Georgia, It is important that lawyers ensure that information about sexual orientation and gender identity of participants in proceedings is disclosed at open court hearings and/or questions aimed at disclosure are asked only for a legitimate purpose and in a proportionate amount.

VIII. PERSONAL DATA PROTECTION IN THE PROCESS OF ADMINISTRATIVE AND CIVIL PROCEEDINGS

INTRODUCTION

Court proceedings involve processing of personal data of persons involved in the case, which often contain sensitive details about their personal lives.

In order to exercise the constitutional right to apply to the court, it is essential for LGBT+ people to create appropriate guarantees for the protection of their personal data in court.

IDENTIFIED SHORTCOMINGS

A representative of an organization that protects the rights of the LGBT+ community members noted that members of the LGBT+ community have a problem with the protection of personal data during consideration of cases at the court, since administrative and civil legislation does not provide for their so-called “forced coming out” protection mechanisms.

In particular, the Organic Law of Georgia on Common Courts, the Civil Procedure Code and the Administrative Procedure Code of Georgia do not provide for the possibility of conducting a case in a

closed court session in order to protect personal data,[16] therefore, civil and administrative cases are mainly heard in court in an open court session. It should be noted that such a possibility is provided for by the Criminal Procedure Code (according to paragraph 3 (a) of Article 182, the court may, at the request of a party or on its own initiative, decide to partially or completely close the hearing in order to protect personal data and secrecy).

"I have never had a case where a judge of the Chamber of Civil Cases of the Tbilisi City Court granted a motion to close a trial in an LGBT+ person's case, even if the issue concerned damage caused by so-called "coming out" or other particularly sensitive issues. As for administrative cases, in the case of legal recognition of the gender of a transgender man, the judge took into account the interests of the applicant's minor children and granted the motion to close the court hearing. In the second case of similar content, despite the absence of minors, the judge applied the same practice. However, it is clear that the Chamber of Administrative cases cannot be sensitive to these matters in all cases. Therefore, it is important that civil procedural legislation provide for the possibility of considering a case in a closed court session in order to protect a special category of personal data. Moreover, the so-called "coming out" is one of the main barriers to accessing justice and going to court among the LGBT + community,"- a representative of the organization Women's Initiatives Supporting Group (WISG).

"A transgender woman filed a civil lawsuit against a medical institution seeking compensation for the unlawful processing of personal data related to her gender identity and health. At the preparatory session, the plaintiff applied to the court for consideration of the case in a closed session, but the judge refused to grant the request. Due to the fear of considering the case in an open session, the transgender woman agreed to settle with the medical institution in exchange for compensation," – a representative of the organization Women's Initiatives Supporting Group (WISG).

CONCLUSION

The above facts show that the absence of a guarantee to close a court hearing in order to protect personal data in civil and administrative cases hinders the exercise of the right of LGBT+ people to apply to court due to the fear of disclosure of information about their gender identity or sexual orientation. And, open court hearings, where the harm caused by so-called "coming out" or other issues related to LGBT+ people are considered, quite often become the reason of so-called "forced coming out".

When considering civil and administrative cases containing intimate details of personal life, an LGBT+ person should have the right to demand full or partial closure of a court session if s/he considers that this violates his/her right to privacy and protection of personal data.

Thus, it is important that the Civil Procedure Code foresee the same guarantee as is provided for by the Criminal Procedure Code (the possibility of considering a case in a closed court session in order to protect personal data).

16 *According to paragraphs 1 and 2 of Article 13 of the Organic Law of Georgia on Common Courts, all court cases are considered in an open session. Consideration of a case in a closed session is allowed only in cases provided for by law.*

According to Article 9 of the Civil Procedure Code of Georgia, all court cases are considered in an open session, unless this is contrary to the interests of protecting state secrets. Consideration of a case in a closed session is also allowed in other cases provided for by law, on the basis of a reasoned motion of a party.

Pursuant to part 2 of Article 1 of the Administrative Procedure Code of Georgia, unless otherwise provided by this Code, the provisions of the Civil Procedure Code of Georgia shall be applied in administrative proceedings (certain articles of the Administrative Procedure Code provide for the consideration of a case in a closed court session, but not on the basis of personal data protection).

IX. PERSONAL DATA PROCESSING BY LEPL – PUBLIC SERVICE HALL

INTRODUCTION

LEPL – Public Service Hall processes (receives, stores) personal information of citizens in the process of providing various public services, including changing the name/family name and/or gender. At the same time, the procedure for changing the data specified in the record of the civil act includes submission of documents containing personal data to the Public Service Hall/operator of the Public Service Hall and clarification of issues related to the change of personal data from the operator. During the process of communication, an LGBT+ person may need to disclose information about gender identity, gender reassignment surgery for confirmation of gender. Illegal/accidental use or disclosure of said data may cause particular harm to LGBT+ people, especially if that person has not "come out". Therefore, it is important that the Public Service Hall processes this data in complete confidentiality.

IDENTIFIED SHORTCOMINGS

Members of the LGBT+ community and representatives of organizations protecting the rights of members of the LGBT+ community interviewed within the framework of the study indicated that there are cases of disclosing personal data by the Public Service Hall. However, no measures have been taken to protect data security.

In particular, one of the problems was the protection of the confidentiality of the content of communication with the operator when changing the name and gender in the Public Service Halls. Several respondents noted that the reception desks (where the reception of citizens and the provision of services is conducted)

are located too close to each other which creates a problem when going through the procedure for changing the name and/or gender. In particular, when a member of the LGBT+ community, in case of a desire to change a name and/or gender submits documents to the operator of the Public Service Hall providing the service, the operator asks him/her questions, including clarifying whether this person really wants to change the name and gender record and receives responses that often contain and/or emphasize information about gender identity. This conversation is heard at least by the operator sitting next and the citizen served by the specified operator.

One of the interviewees also spoke about the disclosure of data of a LGBT+person by an employee of the Public Service Hall to a third party.

> "There was one such case about 3-4 years ago when a transgender woman who had changed her name came to the Public Service Hall for a passport. The operator who served the transgender woman was her fellow villager. This employee of the Public Service Hall informed the transgender woman's parents about her altered data and gender identity which caused her very serious problems," - a member of the LGBT+ community.

CONCLUSION

The above facts indicate that in the process of providing services to citizens by operators in the respective spaces, LEPL – Public Service Hall does not have in place appropriate measures to protect data. Therefore, receiving services in such spaces constantly creates risks of illegal or accidental disclosure, acquisition and use of data of LGBT+ people. In addition, the disclosure of data of LGBT+ people without legal grounds, for non-official purposes, in personal interest, contrary to the requirements of the law, is recorded on the part of an employees of the Public Service Hall.

Employees of the Public Service Hall who are granted access to personal data in order to perform their official functions, are required to comply with the requirements of the law and applicable regulations on data confidentiality. [17] In addition, the Public Service Hall must assess the risks of data processing and take appropriate organizational and technical measures to protect their security.

17 *Article 13 of the Order N434/ს of 01 June 2020 of the Executive Director of the LEPL – Public Service Hall "on amending the Order N875/ს of 29 December 2017 on the approval of the internal regulations of the Public Service Hall bylaws " See: https://psh.gov.ge/res/editor/chven_shesaxeb/shinaganawesi_-_2020.pdf*

X. UPDATING PERSONAL DATA WHEN CHANGING ENTRIES ON FIRST NAME/ FAMILY NAME AND/OR GENDER

INTRODUCTION

The principle of data accuracy and validity ("data must be valid and accurate, and must be updated, if necessary. Data that are collected without legal grounds and irrelevant to the processing purpose must be blocked, deleted or destroyed") is one of the important principles of the Law of Georgia on Personal Data Protection which must be taken into account when processing data.

Considering the importance of processing accurate and up-to-date data, data subjects have the legal right to demand the correction, updating, deletion, etc. of their personal data. In particular, according to paragraph 1 of Article 22 of the Law of Georgia on Personal Data Protection, when requested by a data subject, the data processor is obliged to correct, update, add, block, delete or destroy the data if they are incomplete, inaccurate, not updated or if they were collected and processed in violation of the law. In accordance with paragraphs 1-3 of Article 23 of the same Law, the request provided for in paragraph 1 of Article 22 of this Law may be submitted in writing, orally or using electronic means. Within 15 days after receiving the data subject's request, the data processor is obliged to correct, update, add, block, delete or destroy the data or inform the data subject of the ground for the refusal. If the data processor considers, without a request from the data subject, that the data in question is incomplete, inaccurate or

not up to date, it must correct or update the data accordingly and inform the data subject. [18]

The accuracy of the data is necessary to adequately protect the personal information of data subjects. In addition, it should be taken into account that for representatives of the LGBT+ community, it is especially sensitive to correct these data in time in case of a change in the name/family name and/or gender entries, since in most cases, this is related to their gender identity and the issues of so-called "coming out".

IDENTIFIED SHORTCOMINGS

One of the problems indicated by the members of the LGBT+ community interviewed within the framework of the study, was updating their personal data after the official change of name/family name and /or gender (in accordance with the law).

In particular, it was noted that after changing the entries concerning the name/family name and/or gender record, the data is automatically changed in public agencies (for example, in the Central Electoral Commission,where voter lists are updated automatically), and in some public agencies that have access to the electronic databases of the Public Service Development Agency, development of public services, these data are not automatically changed.

For example, a transgender woman who changed her identity card details (name, family, gender entries) came to one of the banks for an installment plan. Her data was updated at the bank, as she had already applied for data change. However, when the bank requested information about the client's income from the Revenue Service, the bank was provided with information containing her old personal data. After the statement of the transgender woman, the Revenue Service corrected her personal data based on the submitted documents. However, processing her inaccurate data endangered the confidentiality of information about her gender identity. In addition, due to the existence of the old data in the Revenue Service, the financial manager of the transgender woman encountered a problem when transferring funds as her current personal data did not match the old data recorded in thedatabase of the Revenue Service.

"A trans man, whose name has been changed, came to one of the medical facilities to get vaccinated against COVID-19. It turned out that he was registered in the database under his old name. Due to the difference in the data, the clinic employee announced the information about the old and new name of the transgender in the corridor, in the presence of everyone, and tried to find out what had happened in the presence of people there. It was so hard for him to emphasize his individuality that he was going to refuse vaccination," – a representative of the organization Women's Initiatives Supporting Group (WISG) organization.

As for private institutions, the interviewees noted that they contact private institutions individually with a request to update the data. In the event of a request (upon submission of a document confirming the change), some private institutions change the data without any problems (for example, banks, educational institutions), and some refuse to update the data.

However, it was noted that members of the community are generally not aware that if data is changed, they should contact private institutions and request data changes.

18 *Pursuant to Paragraph 1 of Article 24 of the Law of Georgia on Personal Data Protection, the rights of a data subject under Article 22 of this Law may be limited by the legislation of Georgia if the exercise of these rights endangers: the interests of the national security and defence; the interests of public security; crime detection, investigation and prevention; significant financial and economic interests of the country (including those related to monetary, budgetary and taxation issues); the rights and freedoms of a data subject and others.*

"When receiving services at one of the banks, a transgender woman was approached with the name written on her old ID card (male name), although she changed her name 2 years ago and her ID card was also updated. The bank staff showed her that no changes had been made to their database. The community member had no information that this data was not provided to the banks by the Public Service Hall and was not updated automatically," - a member of the LGBT+ community.

Updating data in pharmacy chains was cited as an important problem by members of the LGBT+ (transgender) community. It is noted that some pharmacy chains refuse to change the name due to the fact that at the time of taking the discount card another name was recorded. In particular, the interviewees noted that:

- Pharmacy chain "PSP" promptly corrects/updates personal data recorded in their database;
- Pharmacy chains "GPS" and "Pharmadepo" cannot change already registered data, they leave them in the database, issue a new discount card as an exception, however the history of the previous discount card is not transferred.

  In this case, transgender people are warned to present only the new card when receiving services at the pharmacy, because if they provide personal ID number and check against this number in the database (since the personal number is linked to the old data), the old data is detected.

  In addition to facing embarrassing problems many times, this is also a big obstacle for transgender people in terms of using a discount card and benefits as they constantly use medicines and refusing to change their name leads to the annulment of benefits (points) accumulated under the former name;
- "Aversi" pharmacy chain neither corrects the data nor issues a new discount card for the changed name.

Failure to update data by the pharmacy chain negatively affects the availability of medicines - transgender people may refuse to buy medicines in a pharmacy where it is possible for them to get medicines at a better price. And, using its services, due to the refusal of the pharmacy chain to update data, transgender people are forced to hear the name that they officially changed every time they visit the pharmacy, sometimes in the presence of other people. This leads to the disclosure of their gender identity, the so-called "forced coming out".

"Constant recall of previous data is very stressful. A transgender person may refrain from applying to a pharmacy precisely because his/her old data is recorded there," – a member of the LGBT+ community.

It was also noted that members of the community do not have information about which institutions they should address after changing their personal data and what documents they must provide to update their data.

CONCLUSION

The results of the study show that after changing the name/family name and/or gender entries in the Public Service Development Agency, the specified data is automatically changed in some public agencies and some of them are waiting for application of the data subject.

Important gaps are identified in the direction of updating data on LGBT+ persons in private companies. In particular, some pharmacy chains, despite the request of the data subject, refuse to update personal data. Refusal of pharmacy chains to update data in their database, improper updating of data and/or

processing incorrect data by them is contrary to the current legislation and constitutes a gross violation of the rights of the data subject guaranteed by the Law of Georgia on Personal Data Protection. In addition to the legal and practical problems, this often creates inconvenience, causes so-called “coming out” of the community members and is associated with stress due to the fact that when receiving services, they are called by a name that does not correspond to their gender identity.

Taking into account the realization of the rights LGBT+ people and the principle of data accuracy, when necessary, private and public institutions are obliged to ensure that data is updated and processed correctly.

In addition, in order to protect the rights of data subjects, it is important that LEPL Public Service Development Agency take appropriate measures and ensure that data subjects are informed about the procedures for updating data in other public and private institutions after changing entries on name/last name and/or gender.

XI. PERSONAL DATA PROCESSING IN THE WORKPLACE

INTRODUCTION

In the process of labor relations, for the purposes of staff selection, recruitement, health insurance, organizational security etc. voluminous information is processed about a person, including identification and contact information, photograph, education, qualification, evaluation information, data related to criminal record and health status, etc. The processing of data about a person's sexual orientation and gender identity is permitted only in exceptional cases provided for by the Law of Georgia on Personal Data Protection. Therefore, in the process of labor relations, it is essential to properly process and protect the above-mentioned personal data (in the presence of the appropriate purpose and legal basis), since LGBT+ persons may become victims of discrimination and bullying in the workplace due to their gender identity or sexual orientation. The employer must respect the constitutionally guaranteed rights and freedoms of LGBT+ persons, their rights to respect for private life, honor and dignity.

IDENTIFIED SHORTCOMINGS

The absolute majority of persons interviewed within the framework of the study, indicated that the community members in the workplace are forced to conceal information about their sexual orientation/ gender identity, as disclosure of this type of personal information is usually grounds for denial to hire, and the dissemination of this information after employment (the source of which may be another employee) becomes a reason for dismissal.

A number of cases were mentioned when a member of the LGBT+ community was dismissed for dissemination of information about a person's sexual orientation and gender identity at the workplace. However, as a rule, the official reason is always something else and employers never indicate it as the actual reason for dismissal. It has also been mentioned that sometimes a member of the community is forced to leave work given the hostile environment created at work due to this.

"A colleague discovered a female social media account of a trans woman colleague (she worked as a guy but had a female social media account) and told everyone at work about it. Because of the bullying, she was forced to quit the job," – a member of the LGBT + community.

"One of the community members left his job because he faced a difficult environment at work after coming out to his colleagues about his sexual orientation. Because of this, many people try not to disclose this personal data in order to keep their jobs," – a member of the LGBT+ community.

A case was also mentioned, when after the disclosure of information about gender identity, the true reason for the dismissal of a person was directly communicated by the manager to a transgender woman.

"My friend, a trans woman who has "come out" was dismissed from work by the management for the reason that clients would not want to receive services from such a person. Basically, transgender people are not employed at all," – a member of the LGBT + community.

CONCLUSION

The foregoing shows that, upon learning information about gender identity or sexual orientation, employer organizations often dismiss an LGBT+ person, which is contrary to current legislation. The processing of personal data must not be directed and must not give rise to any discrimination in the course of the labour relations.

Regarding the disclosure by an employee of information about the gender identity and sexual orientation of another employee, it should be noted that the Law of Georgia on Personal Data Protection does not apply to the processing of data by an individual for clearly personal purposes, if their processing is not related to entrepreneurial or professional activities. [19]

Based on the foregoing, the employer organization, as well as employees of the organization, when processing data in connection with the implementation of entrepreneurial or professional activities, are obliged to process personal data only in full compliance with the requirements of the law.

19 *Article 3 of the Law of Georgi on Personal Data Protection, see: https://matsne.gov.ge/document/view/1561437?publication=23*

XII. PERSONAL DATA PROCESSING BY THE MEDIA FOR THE PURPOSE OF INFORMING THE PUBLIC

INTRODUCTION

The media play an important role in a democratic society. They are obliged to provide the public with all information and to acquaint them with issues of interest to them. However, journalist's freedom of expression is not absolute.[20] Therefore, maintaining a balance between the right to privacy, the right to protection of personal data and freedom of expression is of fundamental importance in the implementation of journalistic activities, especially when covering interviews involving LGBT+ people, preparing stories, reports, broadcasts about them, given vulnerability of this group and the risk of their stigmatization.

EXISTING CHALLENGES

Within the framework of the study, the LGBT+ community members and representatives of organizations protecting the rights of members of the LGBT+ community pointed out to challenges in terms of protecting the privacy of data LGBT+ persons from the media.

20 *Article 17 of the Constitution of Georgia, see: https://matsne.gov.ge/document/view/30346?publication=36*

In particular, the majority of community members noted that the standard of coverage of representatives of the LGBT+ community has recently improved in the media, although there are still problems in this area. It is noted that the media love to cover the problems of the LGBT+ community more intensively than it really is. It is for this purpose that the personal data of community members are made public.

The interviewees named several examples when the media directly or indirectly identified members of the community during the coverage of a report, broadcast, including by indicating their real names and family names, which brought information about their sexual orientation and / or gender identity to the public.

"In one of the shows, a transgender woman was invited, who had been hiding information about her gender identity in her village. Her visual appearance has changed to the extent that no one would have recognized her. During the broadcast, the real name of this transgender woman was written in the credits. This is how his gender identity became known to her family and fellow villagers. After this show, she could no longer go to the village," - a representative of the organization Women's Initiatives Supporting Group (WISG).

One of the interviewees recalled what an incident that happened several years ago, when information about his/her gender identity became known to public through a TV show.

"My friend was invited to one of the TV programs concerning the attitude towards the LGBT + community. On the recording of the show, I accompanied my friend as a guest. I also told the host of the show that I should not have appeared in the frame at all. During the recording of the program, an incident occurred, in particular, one of the participants in the program insulted representatives of the LGBT+ community, because of which I got into an argument. The program broadcast the entire incident on television, where I was seen, including in my outfit. The show has made available my gender identity, that I am a transgender woman," – a member of the LGBT+ community.

One incident was also mentioned, when a suicide attempt by a transgender woman was covered by the media in an identifiable form.

One problem that was identified is the improperly blurring community members which makes it easy to identify a person. Facts were also mentioned, when a member of the LGBT+ community received a guarantee from a journalist that his/her face would be covered/blurred and the voice changed, but this promise was not fulfilled.

"A few years ago, a TV show featured members of the community who had to tell their personal stories. As agreed, their images were to be blurred and their voices altered. When the announcement of the program came out, the frame was blurred in such a way that community members could be easily identified and their voices were not changed. This promo was available for about 2 hours before we contacted the program and it was replaced," – a member of the LGBT+ community.

Sometimes the media do not show the name and surname of a member of the LGBT+ community, a visual image, although the plot describes such details that make it easy to identify a the community member.

"Several months ago, in the stories prepared about the attack on five transgender people, the place of the attack and the surrounding area (which at the same time was the place of residence of the transgender person) were described in such detail that information about the place of residence of the transgender person became available to the interested person," – a representative of the organization Women's Initiatives Supporting Group (WISG) representative.

It was also pointed out that the place of residence of a member of the LGBT+ community (village, street,

house, apartment, yard) is directly indicated in the media and it is easy to determine which member of the community is being referred to. It was also noted that showing the place of residence is dangerous not only for members of the community, but also for people who have rented/transferred for use the premises and place of residence to community members.

"The last case happened recently, an elderly woman had a transgender women sheltering in her house. The owner of the mentioned apartment told the media that she did not want his close relatives to know about it and would agree to be photographed if her face did not appear in the story and the house was not identified. Despite the request, the story covered the house in such a way that this lady was recognized by her relatives, which is why they called her and cursed her. While there is a threat of violence against community members, such facts are problematic for them. This also creates a problem for people who rent apartments to trans people, especially in the conditions when it is a big challenge for community members to rent an apartment," – a member of the LGBT+ community.

"There was one case when two lesbians were attacked. Information about this was posted on social networks, followed by even more aggression from the public, harsh comments that they should be killed, etc. Community members refused to communicate/interview with the media in order to ensure their safety. The media independently located the lesbians and arrived at the scene. There were many of them and almost the whole district heard why they came. It is also worth noting that one of the lesbians was with a minor child. Residential street, entrance, floor, apartment number of lesbians became available in the stories. In addition, the footage was allegedly blurred, although the faces were identified. These two persons could be identified by anyone who saw this footage and if someone did not know about their sexual orientation, they would have learned about it from these footage. They had to change their address," - a representative of the organization Equality Movement.

Interviewees noted that while events and gatherings with community participation are mostly kept secret from the media in order to ensure security and prevent attacks on community members, sometimes media discloses their location (for example, when covering a demonstration, media representatives at the rally announced the location of the meeting/movement of the LGBT community and provided this information to aggressive groups (for example: "Georgian March") who were searching for the community members.

It was noted that the media should cover the issues of the LGBT+ community with extreme caution, since even if the community agrees, it can be very risky to cover the issue in an identifiable form. A case was indicated when a community representative cooperated with the media, but later requested that the material/recording covered by the media be deleted as the dissemination of information about his/her sexual orientation was followed by negative comments. In addition, information became available to those people with whom the LGBT+ person had not "come out".

"It is difficult to understand in advance what kind of reaction all this can cause and what psychological damage can be caused to a community member by making information about his/her sexual orientation public," - a representative of the organization Women's Initiatives Supporting Group (WISG).

CONCSLUSION

The above facts confirm that the media/journalists often disclose information about sexual and gender identity of LGBT+ people, including without their consent, in inappropriate volume and form (improper blurring of images and voice of LGBT people in a report or a program; sometimes indicating a name/family name; coverage of details of residence/entrance/apartment, nearby territory, as well as other locations; showing an LGBT+ person in a program in an identifiable form despite the promise of confidentiality; showing a suicide attempt of an LGBT+ person in an identifiable form).

Despite the restrictions of the Law of Georgia on Personal Data Protection in respect of the media, [21] it is important that media outlets (journalists) fulfill their obligations in accordance with Article 15 of the Constitution and Article 8 the Convention on the Protection of Human Rights and Fundamental Freedoms to ensure respect for private life. In addition, according to the 10th principle of the Charter of Journalistic Ethics of Georgia, [22] a journalist must respect private life and not interfere with private life unless there is a special public interest. [23]

Journalists should be cautious when disclosing personal data of the LGBT+ people and strike a balance between the right to privacy and personal data protection and freedom of expression to avoid interfering with the privacy of others without a legitimate need, especially when covering highly sensitive issues of LGBT+ persons. [24]

Even if there is a special public interest, personal data of an LGBT+ person should not be disclosed without their consent. However, it is important that journalists consider the manner of disclosing data. Before distributing information, a journalist should properly analyze the negative consequences of disclosure of information for an LGBT+ person and, in accordance with the risk assessment of the potential impact of this information on the personal life of an LGBT+ person, make a decision on the disclosure/non-disclosure of information containing personal data.

21 *Pursuant to paragraph 4 of Article 3 of the Law of Georgia on Personal Data Protection, this Law (except for Article 17) shall not apply to processing of data by media for public information.*

22 *Since 2009, the Charter of Journalistic Ethics has been in force in Georgia, the mission of which is to increase the public responsibility of the media through the protection of professional and ethical standards and the creation of self-regulation mechanisms. see: https://www.qartia.ge/ka/qartia*

23 *Principles of the Charter, see: https://www.qartia.ge/ka/mthavari-gverdis-aikonebi/article/30513-preambula*

24 *In the process of creating the practice of balance, the Charter of Journalistic Ethics of Georgia as a self-regulation mechanism has a special role.*

XIII. DISCLOSURE OF PERSONAL DATA BY THE COMMUNITY MEMBERS FOR PERSONAL PURPOSES AND THEIR AWARENESS ON PERSONAL DATA PROTECTION ISSUES

INTRODUCTION

Members of the LGBT+ community often have more information about each other than is available to non-LGBT+ members. For the purposes of realization of the rights of LGBT+ people, prevention of their so-called "forced coming out" and its consequences (which are often related to violence, death threats, leaving their place of residence, dismissal, etc.), it is important that representatives of the LGBT+ community understand the importance of protecting sensitive data about gender identity, sexual orientation, health and the consequences of publicizing and disclosing such data to third parties. To this end, it is important that LGBT+ individuals have proper knowledge of personal data.

EXISTING CHALLENGES

PUBLIC DISCLOSURE OF DATA BY MEMBERS OF THE LGBT+ COMMUNITY

Members of the LGBT+ community, as well as representatives of organizations protecting the rights of members of the LGBT+ community, noted that community members often disclose information about each other's sexual orientation or other details of their personal lives for personal reasons. Members of the LGBT+ community disclose information about gender identity or sexual orientation of other members

of the community to family members, relatives, neighbors, and even each other's employers, and sometimes, along with providing information, send photos confirming this information through social networks.

"More than half of the cases of so-called "coming out" are carried out by members of the LGBT+ community. Threats to disclosing personal data, blackmailing are generally accepted in the community," – a member of the LGBT+ community.

"One member of the community wrote to another's mother that her son liked boys. In this case, the parent did not believe this fact. The reason for disclosing data is usually revenge, anger," – a member of the LGBT+ community.

The community members disseminate information about each other's medical diagnosis.

"With regard to the diagnosis of AIDS, members of the community are more aware that it is incorrect to talk about this data. However, they talk freely about other diseases. They don't have the sense that it could be someone's personal data," - a member of the LGBT+ community.

Sometimes personal data (information about sexual orientation, information about a medical diagnosis) is used by the community members to blackmail each other.

"There are such threats - "If you don't do this, I will publicize information about your illness, sexual orientation," - a member of the LGBT + community.

It was noted that in case of significant damage in the dissemination of information about sexual orientation, gender identity or other data (for example, information about HIV status), members of the community sometimes turn to the investigative body. The investigation into such facts starts under Article 157 of the Criminal Code of Georgia (encroachment on personal information or personal data). It was also noted that cases of extortion through threats of disclosure of the specified personal of the LGBT+ community members were transferred to the investigative authority. In addition, interviewees noted that such appeals are not frequent, as members of the community, when spreading information about each other or making such threats and identifying signs of a crime, try to resolve the issue among themselves within the community.

On September 23, 2020, a memorandum was signed between the Supreme Court of Georgia, the Prosecutor's Office of Georgia, the Ministry of Internal Affairs of Georgia and the National Statistics Office of Georgia on the production of statistics on crimes committed on the grounds of intolerance based on discrimination and the issuance of a unified report.[25] Based on the mentioned memorandum, according to the report of 2020 published on the statistics of crimes committed on the grounds of intolerance based on discrimination, in 2020 an investigation was launched under Article 157 of the Criminal Code of Georgia (encroachment on personal information or personal data) only in 3 criminal cases, while under Article 181 of the same code (extortion) - no investigation has been launched. [26] According to the 2021 report, in 2021, under Article 157 of the Criminal Code of Georgia (encroachment on information reflecting private life or personal data), investigation was launched only in 4 criminal cases and under Article 181 of the

25 *Memorandum of cooperation on the production of statistics and the issuance of a unified report on crimes committed on the grounds of intolerance based on discrimination, see: https://www.geostat.ge/media/35290/%E1%83%9B%E1%83%94%E1%83%9B%E1%83%9D%E1%83%A0%E1%83%90%E1%83%9C%E1%83%93%E1%83%A3%E1%83%9B%E1%83%98--GEO.pdf*

26 *The unified report of 2020 on the statistics of crimes committed on the grounds of intolerance based on discrimination, see: https://www.geostat.ge/media/36779/diskriminaciis-nishnit_2020_IV.pdf*

same Code (extortion) - also in 4 criminal cases.[27] It is worth noting that the report does not differentiate or define, in relation to any of the above articles, how many of them were related to encroachment on data on sexual orientation, how many of them were related to encroachment on data on gender identity, how many were related to extortion under the threat of disclosure of sexual orientation and how many of them were related to extortion under the threat of disclosure of gender identity. Nor is it differentiated in how many cases the fact of committing the above crimes by a community member was established.

AWARENESS OF LGBT+ PEOPLE ON PERSONAL DATA

The absolute majority of the interviewees interviewed within the framework of the study noted that, despite holding information meetings on data protection issues by organizations that protect the rights of members of the LGBT+ community, awareness of community members about personal data and the importance of protecting it is very low.

In addition, members of the LGBT+ community usually do not know who to address in case of violation of their personal data processing. Most members of the LGBT+ community do not know that there is the Data Protection Authority, only a small part is aware of the existence of such a body and its powers. When their rights are violated, representatives of the LGBT+ community usually call the patrol police or turn to the Ministry of Internal Affairs of Georgia if a police officer violates ethical standards. It was also noted that after the events that took place in relation to the State Inspector's Service, more people learned about the right of personal data protection and the existence of a supervisory authority, however, even these representatives of the LGBT+ community do not have information about the mechanisms for applying to the supervisory authority (how to apply, what procedures to go through).

Members of the LGBT+ community and representatives of organizations protecting the rights of members of the LGBT+ community noted the need to raise awareness of the LGBT+ community members on data protection issues. In their opinion, the following measures will be effective:

- Organization of informative field meetings, where problems will be discussed on specific examples and cases.

  It was also emphasized that it is very difficult to organize and conduct training for the community members. Most of them may not come to the scheduled training. Therefore, it may be more effective to train community members who are active within the community and who have the trust of community members. They periodically arrange meetings in queer spaces where they discuss various issues with representatives of the community;
- Preparing information brochures that can be placed in the offices of organizations that protect the rights of the LGBT+ community members and through them convey to the community members information about the importance of protecting personal data and relevant protection mechanisms;
- Carrying out information campaigns in the online space - as a rule, a large number of people view them and via this means the community members become better acquainted with the information. It will be effective to prepare (and further disseminate) informational videos that not only will be graphic but also meaningful and will contain information about the importance of data protection, the rights of the data subject and their implementation in practice;
- Preparing informational stickers and placing them in places (e.g. nightclubs, cafes) where community members gather.

27 *The unified report of 2021 on the statistics of crimes committed on the grounds of intolerance based on discrimination, see: https://www.geostat.ge/media/43558/diskriminaciis-niSniT_2021.pdf*

CONCLUSION

In connection with publicizing /disclosing data about each other by the community members identified as a result of the study, it should be noted that according to paragraph 3 (a) of the Law of Georgia on Personal Data Protection, this Law does not apply to data processing by a natural person clearly for personal purposes when the data processing is not related to his/her entrepreneurial or professional activities. Thus, the processing of data for clearly personal purposes, if it is not related to the entrepreneurial or professional activities of an individual, is not subject to the Law of Georgia on Personal Data Protection and, therefore, is not an administrative offense.

In addition, it is a crime to illegally obtain, store, use, distribute or otherwise provide access to personal data that caused significant damage, as well as extortion, accompanied by the threat of disclosure of information discrediting the name of the victim or his/her close relative, or dissemination of other similar information that can significantly infringe on their right.[28] The study, including the reports on hate crime statistics, has shown that community members less address law enforcement agencies even when there is evidence of a data breach or threat of extortion.

In order to ensure respect for personal life and personal data protection of LGBT+ people, prevent crime and provide adequate response, it is important to raise their awareness on the issues of personal data protection, including on its importance, relevant data protection mechanisms, legal regulations and consequences of data breach.

28 *Articles 157 and 181 of the Criminal Code of Georgia, see: https://matsne.gov.ge/en/document/view/16426?publication=235*

XIV. RESPONDING TO FACTS OF ILLEGAL PROCESSING OF PERSONAL DATA OF THE LGBT+ COMMUNITY MEMBERS

INTRODUCTION

According to the first paragraph of Article 26 of the Law of Georgia on Personal Data Protection, if the data subject believes that his/her right under this Law has been violated, s/he may apply for the restoration of the violated right: to the Personal Data Protection Service[29] or to the court, and if the data processor is a public institution, the complaint can also be lodged with the same or a higher administrative authority.

EXISTING CHALLENGES

The interviewees noted that representatives of the LGBT+ community in cases of illegal processing of their data by police officers/investigators, for the most part, do not apply to the relevant body for a response (the higher administrative body - the General Inspection of the Ministry of Internal Affairs of Georgia, Data Protection Authority, the court), because they perceive it as a confrontation with a representative of a law enforcement agency. However, if there is such a desire, an appeal is often hindered by the lack of sufficient evidence on the relevant fact.

As for misconduct or violations by medical personnel, in such cases, members of the LGBT+ community, as a rule, refrain from contacting the relevant authorities (the higher administrative body - Professional Development Council of the Ministry Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs, Data Protection Authority, the court), because they do avoid straining relations

29 *The first Data Protection Authority in Georgia which exercised control over the legality of personal data processing, was established in 2013 in the form of the Personal Data Protection Inspector. Since May 10, 2019, State Inspector's Service became the legal successor of the Office of the Personal Data Protection Inspector and from March 1, 2022, this function is performed by the Personal Data Protection Service. See https://personaldata.ge/ka/about-us#*

with doctors. In particular, it was noted that the financial situation of a significant part of the community members does not allow them to turn to doctors in private clinics. Because of this, they have constant contact with those clinics/doctors where the state finances certain studies (for example, JSC Scientific-Practical Center of Infectious Pathology, AIDS and Clinical Immunology). Therefore, they prefer to turn a blind eye to such violations.

"Referring to service personnel even in a polite form about certain misconducts causes irritation, awkward communication and spoiling of the relationship. That is why I have often refrained from raising this issue," - a member of the LGBT+ community.

Other barriers that might make it impossible to apply to the relevant authority were also mentioned.

"In most cases, members of the LGBT+ community do not have information about personal data, including when this right is violated, to which authority and how to address them. However, even if information is available, the community members may not contact the relevant authority, as the community members avoid the secondary activation of information about their gender identity and sexual orientation, which, in turn, may be associated with stigmatization," - a member of the LGBT+ community.

Within the framework of the study, cases were identified when representatives of an organization protecting the rights of members of the LGBT+ community applied to the Professional Development Council of the Ministry Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs regarding the fact of illegal processing of personal data by a doctor, however, since the case is being discussed in the Council for years (2-3 years), a member of the LGBT+ community no longer shows interest in the case. Therefore, the community representatives consider appealing to the Council to be ineffective and, for this reason, avoid using this mechanism.

Within the framework of the study, it was also noted that cases of illegal data processing by lawyers are referred to the Ethics Commission of the Georgian Bar Association, however, the rate of referral on such facts is also low due to the aforementioned barriers.

CONCLUSION

The above facts show that referral to relevant authorities on facts of illegal processing of personal data of LGBT+ persons by data processors, including publicizing and disclosure, is low. In most cases, members of the LGBT+ community do not have information about personal data and the protection mechanisms in case of illegal processing and the procedures for their use, and even if such information is available, they do not have evidence to confirming the fact or refrain from using these mechanisms.

The facts that LGBT+ persons have less information about the cases when their right to personal data protection is violated and/or when they can apply to the bodies provided for by the Law of Georgia on Personal Data Protection to have violated right restored or that they less often use these mechanisms, impede their legally guaranteed right to the protection of personal data and improving the data protection standard by exercising effective control over cases of unlawful processing of personal data.

In order to ensure respect for private life of LGBT+ people and the protection of personal data, it is important to raise their awareness on the issues of personal data protection, including the rights of members of the community in this area, the mechanisms for protecting these rights and the importance of their use.

In addition, it is important to strengthen the staff of the bodies that consider the facts of unlawful processing of personal data of LGBT+ persons regarding the peculiarities accompanying consideration of this type of cases.

XV. PERSONAL DATA PROCESSING BY NON-GOVERNMENTAL ORGANIZATIONS

INTRODUCTION

Organizations that protect the rights of members of the LGBT+ community serve hundreds of members and offer various types of services throughout the year. Accordingly, organizations process their personal, including special categories of data.

It is also worth noting that sometimes these organizations act as intermediaries between other institutions and members of the community which also aims to provide services.

EXISTING CHALLENGES

As the organizations interviewed within the framework of the study noted, precisely because organizations have contact with sensitive data, they pay special attention to the security and confidentiality of community members' data: when providing services to beneficiaries, they do not indicate their names and family names in the respective forms. Only initials are written, this is also in order that the recipient be identified by the service provider; they try not to store personal data on paper and digitize it as much as possible; data on a community member is usually entered into an electronic program where the amount of data is kept to a minimum; a limited circle of persons has access to data, only based on a strict business need; organizations ensure that appropriate inventory (eg. a safe) is purchased to adequately protect paper data; when implementing various types of projects with the assistance of donors, the lists of project beneficiaries or assessments are fully coded (for example: several digits of a personal number are indicated). Donor organizations also never ask for the names and family names of the beneficiaries who received assistance.

Organizations noted that the principle of confidentiality is enshrined in internal organizational documents the protection of which is of particular importance. For example, the recipient signs a consent form for the processing of their data when receiving service of a psychologist. The same form states confidentiality. This document is only available to the psychologist providing the service and may be shared with others if vital interest of a community member is at stake.

If the recipient wishes, when providing the service, an agreement is even concluded that the representative of the organization does not disclose his/her acquaintance (for example, greets him/her) when meeting on the street or in another setting, so that this person cannot be identified as a member of the community.

Even information about meetings held by organizations with the community members is protected, among them, the pages of organizations are closed and they do not upload photos depicting meetings.

In parallel with the above measures, it was found that some organizations have not introduced a special personal data protection policy document that would describe the data processing process as well as describe the grounds and purposes of data processing, data storage periods, organizational and technical measures taken to protect them, the rights of the data subject and the mechanisms for enforcing these rights, procedures/rules for responding to cases of illegal data processing, the rights and obligations of persons involved in data processing.

In parallel with the above measures, it was found that some organizations do not have in place a special personal data protection policy document that would describe the data processing process, as well as describe the grounds and purposes of data processing, data retention periods, organizational and technical measures taken to protect them, the rights of the data subject and mechanisms for their realization, procedures/rules for responding to cases of illegal data processing, the rights and obligations of persons involved in data processing.

Representatives of the organizations also noted that some of the employees were trained on personal data protection, however, along with the arrival of new employees in the organization, the training of employees of the organization must be systematic.

Organizations have indicated that since they are in possession of a large amount of sensitive information, they welcome the strengthening of the non-governmental sector (including in the regions) in terms of data protection. Although special attention is paid to the personal data they protect, there is a need for periodic training of employees on the protection of personal data, as well as further improvement of internal data processing processes to ensure data security.

"Not only organizations protecting the rights of the LGBT+ community members, but also non-governmental sector in general need to be strengthened on data protection issues so that all employees of the organization are properly aware of the importance of data protection, including within the organization,"
– a representative of the organization protecting the rights of the LGBT+ community members.

CONCLUSION

Taking into account the category, content, volume of data processed by organizations that protect the rights of members of the LGBT+ community and the risks of their illegal processing, it is necessary to strengthen organizations in the direction of data protection: it is recommended to describe data processing processes, develop data protection policy documents and introduce appropriate data security measures, as well as conduct periodic training/awareness raising for employees on personal data issues.

XVI. PRACTICE OF THE PERSONAL DATA PROTECTION AUTHORITY

INTRODUCTION

In order to familiarize and analyze the practice of the Data Protection Authority in terms of providing response to cases of unlawful processing of personal data of representatives of the LGBT+ community, on June 27, 2022, the Personal Data Protection Service was requested, on the one hand, to provide information on the cases studied by the Service from 2013 onwards (whether the data protection authority has studied cases of processing of personal data of a representative of the LGBT+ community (indicating the number and results)), and, on the other hand, decisions on cases that are referred to in separate reports of organizations protecting the rights of the LGBT+ community members as cases of the LGBT+ community members studied by the Personal Data Protection Inspector. [30]

30 *Litigation Report „Discrimination and Violence against LGBTQI Persons", Women's Supporting Initiative Group WISG, 2019, p.22-23, 24-25, 31-32. See: https://women.ge/data/docs/annual-reports/WISG_litigation%20report_2019_ENG.pdf*

2018 report on the "Violation of Human Rights of Gay Men, other MSM and Trans People", Mariam Kvaratskhelia and Non-governmental Organization Equality Movement, 2019, p.10. See:

http://www.equality.ge/wpcontent/uploads/2019/09/GEO_%E1%83%A3%E1%83%A4%E1%83%9A%E1%83%94%E1%83%91%E1%83%94%E1%83%91%E1%83%98%E1%83%A1-%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98-2018.pdf

2019 report on the "Violation of Human Rights of Gay Men, other MSM and Trans People", Ana Aptsiauri and Non-governmental Organization Equality Movement, p.21-22. See:

http://www.equality.ge/wp-content/uploads/2019/12/2019-%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98.pdf

According to the Personal Data Protection Service, the Data Protection Authority does not collect statistics on the number of cases of processing personal data of the LGBT+ community members, and therefore, the information on the number of such cases from 2013 is not available.

In addition, the Personal Data Protection Service provided in anonymized form the requested decisions on cases of LGBT+ community members (5 decisions in total) which were indicated in the above-mentioned reports. [31] Among them, in one case, the consideration of which was completed within the framework of classified proceedings, the Service sent only unclassified parts of the decision.

Below are the above decisions (cases) in redacted form. In particular, in order to exclude the processing of unnecessary information and highlight noteworthy points in the case, certain factual circumstances and dates indicated in the cases have been changed/removed. The legal norms specified in it are given in accordance with the legislation in force at the time of the consideration of the case. Each case consists of several parts - factual circumstances, legal assessment, Inspector's decision.

CASES

CASE NO. 1 – DISCLOSURE OF INFORMATION ON RESIDENTIAL ADDRESS

FATCS

On February 1, 2018, a citizen applied to the Personal Data Protection Inspector with a request to respond to the fact of disclosure of address of residence to his/her parents.

The mentioned person (hereinafter - the applicant) indicated that s/he was a victim of domestic violence by his/her parents, which is why on January 17, 2018 s/he left home and moved in with a friend. On January 19, 2018, the applicant addressed the police and, in the course of reporting the fact, asked the police not to inform hi/hers parents about his/her actual address of residence (this request was recorded both in the statement and the interview protocol), because there was a risk of repeated violence. On January 22, 2018, the case was transferred to another police department for further response, where, during a conversation with an employee of the department, the applicant again stated his/her request to keep the actual address of residence confidential.

On January 24, 2018, a restraining order was issued against the applicant's parents, on the basis of which the parents were forbidden to approach the victim's location at the place of residence, work etc. The restraining order also contained information about the victim's actual address of residence.

According to the Ministry of Internal Affairs of Georgia, all required fields, including the address of the actual residence of the victim, were included in the restraining order and the protocol on the restraining order. According to the law, one copy of the restraining order was provided to the applicant who did not make comments/complaints when signing it and one copy was handed to the perpetrators through which they learned about the applicant's actual address. According to the explanation of the Ministry, during the familiarization with the order, it was explained to the applicant that one copy of the document would also be passed to the abusers.

In the process of considering the application, the applicant additionally indicated that, despite his/her insisting, the actual address of residence was indicated in the restraining order issued by the police on 24 January 2018 against his/her parents. The content of the restraining order was not explained to him/her, and although s/he signed the order, s/he did not even notice that it contained the address. Due to the fear of violence from parents and the fear of a repeated attack, s/he was unable to fully understand all

31 *Persons indicated in the reports are indicated as LGBT+ persons.*

the procedural details that the police carried out, including the indication of the address in the restraining order. In addition, s/he had notified the police in advance not provide parents with information about the actual address of residence, however, despite this requirement, the police failed to properly assess the risks of disclosing information, thereby endangering his/her life and health.

LEGAL ASSESSMENT

Pursuant to Article 5 (b)(c) of the Law of Georgia on Personal data Protection, data processing is admissible if this is provided for by the law and/or data processing is necessary for a data controller to perform his/her statutory duties.

Pursuant to Article 9^1 of the Law of Georgia on the Elimination of Violence Against Women and/or Domestic Violence and the Protection and Support of Victims of Such Violence, identification of and relevant response to cases of violence against women and/or domestic violence is carried out by Law enforcement and judicial bodies, as well as the Group for Determining Victim Status in accordance with the rule determined by the law. According to Article 10 of the same Law, to ensure prompt response to facts of violence against women and/or domestic violence, the authorized body, in order to ensure protection of the victim and to restrain certain actions of the abuser, may issue a restraining or protective order as a temporary measure.

A restraining order is an act issued by an authorized police officer that establishes temporary protection measures for victims in case of violence against women and/or domestic violence. The restraining order must state the date and place of its issuance; the circumstances that served as the basis for its issuance; name and family name, date and place of birth, occupation and place of residence of the offender; a list of actions that the offender is prohibited from doing, including the issue of evading the offender from the victim's residence, regardless of whether s/he is the owner of this house or not; the question of approaching the victim, his/her work and other places where the victim is located, approaching him/her as well as other issues that need to be resolved for the safety of the victim. A restraining order may prohibit one, several or all of the acts in accordance with the violence. A restraining order takes effect immediately upon its issuance. It is sent/delivered to the victim and abuser within 24 hours and one copy of the restraining order remains with the issuing authority.

In accordance with paragraph 3 of Article 21 of the same Law, the forms of the restraining order and the protocol on it were approved by order of the Minister of Internal Affairs of Georgia dated July 2, 2014 No. 491 "on the aaproval of the forms of a restraining order as well as determining person authorized for drawing them". The forms contain information fields about the demographic data of the victim, including his/her place of residence.

Based on the analysis of these legal norms, the Inspector stated that, based on the content of the ban imposed by law enforcement officers on the abusers, providing them with information about the actual address of residence of the victim, that is specifying the area which they were forbidden to approach, can be considered legal and in accordance with grounds of data processing pursuant to paragraphs "b" and "c" of Article 5 of the Law of Georgia on Personal Data Protection.

However, the Inspector stated that the Law of Georgia on the Elimination of Violence Against Women and/or Domestic Violence and the Protection and Support of Victims of Such Violence (as well as the Order N491) does not require mandatory and complete indication in the restraining order of all the demographic data of the victim, including the place of residence. In addition, the amount of the victim's personal data to be reflected in the restraining order (as well as in the protocol of the restraining order) depends on the specific circumstances, as well as on the type of temporary measures taken by the law enforcement agency against the abuser. Therefore, when determining the measures to be taken in order to ensure the safety of the victim and indicating the data in the restraining order and the protocol on

the restraining order (due to the fact that the data specified in these documents become available for the abuser), it is important that the law enforcement agency individually and properly assess the will and interest of the victim in protecting the confidentiality of data, especially if the confidentiality of these data (for example, address of residence) may represent an additional means for protecting the security and legitimate interests of the victim. In addition, the law enforcement authority must clearly and intelligibly explain to the data subject the need to process their data and the possible consequences.

INSPECTOR'S DECISION

Despite the fact that no violation of the rules established by the Law of Georgia on Personal Data Protection was found during the consideration of the complaint, the Ministry of Internal Affairs of Georgia was recommended to take organizational and technical measures ensuring assessing the amount of data to be disclosed to abusers, duly informing the victim about the purposes and expected results of the disclosure in order to ensure safety of victims when carrying out measures provided for by the Law of Georgia on the Elimination of Violence Against Women and/or Domestic Violence and the Protection and Support of Victims of Such Violence. [32]

CASE NO. 2 – OBTAINING THE DATA ILLEGALLY FROM THE CENTRAL INFORMATION BANK

FACTS

In July 2018, a citizen (hereinafter referred to as the applicant) contacted the Personal Data Protection Inspector, who indicated that a few days ago his/her mother contacted him/her through the social network - Facebook and sent the so-called screenshot showing his/her personal data in the Central Information Bank of the Ministry of Internal Affairs of Georgia (hereinafter - the Ministry), including information about the alleged criminal act committed against him/her in 2017. According to the applicant, the aforementioned so-called screenshot could have been obtained and disseminated by the Ministry official who knew him/her and his family.

In the course of considering the application, the Ministry explained that, based on a letter received from the Office of the Personal Data Protection Inspector, the General Inspection of the Ministry had been conducting an internal audit in order to study the legality of checking the applicant's data in the Central Information Bank. As a result, it was established that on June 27, 2018, the applicant's data was viewed/obtained for non-official purposes in the Central Information Bank by an Inspector-Investigator of the District Inspector's Unit of the Department of A/R of Abkhazia of the Ministry, using a personalized device (was checked twice) for generating a one-time digital password (DIGIPASS). The conclusion of the General Inspection submitted by the Ministry also states that, as part of the internal audit, the Inspector-Investigator confirmed the fact of viewing and obtaining the applicant's data in the Ministry's secure computer database, although he did not remember the fact of photographing the information and transferring it to a third party. This explanation was not shared by the Ministry's General Inspection as it could have been invented for the purpose of averting liability. The Ministry regarded the actions of the Inspector-Investigator as a disciplinary offense, and on the basis of the order of the Minister of Internal Affairs of Georgia dated August 29, 2018, he was dismissed from his post.

The applicant, taking into account strained relations with family members, refused that the Office of the Personal data Protection Inspector contact his mother and another relative, through whom the aforementioned so-called screenshot became available to the applicant's mother. Due to this reason the Inspector was unable to obtain further evidence regarding the disclosure of the data to applicant's mother.

32 *Pursuant to the Order of the Minister of Internal Affairs of Georgia No. 81 of July 13, 2018, the forms of the restraining order and the protocol of the restraining order were updated, which no longer include the field of information about the actual address of the victim. See: https://matsne.gov.ge/ka/document/view/4262664?publication=0*

LEGAL ASSESSMENT

With the evidence examined as part of the consideration of the application, it was clearly established that on June 27, 2018, the applicant's data in the Central Information Bank of the Ministry was checked by an employee of the Ministry for non-official purposes, which the Inspector assessed as data processing without the basis provided for in Article 5 of the Law of Georgia on Personal Data Protection.

In addition, despite the fact of illegal access to the applicant's data in the Central Information Bank of the Ministry and the fact that the applicant disclosed these data, for objective reasons full collection of evidence was not possible in the course of consideration of the complaint (among them, on the basis of the applicant's request, interviewing the applicant's mother and her relative and obtaining an explanation concerning circumstances of the case could not be carried out), which would allow establishing additional circumstances related to the disclosure of the data to the applicant's mother. Accordingly, based on the requirements of articles 230 and 237 of the Code of Administrative Offenses of Georgia, the Inspector could not establish the fact of an administrative offense in this part.

INSPECTOR'S DECISION

Due to the expiration of statute of limitations for imposing an administrative fine, as established under Article 38 of the Code of Georgia on Administrative Offenses, the employee of the Ministry could not be held administratively liable for obtaining the applicant's data without a ground provided for in Article 5 of the Law of Georgia on Personal Data Protection.

CASE NO. 3 - DISCLOSURE OF PATIENT'S DATA VIA SOCIAL NETWORK

FACTS

On the basis of the citizen's application (who was represented by an authorized representative) dated February 12, 2018, the Personal Data Protection Inspector studied the fact of disclosure of his/her (hereinafter - the applicant) personal data through the social network - Facebook by one of the medical institutions (hereinafter - the clinic).

As established in the course of considering the application, at the beginning of 2018, an article was published on the website of one of the media outlets, in which the applicant described the incident related to his/her beating on the street and the events that subsequently took place in the clinic (according to the applicant, no appropriate assistance was provided in the clinic) and its surrounding area where he also became a victim of an attack by two strangers leaving the clinic.

After the article was aired on the Internet, users of the clinic's social network - Facebook page started negatively rating the clinic's page and making offensive comments about the clinic.

The clinic considered that the information disseminated by the applicant through the media was a lie, and in order to protect its reputation and provide accurate information to the public about the events that had occurred, it published a position regarding the incident outside the clinic on its Facebook page, which indicated the applicant's identity, described in detail the fact of beating and taking the applicant to the clinic, medical complaints, the results of examinations carried out and the doctors' assessments. The clinic also indicated that the applicant needed to be observed in dynamics for a certain period of time, which s/he and the persons accompanying him refused and left the clinic after signing the relevant document. The clinic expressed its concern about the fact of violence in the vicinity of the clinic, dissociated itself from it and emphasized that the patient was not insulted, humiliated or abused by the medical staff.

LEGAL ASSESSMENT

The purpose of the Law of Georgia on Personal Data Protection is to ensure the protection of human rights and freedoms, including the right to privacy in the course of personal data processing. In addition, Article 6 of the mentioned law provides for a special procedure for processing a special category od data of a person and prohibits the processing a special category of data, except for the exceptional cases established by paragraph 2 of the same article *(including, in accordance with subparagraph "d" of this paragraph, processing a special category of data is allowed if a data subject has made his/her data publicly available without an explicit prohibition of their use)*. In addition, in accordance with paragraph 3 of Article 6 of the same law, even if there is an appropriate legal basis for the processing of a special category of data, it shall be prohibited to make the data publicly available and to disclose the data to a third party without the consent of the data subject. Issues related to the processing of information about the state of health, including disclosure, are also provided for by the Law of Georgia on the Rights of the Patient, according to Article 27 of which, the health care provider is obliged to protect the confidentiality of information about the patient in its possession.

When processing a special category of data, it is also necessary to comply with the principles of data processing established by Article 4 of the Law of Georgia on Personal Data Protection. In particular, the data must be processed fairly and lawfully, without impinging on the dignity of the data subject. The purpose of data processing must be clear, specific and predetermined, and in each individual case it must be assessed whether the amount of data processed is adequate and proportionate to this purpose.

The Inspector stated that the individual's interest in protecting his/her special category of data and controlling the dissemination of this information is one of the most important elements of confidentiality. Accordingly, the disclosure of personal data, including special category of data, to a third party should be carried out only if there are grounds and in compliance with the principles of data processing provided for by the Law of Georgia on Personal Data Protection. Since the Law of Georgia on Personal Data Protection exhaustively defines the legal grounds for the processing of special category of data, the Inspector did not consider the interest in protecting the reputation of the clinic as an exceptional case of disclosure of information containing the applicant's special category of data. The Inspector noted that the clinic could have achieved the goal of informing the public by processing less data so that information containing the applicant's special category of data would not become publicly available, especially given that the applicant himself did not disclose details of his medical condition, including in the interview given to the media.

INSPECTOR'S DECISION

Due to the disclosure of the applicant's data through the social network - Facebook without a legal ground provided for in Article 6 of the Law of Georgia on Personal Data Protection, the clinic was found liable for committing an administrative offense under the first paragraph of Article 45 of the same law and was fined. The clinic was also instructed to disclose the documentation/information containing the personal data of patients only if there is a legal ground(s) established by law, and to delete the information containing the applicant's special category of data posted on its Facebook page.

CASE NO. 4 - DISCLOSURE OF PATIENT'S DATA BY A DENTAL CLINIC

FACTS

On February 13, 2018, a citizen (hereinafter referred to as the applicant) applied to the Personal Data Protection Inspector through an authorized representative. According to the applicant, on January 19, 2018, he visited one of the dental clinics (hereinafter referred to as the clinic) to receive dental services. After undergoing the procedure, in order to fill out a medical questionnaire, s/he provided the clinic

doctor (hereinafter referred to as the doctor) with information about his/her state of health, in particular, told the doctor that s/he was infected with HIV. According to the applicant, a few minutes after leaving the clinic, he again returned to the doctor and witnessed him/her talking on the phone with a third person and mentioneding that he had had "an AIDS patient".

According to the applicant, about 10 minutes after leaving the clinic, he received an incoming call from the clinic during which he again heard the doctor telling third parties that s/he had had provided services to an "AIDS patient", who was also a homosexual man *(the applicant, according to his explanation, submitted a recording of the conversation).*

The applicant also pointed out that the medical form filled out by the doctor, which indicated his identity, was placed in an open form on the table.

According to the clinic, when the applicant returned to the clinic, the doctor informed the director of the clinic that s/he had an HIV positive patient, since the director of the clinic had temporarily been responsible for the sterilization of instruments. Accordingly, s/he provided the director of the clinic with information about the patient's health condition, without mentioning the name of the applicant, so that the director of the clinic could consider the risk of infection when sterilizing the instruments. In connection with the above-mentioned case, the loud conversation of the applicant was heard by the employee of the clinic in the other working room, to whom the doctor also provided general information about the patient's complaint without indicating the applicant's name. After the arrival of the director of the clinic, all three together discussed what happened in the clinic. During the conversation, the director and the above-mentioned employee of the clinic also denied the disclosure of the applicant's identity. According to the submitted explanations, the information about the applicants's health had been considering for the purpose of proper sterilization of the used instruments, without revealing his identity. In addition, the clinic noted that the applicant's medical questionnaire was kept in a safe place (in the bottom drawer of the table) in several minutes after filling it out.

When examining the application, the recording of the ongoing conversation between the doctor and third parties (two other persons) presented by the applicant, did not reveal the fact that the applicant's name was mentioned. They discussed the incident in the clinic without mentioning the applicant's name.

LEGAL ASSESSMENT

Pursuant to Article 2 (b) of the Law of Georgia on Personal Data Protection, information on health status is a special category of data. The Law on Personal Data Protection enshrines a special rule for the processing of a person's special category of data. In particular, Article 6 of the law sets the grounds when the processing of special categories of data is permitted as an exception. According to paragraph 2 of the said article, processing of special categories of data is allowed, including for the purpose of public health protection, health care or protection of health of a natural person by an institution (employee), and if it is necessary to manage or operate the health care system. In accordance with paragraph 3 of the same article, even when there is a relevant legal ground for processing a special category of data, it shall be prohibited to make the data publicly available and to disclose the data to a third party without the consent of the data subject.

Issues related to the processing of information about health of a person, including disclosure, are also provided for by the Law of Georgia on the Rights of the Patient, according to Article 27 of which, the health care provider is obliged to protect the confidentiality of information about the patient. In addition, in accordance with paragraph 1 of Article 9 of the Law of Georgia on HIV infection/AIDS, an institution providing services that diagnoses, treats, prevents, supports/facilitates and/or cares for HIV/AIDS patients, as well as any legal and natural persons who have information about a person's HIV/AIDS infection are obliged to protect the confidentiality of information in accordance with the procedure established by the legislation of Georgia. According to paragraph 5 of the same article, a person infected with HIV/AIDS has the right to determine the person/persons who can be provided with information about his/her HIV status.

Article 17 of the Law of Georgia on Personal Data Protection should also be considered which imposes on the data processor the obligation to take such organizational and technical measures that ensure the protection of data from accidental or illegal destruction, alteration, disclosure, extraction, illegal use in any other form and accidental or illegal loss. Any employee of the data processor who participates in data processing, is obliged not to exceed the scope of the authority granted to him. In addition, s/he has an obligation to protect the confidentiality of data, including after the termination of an official authority.

As part of the consideration of the application, conflicting explanations were provided regarding the disclosure of the applicant's special category of data to third parties in an identifiable form and the placement of the patient's medical form on the table in a publicly accessible form. In addition, both the applicant and the clinic (including the doctor and clinic staff) were interested parties, which raises the possibility of a private interest in obtaining their explanations in the course of the case. No other reliable evidence could be obtained within the framework of the consideration of the application *(the fact of mentioning the applicant's name was not established in the record of the telephone conversation submitted by the applicant)*. Thus, due to the lack of reliable evidence, the fact that the clinic disclosed the applicant's data in an identifiable form on 19 January 2018 and placed the medical form on the table in a form accessible to all, could not be established.

As for sharing the information about the applicant's health status without the name of the applicant for the purpose of proper sterilization of instruments, according to Article 3 of the Decree of the Government of Georgia dated April 24, 2015 No. 185 on Approval of the Technical Regulations for Disinfection and Sterilization in Medical Institutions, Healthcare Institutions and Institutions of Public Importance, a facility must have a person responsible for sterilization/disinfection of medical instruments/medical objects. In addition, it must have a written operating rule/procedure regarding carrying out sterilization-disinfection and the use of disinfectant working solutions.

In addition, according to Article 17 of the Law of Georgia on Personal Data Protection, the data processor is obliged to ensure adequate data security, as well as to follow the principles defined by Article 4 of the same law, including processing data only for specific, clearly defined, lawful purposes. The data may only be processed to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which they are processed.

According to the Inspector's assessment, based on an analysis of the norms of the above decree, there is no need to transfer information about the state of health of a particular person to the person responsible for sterilization in each individual case. Accordingly, the use of information about the patient's health status (including without specifying his identity) without a respective purpose and necessity creates the risk of processing data for illegal purposes and disclosing it to persons who do not have the right to access it.

INSPECTOR'S DECISION

The clinic was instructed to process information about the health status of data subjects only for legal purposes in the future, in the case of appropriate need and necessity, in accordance with the principles of data processing and security defined by the Law of Georgia on Personal Data Protection.

CASE NO. 5 - OBTAINING AND DISCLOSING INFORMATION ON GENDER IDENTITY FOR PERSONAL PURPOSES

FACTS

On March 11, 2019, a citizen (hereinafter referred to as the applicant) filed a complaint with the Personal Data Protection Inspector through a representative, who pointed out that her co-worker had unlawfully

obtained information about her gender identity and disclosed it to other employees.[33]

In particular, according to the applicant, she was a transgender woman and worked for a private company. In the specified company, one of her co-workers (hereinafter referred to as the co-worker), from the user profiles s/he had created with a certain name, obtained the applicant's personal photos and information on gender identity and with the aim of harassing her in the workplace, with malicious intent distributed this information among other co-workers. However, in what form (verbally or physically) and to whom the co-worker managed to transfer the applicant's feminine photographs - the applicant does not know. Due to the pressure and harassment, the applicant was forced to leave the company on the basis of a personal statement, which is why she does not maintain contact with his former co-workers and cannot find out their contact details and names.

In the course of considering the application, it was established that the applicant had registered a profile with a specific name on the social network "Facebook" and the social network "Odnoklassniki'", where photographs reflecting the applicant's gender identity were publicly posted without any prohibition. The co-worker obtained said photographs of the applicant through the aforementioned profiles.

The evidence of the case did not establish the involvement of the employer company in the process of data collection and processing. The staff member officially represented the applicant's supervisor, however, according to his own explanation, he was not responsible for gathering information about the applicant. In the course of reviewing the application, the co-worker indicated that information about the applicant's gender identity and photos (where she looks in accordance with her gender identity) became available to him/her by chance, when, s/he had been viewing a profile with a certain name on social networks out of personal curiosity and s/he recognized the applicant from publicly available photographs in the specified profile of the applicant. After that, a number of his/her co-workers saw photos publicly posted by the applicant.

LEGAL ASSESSMENT

According to Article 1 of the Law of Georgia on Personal Data Protection, the purpose of this law is to ensure the protection of human rights and freedoms, including the right to private life, during the processing of personal data.

Article 3 of the same law defines the scope of the law and the exceptional cases when the law of Georgia on Personal Data Protection does not apply to data processing and, accordingly, the Inspector's competence. According to paragraph 3 (a) of the mentioned article, the law does not apply to the processing of data by a natural person for clearly personal purposes, when their processing is not related to his entrepreneurial or professional activities.

In addition, since the fact of data processing concerned the processing of data of one person by a person working in the same institution, the Inspector also took into account the practice of the European Court of Human Rights when discussing the problem of data processing. In particular, the European Court of Human Rights in the case - ANTOVIĆ AND MIRKOVIĆ v. MONTENEGRO explained that, since one of the most important opportunities for the formation of social relations is the process of working life, it is often impossible to clearly determine which human actions are directly included in the scope of professional activity and which are not. According to the Inspector, the said explanation of the European Court of

33 *According to the Inspector's decision of March 18, 2019, on the basis of paragraph 3 (a) of Article 3 of the Law of Georgia on Personal Data Protection, paragraph 5 of Article 39 of the same law and Article 232 of the Code of Administrative Offenses of Georgia, the applicant was refused that application of 11 March 2019 be considered and it was transferred to the Ministry of Internal Affairs of Georgia for appropriate response. In the application submitted to the Inspector's Office on April 19, 2019, the representative of the applicant indicated that according to the letter of the Ministry of Internal Affairs of Georgia dated April 2, 2019, the application and documentation forwarded by the Inspector did not contain the signs of the crime stipulated by the Criminal Code of Georgia, for which reason the investigation was not launched into the case. Based on the above, the Inspector was requested to reconsider the statement of March 11, 2019 and to take the measures in accordance with the law.*

Human Rights made it clear that professional relations are not enough to exclude the processing of data for personal purposes, since the existence of private life and personal relationships is possible even in the course of official activities.

In view of the foregoing, based on the information and evidence provided during the consideration of the application, it was not established that the applicant's co-worker acted for professional or commercial purposes in the process of data processing as part of official activities. The circumstances identified during the consideration of the application indicated to the processing of data for personal purposes.

INSPECTOR'S DECISION

Since, pursuant to paragraph 3(a) of Article 3 of the Law of Georgia on Personal Data Protection, the mentioned law does not apply to the processing of data by a natural person for clearly personal purposes (when their processing is not related to his entrepreneurial or professional activities), the Inspector could not assess the specified data processing case. In addition, the applicant was advised that in accordance with Paragraph 1^1 of Article 3 of the Organic Law of Georgia on the Public Defender of Georgia and the Law of Georgia on the Elimination of All Forms of Discrimination, she could apply to the Public Defender of Georgia regarding the possible fact of discrimination and harassment by the employer.

CONCLUSION

The analysis of the above 5 decisions of the Inspector (which were requested on the basis of the cases indicated in the reports of the organizations protecting the rights of representatives of the LGBT+ community/information lodged before the Inspector) shows that there are facts of illegal publicizing and disclosure of data of LGBT+ people, cases of inadequate protection of the principles of processing data and data security.

In addition, due to the lack of relevant statistics, it was not possible to obtain and analyze information on other cases of processing of personal data of the LGBT+ community members studied by the Data Protection Authority.

In order to identify the problems of representatives of the LGBT+ community in the field of personal data protection and to fully analyze the practice of the Data Protection Authority, it is important that the Personal Data Protection Service collect and publish statistics of the studied cases regarding the processing of personal data of the LGBT+ community members.

Also, as a result of the interviews, it was revealed that there are a number of problems/shortcomings related to the processing of data of LGBT+ persons in various areas, including the failure to take data security measures, violation of the rights of the data subject, processing data without legal grounds and legitimate purpose, in an excessive amount, in a manner that violates dignity etc. In the process of data processing, a large number of systemic deficiencies in the healthcare sector were identified, especially in the JSC Scientific and Practical Center for Infectious Pathology, AIDS and Clinical Immunology, where LGBT+ people receive free medical services under various programs.

Responding to identified deficiencies by the Data Protection Authority is essential for ensuring lawfulness of data processing, taking effective legal and organizational and technical measures for the protection of personal data and establishing a high standard of data protection, which ultimately serves to implement the rights of data subjects and strengthen trust in data processors.

Accordingly, taking into account the nature, content and scope of the identified problems regarding the processing of personal data of representatives of the LGBT+ community, it is advisable that the Personal Data Protection Service conduct an inspection of JSC Scientific and Practical Center for Infectious Pathology, AIDS and Clinical Immunology, and consider the issue of processing data of LGBT+ people in the inspections plan.

XVII. CONCLUSION

The present report is an analysis of the identified problems and challenges related to the processing of personal data of the LGBT+ community members, as well as an analysis of the practice of the Data Protection Authority and on the basis of these problems, an attempt to assess the state of protection of personal data of LGBT+ people in Georgia. The same report provides recommendations for improving data protection standard.

An analysis of the information provided by members of the LGBT+ community and representatives of organizations protecting their rights, the practices of the Data Protection Authority and legislation regulating personal data revealed that, most often, the community members face data processing violations in the healthcare and law enforcement sectors. Also problematic are: processing and updating data after changing the name/family name and/or gender record; as well as illegal acquisition, use, publicizing, disclosure of data of the LGBT+ people by psychologists, lawyers, other public and private institutions; lack of guarantee of closure of court hearings on the ground of personal data protection when considering administrative and civil cases in court. Many institutions do not have proper guarantees of protecting LGBT+ people from so-called “forced coming out”. Also, their personal data is often processed in an unethical, degrading manner, which causes irreparable harm to their psyche. There are problems with the disclosure of data of LGBT+ people in the media as well. Publication/disclosure of each other’s data by the community members for private purposes has also been identified as a significant challenge. Illegal processing of data causes the biggest problem in relation to those community members who have not “come out”.

Analyzing the information obtained during the interview it was also found that LGBT+ persons have less information about personal data, the importance and mechanisms for their protection. Even if they have such information, they are less responsive to facts of illegal data processing, impingement, extortion with the threat of disclosure and refrain from addressing the relevant authorities.

The protection of the personal data of the LGBT+ community members is important for the exercise of their right to privacy and the protection of personal data, as well as other fundamental rights. It was noted that due to the multitude of facts and the fear of disclosing information about sexual orientation, gender identity, HIV status or other personal data, community members refrain from contacting, for example, medical institutions, law enforcement agencies, while their lives and health are in danger.

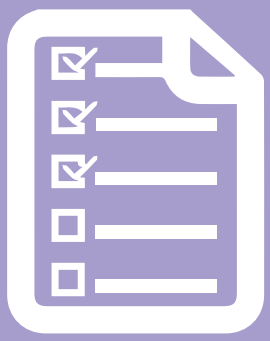
Based on the foregoing, the protection of the data of LGBT+ community members requires a systemic approach and planning and implementation of relevant measures both by data processors and the Data Protection Authority.

In addition, according to the information received from the Data Protection Authority, it has been established that the supervisory body does not collect statistics on the cases of processing of personal data of the LGBT+ community members, which makes it impossible to thoroughly analyze this type of cases.

The interviews also revealed that organizations that protect the rights of members of the LGBT+ community have taken a number of measures to protect the data of the community members. However, in order to strengthen personal data security measures and improve data protection standard, it is necessary to support and strengthen organizations in this direction.

It is important that relevant data processors and supervisory/regulatory authorities pay attention to the findings presented in the report in order to avoid cases of processing personal data of LGBT+ persons in violation of the rules established by the Law of Georgia on Personal Data Protection.

The Center hopes that the recommendations proposed in the report will be supported by data processors, the aforementioned bodies and will have a positive impact on the legal status of LGBT+ people.



XVIII. RECOMMENDATIONS

To the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Helath and Social Affairs of Georgia:

- Instruct medical institutions to develop detailed instructions for the processing of personal data;
- Instruct medical institutions to determine the person responsible personal data protection;
- Instruct medical institutions to take appropriate organizational and technical measures to ensure the confidentiality and security of data;
- Iinstruct medical institutions to periodically conduct training of medical personnel on the personal data protection issues;
- Ensure conducting training on the issues of personal data protection and discrimination for the members Professional Development Council and the employees of the Secretariat of the Council of the Ministry Internally Displaced Persons from the Occupied Territories, Labour, Health and Social Affairs, on the issues of Data Protection and Discrimination.

To medical institutions/medical workers:

- Carefully protect the confidentiality of the patients' personal data. Information related to medical services be processed, including disclosed, only with the consent of the data subject or if there are other grounds provided for by law;
- Duly Inform the patient about the processing of personal data upon receipt of the written consent;
- Process personal data fairly and lawfully, without prejudice to human dignity and observing the principle of data minimization;

- Develop detailed written instructions for the processing of personal data and determine the person responsible for personal data protection;
- Ensure the organization and management of the system for booking visits to the doctor, determine a reasonable interval between visits of different patients;
- Introduce a queue numbering system for those waiting to see a doctor. Ensure calling a patient with the appropriate sequence number and not by disclosing the data identifying the patient to third parties;
- Provide consultation and other medical services in an isolated room, without presence of third parties;
- Ensure storing material documentation in an isolated room, in a cabinet equipped with a lock, or in other properly protected storage, in order to prevent access by unauthorized persons;
- Strictly determine the circle of persons having the right to access the patient's medical documents, the personnel of the medical institution have access to the data only to the extent necessary to perform their official duties;
- Develop a detailed rule for disclosing information about the patient to third parties, which will describe the conditions for providing information, the circle of authorized addressees, security issues, etc.;
- Determine the responsibility of medical workers and other employees of a medical institution for neglecting the rules on data processing;
- Ensure regular monitoring of personal data processing and compliance with established instructions by medical workers and other employees of the medical institution;
- Ensure periodic training of medical workers and other employees of a medical institution on personal data protection issues;
- Ensure that JSC Scientific and Practical Center for Infectious Pathology, AIDS and Clinical Immunology take technical and organizational measures to ensure the protection of data of HIV-infected persons and persons participating in the HIV prevention program from accidental disclosure, disappearance of the so-called "sick spot";
- JSC Scientific and Practical Center for Infectious Pathology, AIDS and Clinical Immunology also develop such a mechanism that excludes access of one patient to the data of other patients when disclosing the results of examination.

To psychologists:

- Ensure confidentiality of information received in the course of consultation from a LGBT+ community member.
- Ensure processing of personal data of members of the LGBT+ community on a fair and legal basis, without degrading human dignity, including in the case of processing the data with the consent of the data subject;
- When disseminating data in a non-identifying form, take all necessary measures to exclude indirect identification of a person (when disclosing specific information about LGBT +person in various forms (for example, through a post and/or paper), in case of indicating the name and surname of the person, the psychologist must make sure that it is impossible to identify a specific person through other information disseminated, or linking the disseminated information with this person requires a disproportionate amount of effort).

To the Ministry of Internal Affairs:

- Ensure protecting the data of the LGBT+ community members and their processing be carried out only if there are grounds specified by law;
- Ensure that data of the LGBT+ community members is processed for legitimate purposes, fairly, without degrading human dignity, only to the extent necessary, observing the principle of data minimization;
- Develop detailed rules and procedures in writing for the processing of personal data in the process of investigating criminal cases;
- Conduct interviews of participants in the process in an isolated room, without the presence of third parties. In the future, take the issues of personal data protection into account in the process of spatial arrangement of the buildings of the Ministry;
- Participants of the proceedings be interviewed only by the investigator who directly conducts the interview and draws up the protocol of the interview/interrogation;
- The number of investigators in criminal cases involving LGBT+ persons be limited as much as possible and only the number of investigators proportional to the complexity of the case be involved in the investigation process;
- Develop detailed instructions on the practical application of Article 104 of the Criminal Procedure Code of Georgia, which will be used to protect personal data;
- Develop a training module for police officers on personal data protection;
- Ensure periodic training for investigators, as well as managers (heads of police, departments), employees of the General Inspection on the issues of personal data protection;
- Examination protocols and other documents related to the criminal case be stored in an isolated room, in a properly protected storage (locked box, drawer) so that the personal information of the participants in the process does not become available to third parties;
- Ensure regular, proactive control over data processing processes by the Ministry employees, identify violations of data processing rules by law enforcement officials and hold them accountable (including developing an effective mechanism for periodic control over unauthorized access to the electronic criminal case management program and other electronic databases) ;
- Provide detailed statistics on Article 181 of the Criminal Code of Georgia (which will allow obtaining the following information – how many of them were related to extortion under the threat of disclosure of data on gender identity, how many of them were related to extortion under the threat of disclosure of data on sexual orientation and how many of them were committed by an LGBT+ community member);
- The Department of Human Rights Protection and Investigation Quality Monitoring of the Ministry of Internal Affairs of Georgia provide monitoring of the issues of personal data protection when conducting investigative and procedural actions with the participation of LGBT+ persons.

To the Office of Prosecutor General of Georgia:

- Limit as much as possible the number of investigators in criminal cases involving LGBT+ persons and engage a proportionate number of investigators corresponding to the complexity of the case the investigation process;

- In order to protect personal data on LGBT+ persons on sexual orientation and gender identity, ensure that a criminal case initiated into the crime committed against members of the community be transferred for investigation to another investigative unit according to territorial jurisdiction.

To Special Investigation Service:

- Ensure collection of detailed statistics on article 157 of the Criminal Code of Georgia (which will allow to obtain the following information - how many of them were related to impingement of data on gender identity, how many of them were related to impingement of data on sexual orientation and how many of them were committed by members of the LGBT+ community).

To Georgian Bar Association/Lawyers:

- Lawyers, engaged in advocacy, ensure compliance with the Law of Georgia on Personal Data Protection and the processing of data only if there are grounds specified in this law and in accordance with the principles;
- Prepare a training module for lawyers on personal data protection issues;
- Ensure training of lawyers on personal data protection issues.

To LEPL – Public Service Hall:

- Protect the privacy of personal data of LGBT+ persons and disclose their data only when there are grounds provided for by law;
- Take such organizational and technical measures that ensure protecting security of personal data in the process of communicating with citizens in the service area of the Public Service Hall;
- Provide periodic training/raising awareness of employees on personal data protection issues;
- Ensure regular monitoring of the data processing process by employees, identifying cases of illegal access to data and imposing adequate liability.

To pharmacy chains:

- Ensure that the data of LGBT+ persons are updated based on the submission of an updated relevant document, without any unnecessary delay, within the time limit established by law and that the correct data is processed.

To LEPL – Public Service Development Agency:

- Prepare a manual/brochure for data subjects containing information on the procedures for updating data in other public and private institutions after changing the name, surname and/or gender entries.

To Employer organizations:

- Ensure processing of personal data in compliance with the requirements of the legislation.

To media outlets:

- Observe the 10th principle of the Charter of Journalistic Ethics of Georgia and assess the need for data processing in each specific case;
- Ensure coverage of issues of the LGBT+ community members with particular care, choose the form and scope of their coverage and assess what negative impact the disclosure of information in such a form can have on the private life of a LGBT+ community member;
- Ensure obtaining the consent of an LGBT+ person when disclosing his/her personal data;
- Take all necessary measures when disseminating the data of an LGBT+ community member in a non-identifying form in order to exclude indirect identification of the person (before dissemination, the journalist must make sure that with the material at hand (blurring the frame, changing the voice) and the information provided in the story (residential apartment, house, yard, etc.) identifying a specific subject or linking the disseminated information to it requires a disproportionate amount of effort).

To the Charter of Journalistic Ethics of Georgia:

- Ensure periodic training for journalists on personal data protection issues.

To Organizations protecting the rights of the LGBT+ community members:

- Develop a data protection policy document that will regulate in detail the rules and conditions for the processing of personal data, data security issues, consequences of illegal use of data by employees etc;
- Ensure training of employees on personal data protection issues.

To the Parliament of Georgia:

- "Sexual orientation" and "gender identity" be added to the list of special category of data in the Law of Georgia on Personal Data Protection;
- Institute of data protection officer be introduced in the Law of Georgia on Personal Data Protection for those institutions that process large amounts of data. The existence of such an institute shall increase the data protection standard;
- Amendments be made to the Civil Procedure Code of Georgia, which will allow a case to be discussed in court in a closed session in order to protect personal data.

To the Personal Data Protection Inspector Service:

- Check the legality of data processing in JSC Scientific and Practical Center for Infectious Pathology, AIDS and Clinical Immunology;
- Consider the issue of processing personal data of members of the LGBT+ community in the plan of inspections;
- Collect and publish detailed statistics on the cases of processing of personal data of the LGBT+ community members.