TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Mariami Tsulukidze 165490IVGM

LEGAL AND TECHNOLOGICAL ASPECTS OF PERSONAL DATA PROTECTION FROM STATE AND CITIZEN PERSPECTIVES (CASE OF GEORGIA)

Master's thesis

Supervisor: Katrin Merike Nyman-Metcalf

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Mariami Tsulukidze 165490IVGM

ANDMEKAITSE ÕIGUSLIKUD JA TEHNOLOOGILISED ASPEKTID RIIGI JA KODANIKU PERSPEKTIIVIST (GRUUSIA NÄITEL)

Magistritöö

Juhendaja: Katrin Merike Nyman-Metcalf

Tallinn 2018

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Mariami Tsulukidze

03.05.2018

Abstract

The rapidly developing field of information and communication technologies has become a significant part of the modern administrative agenda, enabling states to be governed in a smart and seamless manner. ICT-based services increase the need for collecting personal data in order to correctly identify citizen behind the gadget, process his/her request and provide the service in need. Technological possibilities to store/process limitless numbers of provided personal information subsequently give rise to concerns about its safety and rightful usage.

Therefore, with the increasing importance of data privacy in mind, this thesis aims to investigate the process of personal data protection within the frame of e-governance, mainly focusing on available legal and technological protecting mechanisms, their practical usage and importance for realizing principles of good governance in the state.

The scope of this research is defined by the protection of state databases containing citizen's personal data. Its key legal and technological aspects are identified and analyzed with emphasis on the audit trail logging mechanism, which is to be incorporated into e-databases for tracing activities of public officials who access/use the personal data in question. The potential of proper data protection to act as the enabler of e-governance services success is also evaluated. Moving on, qualitative exploration of defense mechanisms in practice at Georgian governmental entities is conducted, followed by investigating citizens' perception of their data safety and knowledge of existing monitoring mechanisms. Finally, guidelines and recommendations are formulated for improvement and raising citizens' awareness on data protection mechanisms for future consideration in theory or practice.

Keywords: e-government, personal data, state databases, audit trail logging, citizen's awareness, Georgia

This thesis is written in English and is 58 pages long, including 7 chapters and 12 figures.

Annotatsioon

ANDMEKAITSE ÕIGUSLIKUD JA TEHNOLOOGILISED ASPEKTID RIIGI JA KODANIKU PERSPEKTIIVIST (GRUUSIA NÄITEL)

Kiirelt arenev info-ja kommunikatsioonitehnoloogia valdkond on muutunud kaasaegse halduslik tegevuskava oluliseks osaks, võimaldades riigijuhtimist nutikal ja sujuval moel. IKT-põhised teenused suurendavad isikuandmete kogumise vajadust seadme taga oleva kodaniku korrektseks identifitseerimiseks, tema taotluse töötlemiseks ja vajaliku teenuse pakkumiseks. Tehnoloogilised võimalused varuda/töödelda piiramatut hulka esitatud isikuandmeid võivad hiljem põhjustada nende ohutuse ja õige kasutusega seotud probleeme.

Seega, arvestades andmete privaatsuse suurenevat tähtsust, on käesoleva lõputöö eesmärgiks uurida isikuandmete kaitse protsessi e-valitsemise raames, keskendudes peamiselt olemasolevatele õiguslikele ja tehnoloogilistele kaitsemehhanismidele, nende praktilisele kasutusele ja hea valitsemistava põhimõtete rakendamise olulisusele riigis.

Selle uurimustöö ulatuse määratleb kodanike isikuandmeid sisaldavate riigi andmebaaside kaitse. Selle peamised õiguslikud ja tehnoloogilised aspektid tuvastatakse ja neid analüüsitakse põhirõhuga auditijälje logimise mehhanismile, mis on lisatud e-andmebaasidesse, et jälgida riigiametnikke, kellel on juurdepääs või kes kasutavad vastavaid isikuandmeid. Samuti hinnatakse nõuetekohase andmekaitse potentsiaali tegutseda e-valitsemise teenuste edu võimaldajana. Edasi teostatakse Gruusia valitsusasutustes kasutuses olevate kaitsemehhanismide kvaliteetne uurimine, mille järel uuritakse kodanike arusaama oma andmete ohutusest ja olemasolevatest seiremehhanismidest. Lõpuks töötatakse välja suunised ja soovitused inimeste andmekaitsealase teadlikkuse parandamiseks ja tõstmiseks tulevikus nii teoorias kui praktikas.

Võtmesõnad: e-valitsus, isikuandmed, riigi andmebaasid, auditijälje logimine, kodaniku teadlikkus, Gruusia

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 58 leheküljel, 7 peatükki, 12 joonist.

List of abbreviations and terms

ACL	*Access Control List*
CoE	*Council of Europe*
DCFTA	*Deep and Comprehensive Free Trade Area*
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
EaP	*Eastern Partnership*
ECHR	*European Convention on Human Rights*
ECtHR	*European Court of Human Rights*
EDPS	*European Data Protection Supervisor*
EU	*European Union*
GDPR	*General Data Protection Regulation*
G2B	*Government to Business*
G2C	*Government to Citizen*
G2G	*Government to Government*
ICT	*Information and Communication Technology*
ID	*Identity Document*
IoT	*Internet of Things*
KSI	*Keyless Signature Infrastructure*
LEPL	*Legal Entity of Public Law*
RO	*Research Objective*
RQ	*Research Question*
UDHR	*Universal Declaration of Human Rights*

Table of contents

List of figures

1 Introduction

1.1 Overview of the research

Analysing right to privacy in a digital age has spurred a number of continuous discussions within various states and international organizations for the present decade. Along with harvesting the benefits of the modern technologies and offering electronic services to the citizens, governments are often confronted with the need for more sophisticated protection mechanisms to prevent data disclosure and adhere to established standards. Although maintaining privacy in IoT (Internet of Things) era is often compared to "shooting at a moving target" – all data controllers are obliged to "keep on shooting". One could even argue that such obligation has a stronger moral basis for the governmental authorities compared to the private sector because here personal data collection occurs on legal basis instead of being given voluntarily by the citizens. Therefore, by neglecting data safety aspect of the e-governance, states run the risk of data leakage and losing the trust of the citizens as a result.

Such risks together with overwhelming invasion of ICTs (Information and Communication Technologies) into modern governing agenda have been adequately acknowledged and evaluated in a recent resolution by United Nations titled "The right to privacy in the digital age" [1] which for the first time asserted the applicability of internationally recognized human rights including right to privacy in the online world in the same manner they stand applicable to the offline activities of the states. The Resolution stressed the importance of government commitment to guarantee citizen data privacy and encouraged member states to take active measures for establishing digital environment reflective of the widely accepted fundamental rights and freedoms.

Ever-increasing importance of the data safety is also reflected in the rapid establishment of personal data protection inspectorates and DPAs (Data Protection Authorities) within and outside of EU (European Union). Despite being founded by state budgets, these governmental bodies serve as independent data protection authorities, mirroring functions of EDPS (European Data Protection Supervisor) in their respective states to ensure incorporation of data protection mechanisms into the public policy.

After proclaiming its aspiration to become a member of the EU, Georgia, one of the EaP (Eastern Partnership) states, has taken responsibility to get compliant with abovementioned standards. On the way to rapprochement with the union, a number of ambitious commitments are to be put into practice. Upon signing the Association Agreement in 2014, [2] Georgia has undertaken the obligation to harmonize legislation with European standards regarding users' rights, personal data security and protection along with promoting e-government initiatives and supporting their active use for G2G, (Government to Government) G2C (Government to Citizen) and G2B (Government to Business) interactions.

Therefore, the Georgian government is challenged to introduce digital counterparts for the majority of its public services while at the same time adhering to the European standards of personal information safety, which is the core requirement for these initiatives to succeed and become appealing for users. While a number of positive reforms have been made in this direction recently, unfortunately, many of the obstacles are still to be overcome, available services differ in level of security for the processed personal data from one public entity to another and user turnout remains low for their majority.

Therefore, this thesis aims to dive into analyses of legal and technological aspects of e-governance for facilitating the creation of secure e-services, respective of the right to privacy and personal data safety to ensure citizen participation and overall success of digital governance in Georgia.

1.2 Thesis motivation

While the safety of digitally processed personal data has been scrutinized from an unlimited number of aspects, angles and dimensions, my interest towards it owes its existence to the widely accepted notion of its fragility. Whereas transparency, accountability and service accessibility are repeatedly named as benefits of digital government – data security rarely makes it into that list, but rather on the contrary; digital processing is often presented to be a sacrifice of safety over convenience. Endangering personal information is portrayed as a price one must pay for enjoying the luxury of casting election vote without having to leave the house or signing contracts electronically. These preconceived notions are undisputedly more relevant for some states compared to the others and Georgia with its unsatisfactory level of digital literacy [3] and a long history

of living within a hostile union[1] possesses all the prerequisites for such opinions to be easily propagated. If we examine the case of implementing IDs (Identity Documents), it becomes clear, that besides religious activists first cycle of implementation was resisted by equally strong civil movement in Georgia – urging to restrain from taking digital IDs as they were believed to endanger data security of the recipients [4], [5]. Such concerns continue to circulate among press and academic circles until this day, notwithstanding eight years since its deployment and more than two million users [6]. The issue of digitally stored personal data has remained the source of distrust in between Georgian government and society, and for this reason getting to know Estonian approach towards this issue has been very beneficial for the author of this thesis, as it provided new insights along with motivation for more thorough analysis.

The presented research can be useful for solving number of practical challenges: first, it will evaluate the standard in Georgian public entities regarding personal data protection and examine it against widely-spread perceptions among citizens, moreover, it will help to better understand how big of a role these perceptions play in forming public opinion towards e-services and e-governance in general. Despite ambitious intentions of the Georgian government to move considerable number of the public services online, - their efforts are doomed to remain futile without user engagement and therefore this thesis intends to understand the motives behind citizens' distrust, offer potential solutions for changing public perception and pose as motivator for the future researchers to broaden the understanding of this issue.

1.3 Research questions and objectives

This research is built around examining the safety of electronically processed personal data in Georgian public institutions on the premise that achieving high security standard is vital to successful implementation of e-governance. In the process of transitioning from traditional to electronic governance, Georgia is challenged to tackle a number of stressing matters and offer redesigned public services in a secure, trustworthy and user-friendly environment. Maintaining proper level of citizen data security is an essential prerequisite

[1] First Republic of Georgia was occupied by Russian armed services in 1921 and forced into The Union of Soviet Socialist Republics (USSR) in 1922; country remained member of the union until its collapse in 1991.

for achieving service diffusion since common perception that e-services increase the probability of data disclosure is likely to enhance the sense of foreboding among citizens and make them reluctant to participate. To address this issue and specify the scope of this thesis, the emphasis has been put on investigating legal and technological aspects of protecting state databases containing citizens' data. Citizens' perceptions regarding their data safety will be assessed and examined against the current situation in Georgian public institutions to draw relevant conclusions based on the results. Below-presented questions were drafted to guide the research process for the thesis:

- *RQ1: How can legal and technological aspects of electronic governance be used to ensure personal data protection?*

Answering this question will allow thorough analysis of available electronic tools for ensuring personal data security which is stored in governmental databases. In response to the widespread perception regarding lack of adequate safety measures for mitigating digital threats to data, existing safety mechanisms will be described and evaluated (with emphasis on the audit trail logging, so-called digital footprint feature).

- *RQ2: How are Georgian government entities adapting to suggested data protection approaches in practice?*

Expanding on this question will allow examining the current state of electronic databases in Georgian public institutions to find out whether they comply with internationally accepted standards and guidelines or not. Challenges and achievements from the service provider perspective will be highlighted to paint a full picture of the present situation.

- *RQ3: What is the citizens' level of awareness about data protection mechanisms and how to define it as a factor of e-governance success in Georgia?*

To conclude, how do citizens estimate the current level of security of their personal data which is collected, stored and processed by state authorities, will be assessed. Their level of trust towards digital processing and overall mental outlook regarding e-services will also be gathered and analyzed. The potential of establishing secure e-environment to increase citizen participation will also be estimated.

In order to provide all-encompassing and comprehensive answers to the presented questions, preference was given to qualitative methods of the research for collecting empirical data. Additionally, following research objectives were drafted to establish agenda for the analysis.

RO1: Conduct a literature review to identify and analyze key legal and technological aspects of protecting databases containing personal data within the frames of e-governance

RO2: Investigate practical adaptation of suggested data protection mechanisms by Georgian governmental entities using qualitative methods (conducting interviews with multiple state officials)

RO3: Explore citizens' perception of their data safety and awareness of existing monitoring mechanisms by employing qualitative methods (distributing online surveys)

RO4: Evaluate the potential of proper data protection to act as the enabler of e-governance services success in Georgia

RO5: Formulate guidelines and recommendations for improving the level of data protection and raising citizens awareness on monitoring mechanisms at their disposal.

This thesis consists of seven chapters and is structured in a way that a separate chapter is allotted to each research question. Introduction is followed by Chapter 2 where new General Data Protection Directive is introduced and its potential effects on publicly-held personal data processing are overviewed. Following Chapter 3 delves into the theoretical background of the right to privacy, familiarizing readers with the theory of Restricted Access. In Chapter 4 respectively, interdependency between data security and e-governance success is outlined together with the overview of legal and technological instruments for maintaining a secure electronic environment for personal data. This chapter serves to answer RQ1. Moving onto the Chapter 5, case study research is introduced, collected data from the Georgian public authorities is presented and analyzed to formulate an exhaustive response to the matters posed in RQ2. The topic of personal data protection is examined from the user perspective in Chapter 6, by the means of citizen surveys. Public opinion is presented and scrutinized together with evaluating the capability of securing personal data to promote e-governance among citizens of Georgia. This chapter covers circumstances put forward in RQ3. Finally, thesis ends with the conclusion and future recommendations for combating challenges on the way to achieving the secure digital environment in Georgian public sector.

1.4 Research design and methodology

After formulating presented research questions suitable methodology was adopted to allow rigorous investigation of the topic. Analyzing specifications of citizens' data safety in Georgian administrative e-environment called for gathering in-depth observational evidence and therefore qualitative research methods were given priority.

Term qualitative research stands as a multimethod tool of choice for exploring, understanding and evaluating new phenomenon through empirical and interpretive analysis of its representations. Chosen methods best serve the purposes of presented research for multiple reasons: first and foremost, they allow describing situation through individuals' perceptions and experiences which is particularly important for citizen awareness component of this study. Moreover, they investigate new phenomena through means of observation and for this reason they are extremely context sensitive, enabling analysis of the matter in question with respect to its surrounding social and historical circumstances. Yet the most prevalent reason has to do with the fact that, qualitative methods are deemed appropriate and frequently employed by the academics when the field of research is new and has not yet been examined sufficiently. The main focus of the presented study is the fields of information systems and e-governance which meet the named criteria owing to their novelty and dynamic nature. [7], [8], [9].

Logical reasoning of this thesis takes bottom-up, so-called inductive approach, which starts with observing specific interactions and builds upon the further analysis of their results. Inductive approach is justified when the research topic has not been studied sufficiently yet and information gaps continue to exist. The matter of personal information security is yet to be amply addressed in scholarly works for this particular sample (Georgian governmental institutions) therefore, it is best explored by the inductive approach. Qualitative methods are regarded useful for inducting approaches in academic literature because they capture the phenomenon in its entirety and allow thorough contextual analysis [10].

Yet another justification for using qualitative approach comes from the 2002 report by J. E. Grunig, [11] which gives preference to qualitative methods when research is assessing relationships in between organizations and the general public. The report argues that qualitative methods grasp the motives of all stakeholders and show how perceptions of both sides (Governments and citizens) correlate with each other. Displaying such correlation of viewpoints on data safety allows comprehensive empirical analyses of both sides of the spectrum for the presented research.

The type of the qualitative research employed in this thesis will be the exploratory case study. In their essence, case studies are comprehensive analyses of chosen matter which can be anything starting from an individual person or a conundrum all the way to the whole institution or a society. R. K. Yin recommends using case studies when these three conditions co-exist:

1. The researcher has no control over behavioral events
2. Study focus is shifted towards contemporary occurrences
3. Research questions are formulated starting with "how" or "why" [12].

All these prerequisites are present for this research.

1. Author of this paper has no means to influence the behavior of the subjects analyzed in this thesis
2. The study deals with personal data security, which is one of the most pertinent matters currently
3. Research questions are formulated using "how" interrogative pronouns. The only exception is the first part of the third question, which is posed in a form of "what" indicating exploratory nature of this case study.

This thesis aims to explore security aspects of publicly held personal data based on the case of Georgia and by specifying the area of interest two units of analysis were defined. First one has to do with security features of governmental databases and the second one is related to users' perception of data safety. Distinguishing multiple units of analysis within the same case study puts this research into embedded, single-case design category. When it comes to choosing sources for collecting data, qualitative case studies offer a wide variety of options. Combining multiple sources of evidence is strongly encouraged in scholarly literature for achieving data triangulation and ensuring the validity of the outcomes [8], [10], [12].

Therefore, priority was given to two independent sources of data, namely, face to face interviews and online questionnaires. Both are primary sources and their usage is justified by the benefits they entail: first, they are collected for this specific study and can be conveniently tailored to answer research questions directly; moreover, the evidence they contribute is current and up-to-date which enables accurate mapping of the present situation and finally, they convey personal attitudes, conjectures and biases of respondents which allow contextual analysis of the phenomenon [13]. It must be mentioned that lack of secondary sources (studies, surveys or published articles) on the given topic also stressed the need for first-hand data gathering. Seven interviews have

been conducted in total from five different administrative institutions during face-to-face meetings. Respondents were either head of the specific institutions or employees designated on personal information safety. All interviews were conducted in Georgian language and transcribed, translated and then coded afterwards. Interviews were semi-structured and allowed going beyond pre-written framework. Respondents were permitted to follow up, expand and stir focus towards the matter which emerged in the course of conversation. Conducting semi-structured interviews is regarded beneficial for exploratory case studies as they serve to capture interviewees' attitudes and points of view and at the same time expose research topic from the new and entirely unfamiliar perspective, allowing discovery of its hidden aspects [7], [14].

Assessing citizens' awareness level about data-protective mechanisms requires first-hand empirical evidence and therefore, multiple-choice questionnaires have been drafted and distributed online, targeting citizens of Georgia for getting an insight into their perspective. To increase the credibility of outcomes, goals and motivations for collecting data were outlined explicitly at the beginning of survey and it was made sure that participants clearly understood the contextual framework. Following the guidelines from academic literature, the questionnaire was designed in a way to compel participants to select only one answer from the suggested list to provoke in-depth reflections on the posed matters. At the same time to cover a wide spectrum of potential responses, options such as "other ", "I do not know" or "no opinion" were also included [15]. Results were analyzed and converted into the form of descriptive statistics for presentation.

Adopting such questionnaires is rather prevalent and well-established method for the purposes of qualitative exploratory research and they are often employed to study empirical diversity in an examined sample. They are characterized by ease of distribution, time-efficiency and broad geographic coverage, moreover, they eliminate observer influence by providing standardized stimulus for every respondent [16], [17]. All these aspects also served as motivators when picking the method of choice within the frames of this research.

The reasoning behind selecting each of these methods along with their advantages was presented in this chapter, their risks and limitations will also be discussed in forthcoming paragraphs upon analysing outcomes of each method respectively.

To be in line with its explorative nature, this research will outline new insights into the security of publicly-held personal data; recommendations and potential solutions for existing problems will be suggested with an aim to lay down grounds for future reforms.

2 GDPR: e-Volution of data protection

Matters related to protecting personal data have made their way to the agenda of contemporary policymakers, scientists and legal experts and are likely to maintain relevance within and beyond EU for at least the coming decade and presumably even further. Although multiple reasons can be named for such limelight, GDPR (General Data Protection Regulation) [18] is undisputedly the biggest catalyst of recent discussions and it is impossible to provide an all-encompassing overview of data protection while evading it.

By the time of this writing, GDPR is nearing the end of its two-year implementation period and is planned to come into full force starting from 25th of May 2018. The Regulation is part of EU data privacy reform and comes in a package with directive 2016/680 concerning data processing related to criminal offences [19] which was adopted alongside the regulation with effect from 6th of May 2018. The latter is intended to cover the areas left outside GDPRs' scope of influence and these two together with another *Lex Specialis*[1] regulation on e-Privacy[2] make up the essence of data protection reform package proposed by European Commission.

GDPR is proposed to replace the data protection directive from 1995, [20] which served as the basis for legislation of numerous states within and outside EU – including Georgia [21]. There are a number of key advantages associated with its implementation. GDPR will be binding in its entirety and directly applicable to every state inside the union, unlike its predecessor, which was transposed into legislation individually by each state as they considered appropriate. Such wide discretion gave rise to differences and peculiarities of security requirements and resulted in data localisation restrictions which hinder achieving

[1] *Lex specialis derogat legi generali* – legal maxim implying that special law prevails over the general one

[2] Regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications was planned to come in force together with GDPR, but in latest report European Council regarded proposed date of application unattainable and its implementation has been put on hold for the time of this writing. Report available: http://data.consilium.europa.eu/doc/document/ST-9324-2017-INIT/en/pdf [Accessed: 21-Apr-18]

trans-border interoperability and the free flow of data within EU. By setting common security standard GDPR makes a crucial step towards achieving data portability inside the union. Another compelling cause for its adoption can be found in rapid technological developments, which have taken an unforeseeable turn since very first laws on data protection were drafted. Both technological and social aspects of ICTs have grown more influential and sprung the necessity to reassess their legal boundaries to tilt the scales in favour of maintaining privacy [22].

GDPR offers precise formulations of already existing privacy principles (fairness and lawfulness; purpose limitation; data minimisation; information accuracy; storage limitation; data integrity and confidentiality) and introduces several mechanisms for guaranteeing their realization in practice [23]. These mechanisms and their presumed effects on data processing for e-government purposes are as follows:

- *Storage limitation*

Article 5(1) of the regulation limits data processing to the purpose it was originally collected for and prohibits its prolonged retainment beyond achieving the primary goal of collection. Abovementioned obliges data controllers to either anonymize or destroy such recordings unless their preservation can be justified by public interest or historical and statistical reasons. In the context of state repositories, it must be pointed out that this limitation still makes data retention possible for public authorities even when initial purposes of gathering did not include data archiving, however, public authorities are to balance this entitlement against rights of an individual with respect to individuals fundamental right to privacy [24].

- *Matter of consent*

GDPR makes effort to change the prevalent notion of so-called opt-out consent where it is presumed given unless declined explicitly by the data subject. Article 4(11) of the regulation requires the cumulative existence of following prerequisites for its validity: "freely given, specific, informed and unambiguous indication of the data subjects wishes" [18, Art. 4(11)] which is at the same time expressed by "statement, or clear affirmative action". Additionally, consent must be verifiable with the possibility to be revoked in future. However, GDPR acknowledges five exemptions under which data processing is regarded lawful without consent and they stand more relevant for the purposes of state institutions since meeting the legal obligation of an institution and meeting the public interest or other legitimate interests of public organization represent the most common legal basis for the actions of governmental bodies. (Art. 6) Although regulation does not

go into the details of what can be regarded as "legitimate interest" here, from overall analysis it can be deduced that data controller's ability to justify every action taken against data will have a decisive role when evaluating its legitimacy [24]. While some actions might be regarded lawful, (storing data without depersonalization for example) others can be considered too pervasive into individual's privacy (such as making same data publicly available).

- *DPOs and mandatory notification of data breaches*

Section 4 of the GDPR (Articles 37 to 39) is dedicated to setting out roles and obligations of DPO's (Data Protection Officers), which are to be appointed by any organization (public and private) which establishes direct contacts with data subjects. Appointed officers are to assess the overall level of information security within an organization. They must be involved in any process which entails processing personal data [25]. Ministries, big agencies and other governmental entities which experience data breaches likely to cause considerable damage, are obliged to notify concerned individuals under the requirements of Article 34(1). The latter has been regarded difficult to attain in practice among experts due to the fact that as broad spectrum of events can be implied under the term "breach" – everything from loss, deletion, alteration and disclosure all the way to unauthorised internal access to the data will have to be conveyed to the data subjects. This would require attaining detailed description of malicious actors' activities together with close surveillance of employees on daily basis [26].

- *Right to be forgotten*

Regulation equips data subjects with the ability to object any form of processing upon their personal data done by public institutions – even when the processing is in accordance with data controllers' statutory obligations. According to Article 21, if such request is made and governmental institution fails to demonstrate legitimate grounds for intrusion into privacy, it is obliged to discontinue processing personal data. An even higher standard of protection is introduced when data in question is made available to the public. The right to be forgotten, which is derived from the EU Court of Justice decision on a case "Google Spain v AEPD and Mario Costeja Gonzalez", [27] has found its way into the Article 17 of GDPR, demanding the removal of irrelevant information upon request of the data subject. Right to be forgotten can be exercised when published information was processed in an unlawful manner, is inaccurate or no longer necessary for the publication purposes. Article 17(2) additionally obliges data controller to notify any other authorities with whom data in question had been shared about the request and ask for the

removal of any copies /replications in their possession. This is a very powerful tool in the hands of data subjects, and if implemented correctly, will grant them the possibility to appeal to a single governmental institution which, in return will facilitate removing the publication from whole governmental network [24].

- *Privacy by design and default*

Outlined in Article 25, privacy by design and by default represents the backbone of regulation, moving the starting point of data controller liability before data processing begins. Building electronic systems with data safety in mind require applying appropriate technological and organizational measures at preliminary stages of software development together with the ability to explicitly demonstrate their existence. Privacy by default guarantees that data processed is no more than what is necessary for achieving a specific purpose, and at the same time ensures that preconceived status of personal information is always private, unless explicitly stated otherwise.

In scholarly literature the requirement to demonstrate compliance with privacy by design has been heavily criticized for supposedly increasing paperwork and legal costs of data controllers while having no real necessity as systems are already being built with privacy in mind [24]. This argument, however logical, loses its ground when examined in the context of influence GDPR will have on third countries processing data of EU citizens. Guaranteeing outright safety of EU citizens' data involves keeping it secure while processed outside of the union borders as well and since many states fail to adhere to internationally accepted privacy standards for databases until this time, GDPR privacy by design requirement can serve as strong legal basis for demanding higher level of privacy for the member states' citizens.

While presented requirements appear rather burdensome if evaluated out of context, it needs to be mentioned that EU already has somewhat lengthy experience of carrying out data safety statutes and none of the complying states will be starting from an empty page with GDPR. While regulation enhances safety requirements and brings legal framework to a higher level, it is still a logical continuation of its predecessors instead of a drastic and radical twist into a new direction. Its evolutionary nature and coherence with pre-existing legislation are highlighted in scholarly articles pointing out that the regulation is not overriding preceding fundamental principles of data privacy but on the contrary, offers contemporary tools to guarantee their fulfilment [24], [26].

As with any other piece of complex legislation, there are multiple grey areas within GDPR as well, some caused by the intricate nature of the area the regulation tries to manage and

others being the result of discordance in between states when legislation was formulated. Professor D. Svantesson [28] analyses the scope of applicability for GDPR from the international perspective and points at a number of problematic cases, which can arise given the high mobility level of modern society and ambiguity of the "extraterritoriality test" offered by the Article 3 of the regulation. The wide scope of GDPR applicability allows a number of speculations in theory, to the point where any organisation whose users have entered the area of EU can be held accountable under GDPR requirements, which is of course an utopian scenario and well beyond the intentions of European legislators. Therefore, it is left upon practice to come up with the optimal application of prescribed provisions.

Another vague aspect of the regulation has to do with fines when it comes to the state institutions violating data protection standards. Article 83(7) of the regulation leaves it up to each individual member state to decide to what extent financial penalties shall be applied to state agencies mishandling personal data - if at all. Therefore, precise means of ensuring public sector compliance with GDPR will be decided by legislation of respective member states and more importantly by the practical application of offered disciplinary mechanisms [29]. For this reason, it is impossible to speculate on how effectively citizens will be able to protect their data when confronted with public authorities until the regulation is enforced and enough real-life examples are accumulated for observation and analysis.

GDPR is only imperative for the EU member states and will not be legally binding to Georgia, but because of its global impact, its potential to affect third countries is noteworthy. Particularly, two transpiring effects are to be highlighted in this regard: First one has to do with the broad territorial scope of its applicability. Analysis of recital 23 in combination with Article 3(2) of the regulation allows the conclusion that GDPR will be applicable to any data controller/processor which offers goods and services within the union [30]. Georgian aspirations to trade with the union have been acknowledged within the frames of DCFTA (Deep and Comprehensive Free Trade Area) provisions which lay down terms for free trade between Georgia and EU and lower entry barriers to EU market for Georgian entrepreneurs [2]. To benefit from these concessions, Georgian legislation regarding personal data safety must reflect the same values and develop efficient monitoring tools to ensure that Georgian entrepreneurs offer the adequate level of data security before they enter EU single market.

The second point of influence, although more abstract, is undisputedly equally compelling as it has to do with so-called “Brussels effect” where European legislation is known to embody role model for the rest of the world. Researchers often point at recent expansion of national regulations on data security for the current decade [31] and as their number exceeds half of the countries in the world already, it can be observed that their absolute majority has been drafted according to the European approach [32]. On the way to harmonizing Georgian legislation with EU standards, a number of legal acts were drafted with European values in mind including the current law in force regarding personal data protection, the basis of which can be traced back to the requirements of EU 95/46/EC directive [20]. Since the latter is now to be replaced by GDPR, proper adaptations are expected to take place in Georgian legislation as well, however, it is still too early to speculate on their nature until the regulation comes into force and its effects on third countries such as Georgia can be observed.

Since Georgia is beyond GDPR’s scope of jurisdiction and also actual effects of the regulation are impossible to analyse prior its enforcement, this thesis does not intend to go into any further details of this piece of legislation. However, forthcoming analysis of the research outcomes will be made with GDPR values in mind. Since this regulation, although not directly applicable for Georgia for the time being, is undisputedly the strongest available legal tool for maintaining personal data safety. Depicting aspiration to harvest benefits of technological developments without excessive intrusion into the individuals’ privacy.

3 Concept of privacy - Theoretical background

This section portrays an overview of restricted access theory of privacy which offers the comprehensive framework for addressing data privacy challenges that accompany technological developments. The theory is relevant in the context of digitally processed personal information as it allows formulating consistent data safety policy and proposes balanced interconnection between the interests of e-states and individuals.

Despite being traced back to the ancient Roman statutes, the right to privacy as we know it is a relatively new right and modern technological achievements have played the pivotal role in its formation [33], [34]. S. Warren and L. Brandeis first emphasized the need for recognizing privacy as right worthy of protection in an 1890 Harvard Law Review article [35]. They argued that recent inventions were intruding into the domestic lives of individuals and threat that "what is whispered in the closet shall be proclaimed from the housetops" [35, p.195] would soon be materialized unless the right to "be let alone" was actively enforced by the state. An available piece of technology which was then threatening the privacy of individuals and inspired this article was nothing more than a photo camera - nonetheless, the review has spurred discussions on this topic and served as point of reference for the large share of academic works on privacy [36].

The concept of privacy has evolved throughout the years reflective of the technological developments and in addition to the original notion of physical privacy incorporated issues related to intrusion in decision making and unrestricted flow of personal data [37]. Privacy as an instrumental value[1] is closely intertwined with multiple aspects of individuals' life and for this reason, creating a comprehensive theory which would grasp its essence has proved to be a rather challenging endeavour [33], [38]. Existing theories vary in their scope and focus, some perceiving privacy as the ability to control information related to the individual in question (control theory and limitation theory) and others interpreting privacy as interest to stay free of interference (non-intrusion theory and seclusion theory). These approaches, however, are often criticized in the scholarly

[1] Values are regarded instrumental when they are necessary means to some further end. Privacy is not valued for its own sake, but rather for its ability to lead towards respected, undisturbed and dignified life.

literature because of their incomplete nature and inability to interpret all appearances of privacy [37].

One of the most comprehensive and well-grounded theories about privacy is restricted access theory. Its origins can be traced back to 1980s' in the hypotheses of authors such as A. Allen [39] and R. Gavison [40] however, it was only in later works of J. Moor [41], [42] when these original incentives were elaborated and conveyed into a functional theory.

Moor based concept of privacy on three pillars of non-intrusion, non-interference and restricted access to one's personal data. The theory defines privacy as "a matter of the restricted access to persons or information about persons" [42, p.30] and goes on to suggest that it is achieved in a situation where individuals and their data are protected from intrusion, observation and surveillance. Moor puts emphasis on a general term "situation" here to broaden the scope of circumstances to which the theory can apply; it can be interpreted as daily interactions, activities or storing and using personally identifiable information in digital databank [41].

Theory of restricted access divides situations into two categories: naturally private and normative private. The first category refers to a setting when people/their data are protected genuinely due to ambient conditions. For instance, biometric data of a person before his fingerprints are taken is regarded to be naturally private because no one has access to it. Situations with normative privacy, on the other hand, are deemed private by legal, ethical or cultural norms and intrusion into the protected area results in violation of the named right. If in previous example fingerprints were collected in the process of obtaining a biometric passport and then securely stored in a state repository, natural privacy would be lost but not violated. Breaking into a database and publishing collected biometric data online would, however, result in ultimate infringement of legal norms and therefore violate data subject's right to privacy [37], [42].

Restricted access theory recognizes the importance of keeping personal space secure from interventions by introducing the concept of natural privacy but at the same time draws the distinct line between intrusion and violation by incorporating additional situation criteria. The mere fact of intrusion is not enough for violating privacy, it must be additionally asserted that unauthorized intrusion was targeting normative private situation.

Moor restrains from specifying a list of normative private situations and points out that they depend on cultural limitations and moral boundaries of any given society and can differ geographically. Even within one specific community these values are not fixed and

change over time. Therefore, we can assume that every case of intrusion is to be evaluated individually with respect to the context in which it took place before deciding if privacy was violated or not [42].

Restricted access approach suggests creating different zones of protection for each private situation to ensure that personal information is only accessed by authorised people, at right times and for predefined purposes. Necessary means for establishing zones of privacy for electronically stored data include technological solutions such as proper filters, firewalls or authentication requirements [43]. Moor suggests that when protected zones are built properly in digital environment individuals enjoy the higher level of privacy compared to traditional paper recordkeeping practices. This is because computing allows restraining all the unnecessary encounters and keeps the list of authorized personnel to the bare minimum.

This theory is very important in the context of digital state and e-governance because of the moderate approach it takes in between technology and individual. It acknowledges ways in which technologies enhanced data safety while at the same time suggests an optimal approach for keeping future innovations on the right track to protect individuals' privacy and personal data.

Moor argues that even computing power, which is regarded as most hazardous to personal data, has contributed to making individual lives more secure and portraying technological advancements solely in the context of threat to the privacy is counterproductive. Employing the theory of restricted access directs discussion towards formulating new zones of privacy; evaluates whether specific situations need access restrictions and if yes, then what types of restrictions would prove the most effective - in this way technology can become part of the solution.

The presented concept obliges governments to apply appropriate restrictions to personal information which was accumulated upon introducing e-services so that users can feel protected from violation of their normative privacy while they harvest benefits of the digital world. Establishing zones of privacy and employing proper technological mechanisms for their realization has the potential to make e-services even more secure than their traditional counterparts [41], [42].

4 State of the art

This chapter intends to provide the comprehensive analysis of available legal and technological mechanisms for establishing a privacy-friendly digital environment within the frames of e-governance. It starts with highlighting the importance of data protection for achieving high user turnout for e-services. Resonating back to the above-presented Restricted Access theory, the necessary regulatory framework and applicable technological tools for constructing protected zones of privacy in practice will be described. Going further, Estonian outlook on personal data privacy will be examined. Putting citizens in charge of their personal information by offering practical monitoring tools helped the state to find the optimal balance between data protection and digital service provision and resulted in high saturation of public sector with e-services. Therefore, Estonian experience can be exemplary for other countries which strive for establishing e-Democracy. Presented conclusions, guidelines and best practices will contribute to fully answering RQ1 as well as to the forthcoming analysis and evaluation of the Georgian case.

4.1 e-Governance and data protection

Incorporating ICTs into public administration has amplified state capabilities to generate and process massive amounts of personal information simultaneously, which led to establishing e-governance and ultimately more citizen-oriented public services.

Data processing by the public sector has several peculiarities which make preventing privacy invasion a rather intricate and obscure matter. First and foremost, states collect data on the legal grounds which not only deviates the submission costs towards the citizens but also deprives them of ability to refuse such collection. Unlike the private sector, governments are not encouraged by the market stimulus to set boundaries for the amount of gathered personal information and hence, are inclined to assign less importance to the mere fact of data collection. Third aspect and perhaps the most crucial one comes with the fact that anonymising or pseudonymising sensitive information is often unfeasible or even prohibited for administrative purposes and sensitive information which

allows identifying an individual is kept in the state repositories so long that it can even outlive the data subject [44].

However, multiple empirical studies have found a strong correlation between adequate data protection and e-governance success which serves to counterbalance above described tendencies. Irrespective of their initial proclivities, governments become bound to secure personal information in order to invoke public trust towards e-services they offer. Citizens refrain from using e-portals unless the state has proven to treat their data in a rational, transparent and predictable manner. Sceptical attitude towards security of digital transactions and apprehension that electronically gathered data will be used for illicit purposes were named as prominent reasons for citizens' reluctance in adopting e-governing initiatives by number of published studies and articles [45], [46].

A 2011 study which was conducted in the Netherlands proved that even when people trust good intentions of government and believe that state officials will not misuse confided information, they abstain from using e-services if they are concerned about potential external interventions from third parties [47]. This shows that users' distrust in government capabilities to protect their data from malicious actors also has the potential to hinder e-governance adaptation.

To harvest benefits of digital services, states are challenged to invoke institution-based trust among citizens. This is to be achieved by clearly defining data protection policies, implementing privacy-enhancing technological solutions and ensuring secure and private transmissions of personal information. Research has shown that when the privacy-related concerns are adequately mitigated, users become less sensitive to risk considerations. Potential threats which would otherwise paralyze their actions no longer hold them back from submitting even sensitive personal data through electronic channels. Therefore, it can be deduced that broad diffusion of e-services cannot be attained unless citizens deem them trustworthy, which turns data protection into the essential prerequisite for e-governance success [48].

Frontline for achieving safe data-handling and consequently increasing user turnout within the frames of e-governance passes through the security level of employed electronic document management systems and databases. These systems represent digital replicas of the organization structure and facilitate internal process execution by digitally connecting different departments of a given state agency, multiple agencies within the public sector or even various levels of government (central and local for instance). Digital platforms for workflow management improve internal cooperation, allow optimal use of

state resources and effective provision of administrative proceedings, they represent indispensable tool in the hands of public sector for keeping up with the demands of modern digitalized and accelerated world [49].

Multiple technological models have been proposed for document management and governmental agencies implement the one which best suits their organization structure, intensity of conducted transactions, number of users, type of processed personal data or available financial resources. In practice, they are often tailored to the special needs of authorities and can vary significantly from the architectural point of view. Therefore, distinguishing one technological solution which would best serve the needs of every governmental agency is not only a futile task but also it is rather irrelevant from the data safety perspective. Determinant factor for declaring document management system secure lies in its ability to ensure integrity, confidentiality, authenticity and traceability of each processed file or document.

- Confidentiality refers to preventing illegitimate access. A system must assure that document is only available to stakeholders such as sender or receiver and third parties cannot view its contents during transactions
- Integrity eliminates risks of unauthorised content modification. Effective means must be proposed to prevent not only deliberate illegitimate manipulations but also technical errors which might result in data loss or alteration
- Authenticity impedes third parties from stealing the identity of original sender in digital communications. Systems must include sufficient means for checking sender identity to ensure that document originated from the claimed source
- Traceability guarantees possibility to reconstruct the data transition process in the system to prove who initiated the transaction and who was the actual recipient of the data [50].

Employing any available model of document management systems can be justified from the perspective of personal information privacy as long as above-discussed four components are in place. Besides achieving a prominent level of security for personal data-in-transit within electronic document management systems, it is also important to implement privacy-enhancing mechanisms for stored data-at-rest to establish the safe e-governing environment. Policy and technological aspects of achieving comprehensive information security will be presented in following sub-sections.

4.2 Legal aspect of data protection

One of the most laconic definitions of personal data is offered by CoE (Council of Europe) 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, where it is regarded to be: "any information relating to an identified or identifiable individual" [51, Art.2(a)].

Despite being well-formulated, some aspects of this definition still call for further clarification. Using term "any information" extremely broadens the concept of personal data, covering some of the obvious examples such as name or address of the individual. At the same time other, more obscure cases also qualify as personal information under this definition such as for example the painting child has made about his parents – depicting their traits of character. It also suggests that information does not have to be accurate, correct or proven; even the erroneous information about the individual is treated as personal data. In terms of its content information can be extremely sensitive, concerning health or financial situation of an individual or alternatively, contain more general (less sensitive) facts such as family name or licence plate number [52], [53].

Wording "relating to" suggests that depending on the context same piece of information is sometimes regarded as personal and other times – not. For instance, price of a house which is used to demonstrate real estate costs for the given city does not qualify for being personal information, but on the other hand, if the price of this very same house is used in relation to the person who owns it – this information is protected under personal data legislation [54].

"Identified or identifiable" are probably the most problematic parts of this definition in practice, because it is not always clear what piece of data or combination of data can be considered sufficient for identifying a person. An individual is identified when he or she can be distinguished from the group or other members of the community. Identifiable here means being identified by a person with serious motivation to pinpoint data subject – not hypothetical possibility [52], [54]. To consider any given data sufficient for identifying individual and therefore personal information, the feasibility of finding the person behind it needs to be examined. However, with technological developments came the possibility to put seemingly insignificant pieces of data together and turn them into a significant source of information about the person (the mosaic theory), [55] which on its behalf enlarges the list of information which can be regarded sufficient for identifying data subject.

The term “individual” is self-explanatory in this context as it refers to any natural person regardless of age, gender, social status or any other characteristics [52].

Right to respect for private and family life is enshrined in article 7 of the EU Charter of Fundamental Rights [56]. The obligation to protect individuals’ personal data is also outlined explicitly under separate article 8 of the charter. Human right conventions outside Europe also encompass similar concepts. However, since this particular right to personal information is derived from the broader right to privacy, a number of international conventions imply its existence under paragraphs concerning privacy and refrain from direct stipulations. For instance, Article 8 of ECHR (European Convention on Human Rights) [57] guarantees right to respect for private and family life. Similarly, respect for individuals’ private life has been portrayed into the UDHR (Universal Declaration on Human Rights) by United Nations stating that “no one shall be subjected to arbitrary interference with his privacy”, [58, Art.12] which also serves as legal basis for personal data protection [59], [60].

A similar tendency of non-homogenous approach can be observed when comparing legislation of various states on personal data as well. Some states have opted for drafting separate legal acts regulating either only personal information safety or right to privacy in general. Studies indicate the dominance of this approach by the time of this writing [61]. The second approach, however, calls for adopting a holistic legal framework for e-governance and it has accumulated theoretical support from the researchers of this area due to its presumed capability to facilitate cross-border e-service interoperability. The holistic approach suggests developing single principle law in which all issues impacting e-governance would be integrated, including matters related to the safety of publicly-held personal data [62].

Leaving aside individual preferences of legal drafting techniques, there is a number of other objective reasons which determine the prevailing approach to data safety regulations in every given state. The list of these reasons can include but is not limited to historical or social context, e-governance maturity level or intensity of cross-border data exchange.

Irrespective of the technique of choice, legal framework must reflect an understanding that law is merely a tool to generate insights for desirable end-result and cannot substitute the system itself. Therefore, attempts to turn legal acts into process descriptions by adding more details and parameters only make them less accurate and sometimes even obsolete [63], [64]. R. Kennedy suggests that constructing policies around employed technology

runs the risk of neglecting factors which cannot be measured precisely (human factors or social context) and results in a mismatch between regulation and matter to be regulated [65]. Therefore, legal framework must take a reflective approach when applied to a digital environment to protect basic values such as privacy without becoming too specific and limiting its own regulatory power.

The notion to set legal boundaries for personal data processing (any manipulation of data items) has been depicted within below-presented principles, which offer a broad framework to measure lawfulness of actions taken against personal information. They are enshrined in a number of international treaties and conventions and also carry over in GDPR, they serve as basis for the absolute majority of data protection regulations on national level.

- *Personal data shall be processed fairly and lawfully without violating the dignity of data subject [51]*

Depicted into the article 5 (a) and (b) of convention 108 and further interpreted within multiple decisions of ECtHR (European Court of Human Rights) [66], [67] the principle of fair and lawful processing obliges public authorities to stay within the legal boundaries when interfering with personal data. This means every action they take must be explicitly allowed by law. Additionally, processing must be either in public interest or deemed necessary for protecting rights and freedoms of others. Incorporating element of necessity suggests that interfering with personal data must be an indispensable way to achieve legitimate purpose of state authority and it cannot be validated by ease or convenience.

Requirement for fair data processing forms the basis for holding state institutions accountable to individuals whose data is being processed. Obligation of public organization to keep citizens informed about how their data is being used corresponds with the data subjects' right to make detailed inquiry about the manipulations which were carried out upon his or her personal information. Above-presented principle additionally prohibits data controllers from conducting pervasive surveillance or any other ways of data processing which might result in violating dignity of an individual [68].

- *Personal data shall be obtained and processed only for clearly defined legitimate purposes [20], [51]*

Both Convention 108 and Data Protection Directive assert that legitimacy of data processing will depend on its purpose. This compels state institutions to:

1. Clearly formulate purposes of each activity undertaken in the process
2. Substantiate necessity of conducting these activities

3. Keep detailed record of carried out manipulations against personal data to provide it upon request of DPA or any other supervising authority.

Additionally, this principle prohibits collecting/processing data for unlimited and undefined purposes. It prevents states from unconstrained data exchange within its agencies in ways which contradict the original collecting purpose and prove unforeseeable from the data subject perspective [69].

- *Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed [51]*

This principle limits data collection only to what is directly relevant to the purpose pursued by processing. Implementing legal framework which embodies this restriction is crucial for protecting data subjects from negative effects of modern data storing and processing technologies. Here it must be additionally clarified that presented "data minimisation" principle must not be interpreted in a way that restrains public entities from collecting essential information for administrative proceedings. Even with data minimisation in mind, processed data still needs to be sufficient to allow forming well-informed decisions and attaining legitimate goals of state authority [70].

- *Personal data shall be accurate and where necessary kept up-to-date, it shall not be kept for longer than it is necessary [51]*

This principle holds public authorities responsible for taking reasonable steps to ensure that citizens' data is accurate and up-to-date before using it in daily administrative proceedings. Respectively, data subjects are entitled to address state institutions with request to update, correct or change information about them which is proved erroneous. Here an important distinction shall be made in between updating information and destroying records of its previous state [54]. Under certain circumstances public authorities are entitled to keep note of the changes that took place for archiving purposes (in case of child adoption for instance, while new birth certificate is released by the state old one can be kept in designated repository).

Presented principle allows personal data retention only for the time period which is required to achieve the original collecting purpose. It encourages public authorities to review obtained information with certain frequency and block, erase or destroy entries which no longer prove adequate or indispensable. Once the initial collecting goal has been attained, these data can be kept in state archives only after being anonymised or pseudonymised [71].

- *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data [20], [51]*

This principle encompasses several obligations for data controller authorities including:

1. Drafting comprehensive policy for data processing and identifying employees with access rights to personal databases; customizing their level of clearance corresponding to their job description
2. Implementing necessary authentication mechanisms for entering the database to minimize the risk of unauthorised access
3. Implementing an effective mechanism for assessing the lawfulness of entering the database and recording every activity which is conducted against electronically stored personal data
4. Ensuring physical and technical security of state databases, taking preventive measures against accidental or deliberate personal data disclosure.

The presented list is not exhaustive and due to the peculiarities of processed data (being extremely sensitive or in great volume) public authority might be exposed to additional obligations. Data controllers must be able to demonstrate compliance with safety regulations and data protection laws in force upon request of data subjects or supervising authorities [72], [73].

Available technological tools to guarantee real-life implementation of above-presented principles will be described in the following sub-chapter.

4.3 Technological aspect of data protection

Moving from traditional to electronic governance involves converting citizens personal information from analogue into digital form and creating secure e-environment where it can be processed in accordance with above-described principles. Modern technologies offer several mechanisms to be incorporated into state databases for enhancing privacy. They will be presented below and described from the technical angle.

Access Control

Access control represents the technical realization of written data security policy in any given governmental entity. It arranges interdependencies between system users and stored

data, establishing authentication mechanisms to eradicate illegitimate intrusion from outsiders. At the same time, it prevents legitimate users from abusing granted privileges by the means of authorisation, which entails implementing selective access restrictions to the accumulated personal information based on what individual public servant needs to know to accomplish work-related responsibilities [74].

There are several technological models proposed for implementing access control within state network including *Discretionary Access Control*, *Mandatory Access Control*, *Role-Based Access Control*, *Team-Based Access Control* and so on. Neither of these approaches represents "silver bullet" solution for all privacy-related concerns and they are to be used in combination for achieving best results. Every state entity must consider database context, its volume and role for the public service provision when formulating the technical strategy for establishing access control mechanisms [75].

Discretionary Access Control is one of the most frequently employed methods for achieving data security. It is implemented through ACLs (Access Control Lists), which indicate what particular user can do or see within the system. Their essence can be modelled by a spreadsheet with columns for data files and rows for system users, displaying their interdependency by showing the level of access individual user has to the data in question. This level can range from no access at all to permission to read, execute, modify, transfer, delete or any other combination of possible activities.

This method is deemed appropriate for the digital environments where security is tied to an individual (for example social benefit portal for employees) but fails to provide adequate protection with extensive and dynamic sets of users as it does not allow temporary delegation of authority [76].

Role-Based Access Control has been suggested to make up for the shortcomings of above-presented model. Here, instead of tailoring restrictions on every employee, they are grouped together based on the roles within the organization and hold access privileges similar to others in the same group. Roles become connecting bridges between system users and stored personal information. Instead of giving direct network access to the employee named X which is a leading specialist in a local municipality, access will be given to role for leading specialists and X will be added to the set of users with that role. Keeping employees access privileges up-to-date with their work-related responsibilities is achieved with great ease in systems which take up role-based approach. As it is done by adding/removing the certain user to the role group or relocating him or her from one set to the other without the need for complex technical adjustments in the system. For this

reason, access rights can be easily tailored to the internal modifications, be it public servant changing work position or terminating employment status [74], [77].

Role-Based Access Control model relies on the functional hierarchy and can be applied to any type of database irrespective of its peculiarities within the organization. When it comes to data exchange between various state agencies however, the role-based model fails to accommodate for distinctive attributes of the horizontal relationship between institutions [78].

A number of new modifications have appeared to compensate for this shortcoming, one of them is *Attribute Based Access Control* model which enables collaboration across different agencies based on pre-agreement (memorandum or legal act). The written agreement outlines access restrictions for the consumer organization, limiting clearance only to the data which is needed for fulfilling its legal obligations instead of the whole database. Data provider organization creates an external user account in its system for consumer organization assigning permission on agreed resources. *Attribute-Based Access Control* layer is implemented within shared database, which acts as authorization architecture, intercepting incoming requests from consumer organization and examining them against the agreed framework. If a request proves to be within the limits of agreed attributes, it is authorized and later authenticated/handled as any other internal request, otherwise, it is denied [79].

Named model is deemed appropriate within the frames of e-governance as it facilitates interconnections between various administrative bodies without changing their internal data security architecture.

Audit Trail Monitoring

Audit trails represent detailed electronic records of events concerning user activities, application or operating system. They are also known as digital footprints which improve system accountability by conveying all actions carried upon digitally stored personal information in state databases [80]. Accordingly, three levels of audit trails can be distinguished:

1. System level – which records log in attempts (even unsuccessful ones), log-on identity, date and time of each attempt/executed login, used device identifiers and list of invoked applications inside the system or alternatively failed attempts to access an application

2. Application level – which documents individual events within employed applications. It logs list of events involving information which was viewed, edited, removed, transferred, printed, inserted or manipulated in any other way. Ideally, "before" and "after" state of each modified record will also be captured to allow comparison of current and past versions of the system and reconstruct the full sequence of preceding events
3. User level – which tracks all commands user had initiated, identification or authentication attempts and list of files/resources which were accessed by the user in question. Here actions need to be recorded from commands to see when the user tried to delete a log file (to hide some unlawful actions) [81].

Importance of maintaining the integrity of audit trail data must be pointed out as well. Due to their evidentiary value, they often become targets of intruders and must be protected against modification or destruction. One way to achieve this is by introducing strong access controls to prevent unauthorised access to log files, additionally, digital signatures can be used to turn them into "read-only" format and prevent changes. It is also suggested to store them on write-once devices or alternatively, automatically upload them to a trusted entity in real-time. *Blind-Aggregate-Forward Logging* scheme has also been proposed for large distributed systems since it produces publicly verifiable signatures and eliminates the necessity of abovementioned trusted entity. Each of these mechanisms can be applied individually or in combination to guarantee not only security of created log files but also their confidentiality. The latter is important because log files themselves can also contain personal information of data subjects (for instance, "before" and "after" files of patient history) [82].

For the purposes of governmental databases, event-oriented logs must be audited with regular intervals, the frequency of which depends on the sensitivity of data or the level of its strategic importance. Since these logs are generated in big volumes, manual reviews are not feasible; instead, technological means must be employed for distilling meaningful information from raw data. Such technological tools include audit reduction tools, which automatically remove information with no safety significance (logs for system backups for example). Additionally, trend monitoring tools detect anomalies in user behaviours (transferring big data files or system log-ins outside working hours for instance). Employing attack detection tools are of crucial importance as well, since they call attention to unusual activities suggesting unauthorised access attempts (such as multiple failed log-in attempts in a row) [83].

Audit trail monitoring mechanism brings the element of individual accountability in publicly-held personal data provision. Authorized access to citizens' data which is given to public servants to accomplish their work-related duties can be exploited and abused. Therefore, attaching irrefutable footprint to their actions can deter authorities from misusing their power. Additionally, recorded logs represent an important piece of evidence while investigating incidents which resulted in data destruction or disclosure [84].

Presented list of privacy enhancing technologies is not exhaustive and as technological possibilities for processing personal information grow in capacity their counterbalancing instruments also continue to appear. For instance, using the incorruptible nature of blockchain technology for achieving a higher standard of data security has received a lot of consideration in academic articles and practice lately [85]. Results of its real-life implementation can be further observed in the Estonian example, which will be presented in the following sub-section.

4.4 Estonian approach to data protection

Past decades have been marked with the accelerated pace of revolutionary changes in the history of Estonia, transforming its population from socialistic into technologically-savvy society. The country has digitalized absolute majority of public services and adopted ICTs in daily proceedings of state institutions. Achieving the prominent level of e-governance service maturity has impacted public administration, economy and even international reputation of the state [86]. Being a member of EU has greatly influenced Estonian approach to data protection and formed the basis of comprehensive information safety framework which envisages both legal and technological aspects of the problem.

To stay in line with previously presented arguments and avoid reiteration of already discussed issues, instead of giving a holistic overview of Estonian approach its two most interesting factors will be highlighted. They concern practical implementation of fair and lawful data processing principle and best serve to explain how Estonia has managed to turn data protection from a hindering factor to e-government success to its enabler.

Estonian policy of handling personal data entails giving citizens effective means to check and monitor how governmental institutions process his or her information. The state has

opted for a decentralized approach for public databases which are made interoperable using X-Road – secure data exchange layer. Therefore, from the user perspective e-services by various state institutions have a single point of access via state portal.[1] Once a citizen has logged into this platform, he can access nearly all personal information which state has accumulated about him and even submit inquiries for correcting erroneous statements if the need arises. State authorities who view/use person's data are also depicted on the portal and citizens have the opportunity to retrieve audit trails of those who have accessed their records [87], [88].

Such prominent level of transparency and accountability is achieved by integrating blockchain-based KSI (Keyless Signature Infrastructure) in Estonian e-government applications. Several state agencies including Healthcare Registry, Succession Registry and Property and Business Registries store the audit logs from their databases into KSI blockchain which on the one hand creates strong, immutable evidence of invoked changes and at the same time guarantees their traceability. The system works by creating compact representations of processed data (called hash values) and integrating them into the cryptographic chain so that any attempt to alter the data in question (in our case audit trails) will result in altering their hash value - hence, in the ultimate detection of manipulations.

Blockchain technology allows achieving system accountability without endangering the security of personal data because the latter never leaves the organization premises. Only the hash value is sent to the KSI and it is impossible to convert hash into original data from which it was produced [89].

By the time of this writing, there are around seventy governmental registers and information systems in Estonia affiliated with KSI, allowing citizens to monitor the safety of their personal data via state portal. This list is not exhaustive and audit trails from some state institutions are yet to be integrated into this unified platform [90]. Nonetheless, Estonian incentive to establish distinct policy and give the citizen means for monitoring its practical implementation has resulted in unified and elevated data protection standards across the whole public sector. This on its behalf demolishes barriers for personal information exchange within administrative bodies and allows practical realization of "once only" principle, encouraging an abundance of e-services in the public sector [91].

[1] See: https://www.eesti.ee/en/ [Accessed: 21-Apr-2018]

Estonian digital framework is built around the principle of decentralization. Therefore, instead of consolidating information systems, the country strives for establishing the homogenous standard of personal data protection across them. This approach turns the matter of information safety into an enabler of system interoperability and facilitates wide diffusion of e-governance across the whole state [92].

5 Case of Georgia – State perspective

This chapter portrays current situation in Georgian public sector with regard to the personal data protection. Empirical data presented in this section was gathered during face to face interviews with state officials and serves to provide a comprehensive answer to RQ2. In order to evaluate to what extent have Georgian governmental entities managed to implement above discussed legal and technological mechanisms for data protection in practice, Office of the Personal Data Protection Inspector was approached at the very beginning of this research. A number of pertinent issues discussed during the interview will be presented within the frames of this chapter, including legal boundaries and used technological tools, existing monitoring mechanisms and preventive measures from data disclosure, the frequency of citizen inquiries to the Inspector and most prevalent complaints against governmental authorities. The precise list of the matters covered during the interview can be found in Appendix 1.

Consultation at the Office of Data Protection Inspector alluded to the differences in technological maturity between different organizations within the public sector. Therefore, additional interviews were conducted in four organizations which were selected to represent diverse segments of the spectrum, some with higher e-governing capacity (Public Service Hall and Public Service Development Agency) and others which lack some prominent features of e-governance (Public schools and Social Service Agency). These interviews were done with the aim to provide specific examples. A detailed description of discussed matters is displayed in Appendix 2. Going further, analyses of interview outcomes will be presented, which serve to fully answer the second research question and at the same time provide the basis for workable solutions and future recommendations. The Chapter ends with listing limitations related to the conducted research.

5.1 Current state of data protection in public sector

Besides international conventions and treaties on privacy or data protection Georgia has subscribed to, the state has also enacted several legal acts on the national level which set

boundaries for personal information processing and compel data controllers to safeguard above-presented information privacy principles. Three dominant pieces of legislation can be distinguished for the purposes of publicly-held personal data safety:

- Constitution of Georgia [93] – individuals' right to privacy is guaranteed in article 20 of the constitution, which prohibits any manipulation of personal information without appropriate legal bases
- General Administrative Code of Georgia [94] – categorizes all the information within public institutions into personal information, commercial secret, professional secret, state secret or public information and establishes appropriate legal regimes for each of these categories; reinforcing "private by default" status of personal data
- Law of Georgia on Personal Data Protection [95] – it was drafted in accordance with Data Protection Directive [20] and enacted in 2011by the parliament of Georgia. It represents the primary source of regulation for processing personal information, establishes the institute of Data Protection Inspectorate and defines the scope of its supervising authority.

Personal Data Protection Inspector of Georgia was founded by the end of 2013 and its core competencies include: conducting audits of data controllers, consulting organizations on matters related to data protection, addressing citizen inquiries and raising overall level of awareness regarding information security. All these activities were covered within the frame of the conducted interview. After coding the outcomes, they were divided into six categories which are presented below. Additional interviews from four data controller entities were coded and categorized in the same manner as well and serve to create an all-encompassing overview of the Georgian case.

Document Management Systems

A representative from the Office of Data Protection Inspector pointed out that while Georgian state authorities differ in their level of e-governance adaptation, they all employ technological means for storing/processing personal data to some extent. Although state entities with only paper-based administration no longer exist, governing through the application of fully paperless management has not occurred either. At this point, public services are being provided by employing electronic means together with conventional methods. This is the case for all four state institutions interviewed within the frames of this research as well. A representative of Public Service Development Agency mentioned

that currently they are digitalizing civil records and contemplate to move onto paperless processing by the year 2024 when the digitalization is complete. Here it must be pointed out that the agency was the only institution among interviewed ones which had gone above requirements of current Georgian legislation and appointed DPO. Other interviewed institutions continue to alternate between the named methods, maintaining hard copies of student personal files (Public Schools) and patient histories (Social Service Agency) along with their electronic counterparts.

As it was discovered during the interviews, implementing electronic systems in administrative bodies preceded adaptation of data protection standards and regulations by a decade in Georgia. Software developments for document management started out as a sporadic and idiosyncratic process, lacking trans-organizational cooperation and considerations for system interoperability. As a result, a number of these systems turned out inadequate to ensure proper security level for personal information which is demanded by later enacted law on Personal Data Protection. Furthermore, these systems proved unviable for incorporating secure data exchange channel between agencies from the architectural standpoint.

To tackle this challenge, the government has elaborated unified minimal standard for document management systems, [96] allowing administrative bodies to adapt any software they deemed appropriate as long as its technical features met certain requirements, permitting system interoperability and secure data processing. Such supportive measures have had positive impact on existing conjuncture and up to 70% of public institutions now employ one out of three information management systems created by either Ministry of Internal Affairs (named "e-FLOW"), Ministry of Justice (named "DES") or Ministry of Finance (named "eDocument"). There is still around 30% of institutions which have developed software tailored to their own peculiarities. Thus, they are obliged to incorporate proper technological means to become compliant with abovementioned security and interoperability standards.

Using several pieces of software for effective document management proved to be well-established practice in Georgian state institutions. As three respondents from Public Schools explained they are using various document management systems for facilitating the administrative process, from which most important ones are "e-FLOW" and "eSchool". A representative of Educational Resource Centre elaborated that:

"eSchool is an electronic database containing personal information of the student, including contact information, social status, information about learning disabilities or

special educational needs with medical records specifying the type of disorder. While e-FLOW depicts daily administrative proceedings and is designated for internal purposes of the structural unit."

Public Service Hall stands out from other state organizations interviewed for this research as it represents the intermediary between citizen and multiple state agencies. It can be described as a front office which is used to facilitate effective service delivery based on "one-stop-shop" principle. It accepts citizen requests and divides them in between responsible state agencies (so-called "back offices") if completing specific request calls for collaboration between several of these agencies Public Service Hall ensures effective data exchange in between them. Although Public Service Hall comes in contact with personal information of the citizens, it is not the process owner. It has gained access to document management systems and databases of other public entities based on above described *Attribute Based Access Control* mechanism. As its representative elaborated:

"We access document management systems and databases of other public entities on the bases of law or written pre-agreement to facilitate effective public service delivery. Infrastructure for digital information exchange as well as database integrity and security represent the responsibilities of data controller while Agency ensures establishing the elevated standard of internal data handling (both policy and technological aspects) to avoid data breaches and violating citizens' privacy."

Exchanging personal information among state agencies

As the representative of Personal Data Protection Inspector's Office explained, there is no preferred method of data exchange defined by the legislation. The law demands that transmitted data must be protected from unlawful disclosure regardless of the employed means for the transaction. This gives authorities discretion to agree upon any secure way of information sharing. The representative of the Inspectorate named two most frequent ways for data exchange in practice. Usually, organizations give out citizens' data based on written inquiries they receive from other state entities where legal basis for the request is indicated.

Alternatively, for instance, *"Database for administrative offences is controlled and maintained by the LEPL (Legal Entity of Public Law) under the Ministry of Internal Affairs of Georgia and number of public and private organizations have digital access to this database according to their needs and legally supported interests. Such practices are quite common and this is only one example out of many".*

It was additionally explained that in practice Inspectorate encounters cases where the capacity of admission rights surpasses legal interests of data recipient organization. Lack of technological restrictive mechanisms allows consumer organization to access whole database instead of a needed portion and view more than what is necessary for realizing its legitimate interests.

Attribute Based Access Control Model which was presented earlier in this paper is frequently employed method for facilitating electronic data exchange between various state institutions. As representative of Public Service Development Agency stated their internal databases are the biggest electronic personal data repositories in the country. They are shared with numerous state institutions and organizations from private sector based on memorandums and pre-agreements which define level of access for the consumer organization. Any institution can become data recipient from the agency by submitting written request which is later evaluated with respect to the principles of Law on Personal Data Protection.

Matter of interoperability between three dominant document management systems which were mentioned earlier ("e-FLOW", "DES" and "eDocument") stands as a challenge to be overcome until this time. As three different respondents from Public Schools explained potential complications in practice are avoided by having the data subject place direct inquiry to the institution which possesses needed information. They have provided below discussed example to better explain established protocol. Giving out school graduation certificates requires the cooperation of given school and Public Service Hall. Since schools use "e-flow" document management system which does not allow receiving direct electronic inquiries from "DEC" system employed by Service Halls, graduates are obliged to submit written inquiry for academic transcript at school and once it is provided stamped and signed on paper, take it to the Public Service Hall which then starts processing to issue school certificate for the concerned individual.

The representative of Social Service Agency reaffirmed wide application of the mentioned method. Agency handles citizen inquiries for funding medical treatments and processes highly sensitive data of patients. Decisions on who will be founded/with what amount are made based on diagnosis and suggested treatment which is sent directly from the hospitals via document management system so that data never leaves the secure digital environment. However, when the agency provides partial financing patients need to submit additional inquiries to other state institutions (local governments for instance) for another half of the bill. Since the system does not support digital data exchange in

between two levels of government (central and local), patients' information is printed out and given to his or her family members which then take it to local authorities to submit the request for missing portion of the treatment expenses. As the interviewee stated:
"Data depersonalization is illegal in the agency as the law demands the recipient of public funding to remain identifiable, however list of persons to whom we give patients data is strictly limited to patient personally, his/her spouse, child and parents."

Access control mechanisms

When it comes to legal regulations concerning electronically processed personal data, the only requirement Georgian law on Personal Data Protection asserts is to maintain detailed records of every manipulation. It does not inquire from data controllers to draft written policy for data processing or establish authentication mechanisms such as individual usernames and passwords for every employee who accesses the database. As a respondent from Data Protection Inspectors' Office explained this factor prevents Inspectorate from officially obligating state entities to implement this mechanism. However, based on the previous experience it can be asserted that this is always one of the recommendations inspectorate gives to the data controllers during monitoring and in practice, a number of public entities have built their databases with personified accounts and access restrictions for their employees.

The representative of Public Service Development Agency gave more credibility to this statement by describing implemented access control mechanisms:
"Rights and obligations are outlined for each individual employee and everyone is given adequate access to the personal data reflective of his or her responsibilities in the agency. Software users can only access the system through a software module that is protected by user and password and needs to be changed regularly."

The existence of comprehensive access control mechanisms at Public Service Hall was also confirmed during the interview. Since this organization is given simultaneous access to several personal information databases from public sector entities, considerable attention is paid to preventing internal data mishandlings and unauthorized system entries. List of possible commands which can be invoked by any public servant is narrowly tailored to his or her work-related responsibilities and continuous monitoring of user activities is conducted within the organization.

A representative of Educational Resource Centre also confirmed the existence of access control mechanisms in school databases, explaining that only designated school personnel

is entitled to make changes in student database. While Resource Centre as school supervising authority is authorized to view database content in a "read-only" mode, they cannot make any changes in the system as latter exceeds their prerogatives. Additional two interviews with school representatives revealed nonhomogeneous approaches to electronic data processing. While employees with access privileges have personalized system accounts in both schools, in one case every staff member works in the system under his or her personal account and decisions are drafted in the digital environment. For the second school however, there is a designated employee for electronic proceedings. Decisions are made using conventional methods and administrator later digitalizes final versions of the documents by inserting them into the electronic environment.

Audit trail logs

The legal requirement to implement automatic logging mechanism in databases containing citizens personal information is actively enforced and monitored by Data Protection Inspectorate in practice. The absence of automated audit trails already provides a legal basis for reprimanding and penalizing data controller even without a recorded case of data mishandling and disclosure. Inspectorate has accumulated a myriad of cases regarding automated logging while conducting provisions of state institutions. In practice, government entities often start building the technological framework for depicting "footprints" on personal data in the midst of inspection to avert anticipated financial sanctions.

The representative of Data Protection Inspector's Office mentioned that in many cases database software which was incorporated into administrative processing before enacting the law on Personal Data Protection does not permit technical implementation of audit trail logging mechanism. Therefore, state institutions are compelled to abandon old systems and implement new software/build them from the scratch which demands time and human resources and is proved to be quite costly depending on the organizations' capacity. As a result, getting compliant with legal requirements is a lengthy process in public sector and there are still institutions which violate data processing standards until this time.

Article 21 of law on Personal Data Protection equips citizens with the right to address any institution and inquire who has accessed their personal data, for what purposes and on what legal grounds. Respectively, data controller authorities are obliged to provide such information within 10 working days. However, the law does not specify the format of

provided information and state institutions enjoy broad discretion in this regard, some give out an excerpt of automatically generated logs while others provide a compilation of events picked out from the journals which are filled in manually.

Two out of four interviewed institutions affirmed the existence of fully-functional audit trail monitoring mechanisms in their electronic systems. Public Service Hall and Public Service Development Agency have implemented technological means for depicting all activities of system users. Agency representative mentioned:

"Our electronic system automatically generates logs (so-called digital footprints), every action, including simply entering keywords in a search bar is logged and recorded automatically. Even if the employee enters part of the last name in a search bar – such as "Tsul", or "Match" for example – even this will be logged and recorded by the system."

Social Service Agency operates the system with deficient logging capability. As the representative of the agency pointed out automated audit trails are not created unless changes are invoked within the system.

"Who had access to the information, who viewed the data is impossible to be tracked down. Meaning, unless the user makes any changes in the system – automatic logs (electronic footprints) are not created."

Three different respondents from Public Schools stated that employed digital software does not generate automated audit trails reflecting access or invoked changes into the database. The "eSchool" platform allows authorities in Educational Resource Centre to sort students' data according to the schools they belong to, but the system does not allow more detailed investigation of which public servant inserted students' data from given school and such feature is yet to be implemented.

Filing systems catalogues

Filing systems catalogues are electronic documents published on the web-page of Personal Data Protection Inspector's Office[1] depicting the list of data categories processed by every data controller in Georgia, public and private institutions alike. They are filled out electronically by data controller authority and entail database description, legal grounds for processing, retention period of the data, categories of data, data subjects etc. Completed catalogues are overviewed by Data Protection Inspector and in case of

[1] See: https://catalog.pdp.ge/SearchCatalogue

mistakes, organizations are instructed to correct erroneous entries before they are made available to the broader public.

As one interviewee mentioned it has been four years since the Inspector's Office was established and many organizations have already provided descriptive information of their databases, which gives citizens ability to check what types of information does named institution possess about them. Currently, web-page displays catalogues from 4 304 (four thousand three hundred and four) public institutions.

Every time organizations start gathering new categories of data or change the way they interact with collected personal information, they are obliged to update their electronic catalogues depicting these changes in order to keep catalogues relevant and up-to-date.

Citizen inquiries

One of the responsibilities of Personal Data Protection Inspector's Office is representing the interests of data subjects and acting as the mediator between citizen and data controller authority. With respect to this competency, a respondent from the Inspectors' Office asserted that amount of citizen inquires has increased at least five times for the past couple of years. Data Protection Inspectorate lawyers now review 20 to 30 cases per day which is a significant growth compared to the year of 2015 when daily consultations amounted to single digit numbers. Respondent suggested that this observation shows the tendency of increasing interest in a personal information handling from the public. She proposed several potential reasons behind this impulse:

"It can be the merit of the activities of our organization and raising awareness campaigns we have conducted for the past years. It is also worth noting that, in parallel with technological development, individuals realized that their personal data is in danger and they need to become more active and informed. Furthermore, the events in the society can have catalysing effect as well – public disclosure of videotapes depicting personal lives of well-known public figures for example[1] – it has had a significant effect on how Georgian citizens perceive privacy."

Interviewees from all four public entities emphasized on the readiness of their organizations to give out information on how individual citizen's data is being handled.

[1] Georgian state surveillance has accumulated years' worth of recordings depicting personal lives of politicians and other public persons. Some of those files have been leaked to the public. See more: https://www.rferl.org/a/georgia-secret-tapes-destroy/25019275.html [Accessed: 21-Apr-18]

Public Schools and Social Service Agency practice paper-based method for making such inquiry, obliging citizens to physically arrive at the institution and submit a written request. Public Service Hall and Public Service Development Agency accept electronic queries as well via citizen portal[1] (MY.GOV.GE). Irrespective of the form of request submission (handwritten or digital) organizations have 10 working days to process it and draft the response. Additionally, the interviewee from Public Service Development Agency pointed out that the share of electronic inquiries remains very low until this time and citizens give preference to conventional methods. For the year of 2017 for example, the agency had received 104 requests from citizens regarding personal information processing while only 6 of them were submitted via electronic portal.

Forthcoming sub-sections of this chapter will focus on conveying analyses of presented interview outcomes and discussing matters related to research method limitations.

5.2 Interview outcome analysis

Analysing findings from this study in light of restricted access theory and suggested legal and technological security mechanisms leads to below-presented interpretations which help to give a comprehensive overview of data safety level in Georgian public sector.

Consultation at the Office of Data Protection Inspector together with the interviews of four different data controller authorities facilitated conclusion that Georgian public sector entails wide spectrum of organizations which significantly differ in their level of technological maturity and adaptation of e-governing mechanisms. These factors consequently define the scope of protection they are able to provide for collected personal information. While there are authorities with DPOs and sophisticated privacy-enhancing infrastructure which corresponds to the data protection standards offered by GDPR, they still represent early minority [23]. The public sector is dominated by institutions which are yet to tackle the issue of comprehensive personal information safety and continue to be inconsistent with commonly accepted security standards in one way or the other.

As it was mentioned above, first waves of building document management systems were characterized by the strong focus on organization needs, flexibility and convenience while

[1] See: https://www.my.gov.ge/public/home/index?id=22&type=Main&index=0&p1=22 [Accessed: 21-Apr-2018]

data protection component was left out of focus. In the recent years, a number of important steps have been made to fill this vacuum and establish secure state network, addressing both legal and software-related aspects of the issue. However, some negative impacts of the primal decisions remain as obstacles until this time, hindering its application.

Besides technological difficulties to tailor old systems to new policies, initial inducement to disregard information privacy has had a negative impact on forming public servants' work ethics as well. Examples from Public Schools and Social Service Agency together with overall experience of Personal Data Protection Inspector prove that information privacy is often regarded as a matter of secondary importance in public sector; indulgent feature rather than the essential prerequisite of digital environment. Such attitude comes in fundamental disagreement with the principle of fair and lawful processing which stipulates preeminence of guaranteeing individual privacy and asserts that no potential benefits coming from the e-service can justify the violation of fundamental right [68]. Unless the named matter is given thoughtful consideration, Georgia runs the risk of failure in accomplishing responsibilities undertaken by Association Agreement. As harmonizing with European values entails guaranteeing the practical realization of already discussed "privacy by design and default" principle prescribed in GDPR [24].

Interpreting legal dimensions of the presented findings suggest that existing law in force has managed to incorporate multiple aspects of secure data processing principles and offers sufficient measures for their practical imposition. However, number of its provisions lack the element of specificity, allowing data controllers to exploit such ambiguous sections of the act for their benefit; be it justifying excessive processing or evading accountability in front of citizens. When it comes to citizen inquiries regarding to whom their data has been disclosed for instance, lack of clear-cut requirements for the response format has facilitated the flawed practice of providing data from record-keeping journals which are maintained manually in some public institutions. Such responses obliterate the possibility to detect internal data mishandlings from the employees who might have accessed citizen' data with no legitimate interests since these journals can be easily manipulated and they fail to accurately depict every activity which was conducted against datasets.

The absence of obligation for data controllers to introduce written policy on information security has also resulted in misconducts in practice. Public entities often handle personal information without explicit protocol and list of authorized employees for accessing

certain sets of data. This impedes identifying internal malpractices and allows data controllers to argue for the legitimacy of certain activities as there is no regulation which would regard them unlawful. From the perspective of Restricted Access theory such failure to establish distinct zones of protection for normative private situations results in the ultimate violation of individual privacy [42]. The established practice also comes in conflict with the first principle of fair and lawful data processing and hinders its realization in Georgian public sector.

Limited technological capabilities also have shown to cause problems to data security. Presented examples confirm that the failure to establish interoperable data exchange systems in between agencies materialized the threat of having individuals' sensitive personal information exposed to third persons. Currently, due to the peculiarities of some of the services provided by the state, absence of data exchange platform between public agencies results in an ultimate violation of individuals' privacy (as shown by the case of Social Service Agency). A certain segment of the public entities has managed to establish the working system for data exchange by granting consumer organizations access to their electronic databases. Failure to tailor access privileges to the legally supported interests of consumer organization remains to be the biggest threat to citizens' data security for such cases. Giving out excessive admission privileges comes into conflict with the internationally approved technical standard for data sharing [79] which was discussed in preceding chapters and violates the third principle of personal data processing [70].

Yet the biggest challenge from the technological perspective has been implementing proper audit trail monitoring mechanisms in public institutions. Two out of four data controllers interviewed within the frames of this research appeared to be processing sensitive personal information without depicting automated digital logs of conducted activities. While Social Service Agency has demonstrated the capability of partial logging, such practice is not considered sufficient by internationally accepted standards and guidelines [20], [51]. As it still leaves the possibility for an undetected data breach, especially for the cases which entail processing extremely sensitive information related to the health of the citizens. Annual reports by Personal Data Inspector [73] also describe myriad of personal information infringement cases in this regard within Georgian public sector. Lack of historical consideration for data privacy, fragmented development of document management systems without preliminary plan for accountability and interoperability, limited financial resources of public entities, current work ethics of public servants and failure to acknowledge crucial importance of information security –

all these factors seem to be responsible for ongoing deficit of audit trail monitoring mechanisms in public sector.

As it was described in previous chapters, besides national legislation on data protection, the importance of depicting digital footprints for electronically processed personal information is acknowledged by international regulations, recommendations and global standards [20], [51]. Despite the existence of several institutions with properly functioning logging system and growing trend of incorporating audit trails in databases among public entities, current situation still must be evaluated as unsatisfactory. Unless changes in this regard are accelerated in time and given more homogenous outlook across the whole sector, Georgia risks failing in system accountability component of e-governance, which would consequently damage citizen trust towards the system and hinder broad applicability of e-services [47].

When it comes to practical possibilities to view how individuals' personal information is being handled by state entities, unlike Estonia Georgia does not offer the direct electronic mechanism for monitoring. Research has indicated that even those authorities which accept electronic inquires via citizen portal (MY.GOV.GE) take up to ten days for drafting the response and do not allow direct, real-time checking of public officials' activities. Lack of unified platform for addressing a broad spectrum of public entities with one inquiry obliges individual to make separate requests for each institution which might possess his or her personal data.

Filing systems catalogues which are being published on the official website of Data Protection Inspectorate represent a useful tool for process monitoring as they contain a precise list of data categories majority of public entities own about the citizen. However, they fail to substitute for direct monitoring mechanism which was described in the example of Estonia as they do not depict the exact list of actions taken against specific datasets for given period of time. At the moment, citizens are given the option to either submit electronic requests (for a limited number of organizations) or paper-based inquiries (for every institution) and wait for the answer. Such mechanism is proved to be insufficient for effective monitoring considering the volume of data public sector holds about citizens and accelerated pace of the digital processing. Additionally, it requires disproportional effort from the citizens and runs the risk of being neglected in practice.

To put things into perspective it must be pointed out that while Georgian state has around 20 years of experience with electronic data processing in public sector, it has been only last 7 years since comprehensive personal information security law started to apply.

Office of Data Protection Inspector was established only 4 years ago as first supervisory authority to monitor practical implementation of the legislation. On the premises of presented timeline, it becomes clear that the state of Georgia is still at preliminary stages of getting compliant with internationally accepted personal information security standards. Initial reforms have resulted in tangible outcomes and high standard of security attained by authorities like Public Service Development Agency gives hope for better future. However, a number of stressing challenges presented in this section still need to be tackled by the state for establishing optimal level of protection for the citizen data while at the same time making steps towards associating with EU and its values.

5.3 Interview limitations

When assessing the quality of the research, validity and reliability of outcomes are two aspects most frequently looked at. Validity is measured by evaluating how closely study has managed to grasp the essence of real world; whether findings represent accurate depictions of matter in question or not. Reliability refers to consistency and repeatability of research method; so that every time same case study is conducted by meticulously replicating procedures of the present one – identical results appear [12].

For the exploratory case studies such as this one R. Yin emphasizes two factors which can pose threat to the outcome validity. First one has to do with lack of objective sets of measures for collecting data during interviews. In order to prevent this threat from materializing effort has been made to define explicit trend of focus for this study – which was the security of personal data in Georgian public sector and select specific measures such as its legal and technological aspects. The second threat to validity is the inability to apply outcomes of the research to broader groups or situations besides its original focus. While generalizability is a point of weakness for case studies overall, a number of preventive measures have been taken to increase its coefficient for the presented research including formulating well-supported design or the study, combining information from multiple data sources and applying substantial theoretical base to analyzing outcomes [12].

Reliability of the research can be jeopardized by the couple of factors as well, the first one being insufficient descriptions of the process which does not allow its precise replication in the future. While there were multiple external factors affecting the

conditions in which presented study was conducted that might be impossible to imitate in future (such as transitional period from 95/46/EC Directive to GDPR during which study took place) an effort has been made to present detailed descriptions of the conducted research to increase its reliability. Starting from portraying detailed research objectives and listing all the sources of information all the way to disclosing names of interviewed public entities and including a precise list of discussed topics during interviews.

Second and undisputedly the most poignant threat to outcome reliability is bias. H.I.L Brink suggests that the possibility of selective observation increases when the researcher gathers data personally. Since he or she can be inclined to give prevalence to one type of information over the other subsequent to personal values and standpoints [97]. Besides conducting interviews personally, it also must be pointed out that the author of this thesis has considerable experience of interacting with Georgian state authorities from the citizen perspective and at the same time has accumulated couple years of experience of working in public sector of the named state. While it is impossible to be utterly free of bias, it can be reduced to the negligible amount by becoming aware of its existence from the very beginning of the research and taking adequate precautionary measures. Within the frames of this study named precautionary measures included:

1. Conducting interviews with a neutral tone and in a semi-structured format without stating individual opinions to avoid influencing respondents
2. Recording interviews and creating detailed transcripts of the responses without subjective interpretations
3. When necessary conducting additional interviews from the same institution to neutralize respondent bias and get a precise description of the situation (In case of Public Schools, representative of Resource Centre was also interviewed together with school principals to gain perspective all every stakeholder involved in maintaining the database for instance)
4. Restraining from interviewing representatives of those public entities author has previously worked for and therefore has pre-existing knowledge of the processes
5. Separating facts from the authors' opinions in the paper by presenting them in different subsections, thus allowing readers to make their own conclusions regarding the posed issues.

6 Case of Georgia – Citizen perspective

The embedded, single-case design of this study allows investigating two units of analysis. After having scrutinized security features of governmental databases as the first one in preceding chapter, users' perception of data safety in Georgian public sector will be evaluated below as the second unit of analysis for this research.

To offer a well-supported overview of the matters posed in RQ3 an online survey has been drafted and distributed among citizens of Georgia using social networks and other electronic channels of communication. Overall 419 responses were received through the course of less than two months (from mid-February till the end of March 2018) which serve to bring light to citizens' awareness level about data protection mechanisms employed in public sector. Responses allow studying the empirical diversity of opinions among survey participants. Visualization of descriptive statistics for each question in the survey can be found in Appendix 3.

Overview of questionnaire outcomes in first sub-section of the present chapter is followed by their analyses in order to fully answer the third research question and establish interdependency between publicly-held personal data safety and achieving a high rate of success for e-governing initiatives in Georgia. Finally, risks and limitations for the given research method will be listed and discussed in relation to conducted activities. Outcomes from this chapter together with the ones posed in Chapter 5 will contribute to final conclusions and recommendations at the end of this research.

6.1 Citizens' perception of data safety in public sector

The conducted survey consisted of 12 questions and aimed at understanding citizens' perceptions, factual knowledge, opinions, concerns and overall attitudes towards the matters posed in this study. Survey was anonymous and participants' personal information has not been gathered. Considering limited amount of time for spreading the questionnaire and existing geographic restrictions, a number of received responses (419) can be regarded as relatively high and sufficient for the purposes of this research.

Survey begun by inquiring whether the respondent was aware of the form state institutions use to store his or her personal data. Majority of the received responses – 53.2% (223 respondents) stated they are aware that their data is stored in both forms electronically as well as on paper. 22.7% (95 respondents) indicated that they are not aware of the means employed in public sector for storing personal data. Participants who believe that their personal data is stored solely in digital format by public entities amounted to 17.2% of the total number (72 respondents). 3.8% (16 respondents) declared their lack of interest in this subject as the reason for not knowing how their personal information is saved by the government. Finally, the least popular answer for this question gathered only 3.1% (13 respondents), which opted for the statement that government only employs paper-based solutions for storing their personal information (see Appendix 3, Figure 1).

The second question continued the theme proposed by the first one, delving into respondents' individual preferences for the form of storing data, asking participants to state which one they prefer in terms of safety, electronic method of data storing or paper-based one. The biggest number of responses in this case refrained from making a choice because as it turned out for 48.2% (202 respondents) neither of these options pass the test of safety. 22.7% (95 participants) stated their preference for electronic means of data storage as latter is regarded safer by them. 20.5% (86 respondents) consider both means of data storage to be equally safe and therefore have no preference in between them. Only 6.4% (27 participants) opted for paper-based data storing mechanisms for the security purposes of their information. This question additionally included "other" option, allowing participants to enter their opinions in case they did not agree with any of the suggested alternatives. 9 respondents out of 419 took advantage of this opportunity; 8 out of these 9 responses stated that paper-based options are preferred in terms of being more security-friendly however, they want data to be stored digitally by the state due to the convenience of e-services they can get. Remaining one response stated: "I prefer if the government did not store my personal data at all" (see Appendix 3, Figure 2).

Moving onto the third question, participants were asked to state which sector they trust more to process their data lawfully, public or private. As it turned out, 37.2% (156 respondents) believe that neither of these sectors measures up to the optimal standards and both fail to protect personal data the way they should. Another big segment of polled citizens 33.7% (141 respondents) gave preference to the public sector, stating latter is better at adhering to data-safety guidelines. 14.8% (62 respondents) proved incapable of making a choice - not knowing which sector to give preference. 7.4% (31 respondents)

believe that level of data protection is equal in both sectors while 6.9% (29 respondents) seem to trust private entities more compared to the public sector when it comes to lawful data processing (see Appendix 3, Figure 3).

The fourth question asked citizens to estimate how well-aware they consider themselves to be regarding security mechanisms which are employed in public sector for keeping their personal information safe. 47% (197 respondents) stated that they are somewhat aware of their essence but would like to know more. 33.2% (139 respondents) declared that they are not at all aware of these security mechanisms as latter is beyond their sphere of interests. 14.6% (61 respondents) stated that they are somewhat aware of how their data is protected in public sector without indicating their desire to learn more. A minority of 4.5% (19 respondents) stated that they have precise knowledge of used data security mechanisms by the public sector. This question also allowed participants to make individual entries which were exercised by 3 out of 419 respondents, essentially paraphrasing already offered options of not being aware of data safety mechanisms but wanting to learn about them and not being aware as this topic is beyond their sphere of interests (see Appendix 3, Figure 4).

Going further, the fifth question focused on investigating whether participants trust state institutions that they are processing citizens' personal data in a good faith. Majority of the responses 52.3% (219 respondents) indicated that they trust good intentions of public entities, however, would prefer the possibility of direct monitoring. 32.5% (136 respondents) declared their destruct which is caused by lack of direct monitoring mechanisms. 9.8% (41 respondents) affirmed their trust towards state authorities in lawful processing of their data beyond any doubt and minority of 5.5% (23 respondents) stated that they don't trust governments to process their data fairly and lawfully for some other personal reasons irrespective of monitoring mechanisms (see Appendix 3, Figure 5).

Following sixth question asked survey participants what they considered to be the biggest problem regarding electronic data processing by the state. 37% (155 respondents) chose systems not being secure enough technologically, 26.3% (110 respondents) opted for public servants' possibility to access citizen data without legal grounds, 21% (88 respondents) named government transferring data to third persons as biggest issue, 12.9% (54 respondents) stated violation of data processing principles by public institutions to be the biggest challenge for electronic data processing. This question also allowed participants to input their ideas if they did not agree with any of the suggested alternatives. Overall 12 respondents practiced this opportunity: 5 of them suggested that all of the

listed reasons stand true for Georgian public sector currently, 3 replays withheld from answering due to lack of information, other 2 respondents pointed at bureaucracy and lack of political will in government to establish secure digital space and remaining 2 responses suggested that personal information security is well-attained in Georgian public sector and there are no problems (see Appendix 3, Figure 6).

The next, seventh question asked if participants knew that they can inquire from any public entity to whom their data has been disclosed and whether they had practiced this opportunity in real life. Majority of 50.1% (210 respondents) indicated they did not know of such opportunity, but they might use it in future after this. 35.5% (153 respondents) stated they knew about this possibility but never used it. 10% (42 respondents) declared they did not know of such opportunity and it's unlikely that they will be exercising this right in future either. A minority of 3.3% (14 respondents) confirmed pre-existing knowledge of this mechanism and at the same time asserted that they had taken advantage of this opportunity in the past (see Appendix 3, Figure 7).

Furthermore, the eighth question of the survey inquired if respondents had heard of Personal Data Protection Inspectors' Office and its functions and if yes, whether they have used its services. 52% of responses (218 respondents) indicated that they have heard of such entity but never used its services. 32% (134 respondents) stated they did not know Inspectorate existed before, but they might use its services in future. 12.4% (52 respondents) said they had not heard of such entity and it is very unlikely that they will be using its services in future either. A minority of 3.6% (15 respondents) confirmed that they not only knew about Inspectorate but also had applied to its services in the past. (see Appendix 3, Figure 8).

Upcoming ninth question focused on the experiences of respondents, inquiring if any public institution had violated data safety standards against them by disclosing their data unlawfully, refusing to correct inaccurate recordings etc. majority of the responses 51.1% (214 respondents) declared that they had never had such experience personally and neither have they heard of someone else with such occurrence in their surroundings. Almost equal number of answers 46.1% (193 respondents) opted for the opposing response stating they have not had such experience personally but they have heard of someone else with such occurrence in their surroundings. Only 1.7% (7 respondents) confirmed having had such negative experience personally with state authorities in the past. This question also included "other" option, allowing participants to enter their opinions and this time 5 citizens used this opportunity. Four of them refrained from

answering due to lack of experience/information while one of them stated: "Personal information of third persons was handed over to me by state institutions by mistake" (see Appendix 3, Figure 9).

Question number ten asked if participants supported implementing e-governing initiatives in Georgian public sector such as e-voting or e-prescriptions for instance. 45.1% (189 respondents) stated that they welcome such initiatives and are willing to use them if implemented. 31.1% (121 respondents) indicated that they do not support e-services due to lack of data safety mechanisms. 11.9% (50 respondents) disapproved of such initiatives owing to the non-transparent nature of electronic systems. 10.3% (43 respondents) stated overall support for e-governance but at the same time demonstrated reluctance to use the services personally. 11 respondents chose to make individual inputs for this question. 2 respondents expressed their approval for practical services such as e-receipts but denounced the idea of e-voting for high importance of election system integrity, suggesting it cannot be maintained online. On the contrary, 1 respondent accepted the idea of moving political processes online and opposed the notion of social services going digital such as medical prescriptions for instance. 2 respondents expressed readiness to consider using e-services only if the system will be transparent and secure. Remaining 6 respondents abstained from responding due to lack of knowledge on this topic (see Appendix 3, Figure 10).

The eleventh question focused on investigating factors with the biggest potential to increase citizens' trust towards e-services in Georgia. 36.3% (152 respondents) opted for raising citizens' awareness regarding existing data safety mechanisms. 33.4% (140 respondents) on the other hand seem to believe that increasing data protection standards in public entities would be the most effective. 14.6% of replays (61 respondents) supported the idea of enabling citizens to directly monitor data processing by the government and 14.3% (60 respondents) suggested that increasing computer literacy and access to the internet across the whole country can result into increased trust in e-services among the public. Here 6 respondents used the opportunity for individual input, 3 of them affirmed the equal importance of all listed factors. 2 respondents suggested that e-services cannot succeed unless government is trusted by citizens first. 1 respondent put emphasis on elevating work ethics of public servants with respect to data privacy, so citizens can trust their good intentions (see Appendix 3, Figure 11).

Presented responses to the questionnaire have been gathered amongst citizens of Georgia representing a wide range of age groups. As responses to the final, twelfth question

indicated the age of 29.8% (125 respondents) varied between 18 to 25 years. Second largest group of participants 21.7% (91 respondents) aged between 26 to 35 years. Number of polled citizens with age category from 36 to 45 years amounted to 16.9% (71 respondents). 13.8% (58 respondents) placed themselves in the age category of 46 to 55 years. A number of participants with age between 56 to 65 years totalled to 10.5% (44 respondents) and finally, polled citizens aging 66 years and above amounted to 7.2% (30 participants). (see Appendix 3, Figure 12).

Forthcoming sub-sections of this chapter will focus on conveying analyses of presented questionnaire outcomes and discussing matters related to sample representativeness as well as outcome generalizability.

6.2 Questionnaire outcome analysis

Having established strong interdependency between data protection and e-governance success in preceding chapters, outcomes of the questionnaire are analysed with regard to their potential to facilitate e-service diffusion in Georgian public sector. Interpretations of the findings help to grasp the comprehensive overview of citizen standpoint regarding matters related to their personal data safety.

Cumulative analysis of responses to the first, fourth, seventh and eighth questions provide an overview of factual knowledge citizens seem to have on matters related to their personal information stored within public entities and on monitoring tools at their disposal. While the majority of the respondents have confirmed being familiar with the existence of digital data repositories within the public sector, only a few of them appear to have sufficient information on legal means they can use to oversee the processes and even fewer seem to have practiced those tools in real life. However, the fact that the most popular replies to these questions were ones expressing a desire to learn more about personal information security in public sector indicates growing interest on this matter among the general public.

Latter interpretation also goes in line with interview findings as representative of Data Protection Inspectorate has similarly highlighted a recent increase in citizen inquiries to their institution. Majority of the respondents confirmed being informed about the existence of Personal Data Protection Inspectorate and many of those who learned about the institution for the first time with this survey demonstrated being open to the possibility

to use its services in future which is undisputedly a positive tendency. However, far less number of respondents seem to be aware of what is probably the strongest tool at their disposal for direct monitoring – placing inquiries at public institutions regarding how their personal data is being handled. Such deficiency of citizen awareness about existing monitoring mechanisms can decrease public trust towards government processes and result in low engagement rate for e-services as it was confirmed by studies discussed in earlier chapters of this research [47].

Second, third and fifth questions delved into subjective attitudes of the participants towards publicly-held personal data processing. Interpreting their responses leads to the conclusion that the considerable number of respondents doubt that electronic data processing in Georgian public sector complies with optimal standards and guidelines. While this apprehension seems to limit respondents' acceptance rate towards e-governing initiatives to some extent, it does not appear to affect their overall trust towards government to the point where they would refrain from using e-services altogether.

The dominant pattern of responses for these questions suggests that although governmental entities are believed to provide more effective protection for personal data compared to the private ones, the public sector still fails to measure up to the standards demanded by the general public in this regard. Thus, as it was already stated in earlier chapters, a gap between social and technical standards of data security can lead to major implications for e-governing initiatives if not addressed adequately by the state [46].

Analyses of the responses for sixth and ninth questions give insights to participants' perception of the most urgent issues related to digital data processing in Georgian public sector. Although every problem which was offered in the suggested list of answers accumulated a certain number of supporters, more than third of total participants seem to believe that the lack of technical security mechanisms in data repositories is the biggest threat to publicly-held personal data at the moment. A study from the Netherlands from 2011 which was discussed earlier demonstrated that citizen scepticism towards state capability to provide adequate protection for their personal data makes them reluctant to use e-services [45]. As named study suggested, despite existing general trust towards good intentions of the public entity, when latter fails to offer proper level of data protection from third parties citizens withhold from using electronic channels of communication and give preference to the conventional methods to receive available public services.

Finally, tenth and eleventh questions focused on evaluating the prospect of e-governing initiatives in Georgia. The idea of more technology-heavy public sector appears to cause nonhomogeneous attitudes among survey participants. A noteworthy number of respondents confirmed their support for digital channels of communication offered by the government owing to their efficiency, convenience and user-oriented nature. The remaining segment of participants however, reacted negatively to the possibility of digitalized public services due to transparency and security hazards. Analysing these outcomes with regard to the responses from previous questions once again reaffirms the conclusion that although a considerable number of citizens are willing to adopt e-services, the circle of users is prone to remain limited due to circulating concerns on information security in the society.

To summarise every point presented above and propose an exhaustive answer to the posed RQ3, it must be pointed out that citizen understanding of matters related to personal data protection remains below the desired level and the public still needs to be made aware of existing direct monitoring mechanisms at their possession. However, questionnaire outcomes have confirmed citizens' growing interest in personal data protection which gives hope for future improvements in this regard.

Current lack of information on the one hand and government failure to guarantee a satisfactory level of data security on the other seems to have turned a certain segment of the society reluctant to adopt e-services. Although such negative effects are limited and therefore unlikely to rule out e-service utilization altogether, they have the potential to challenge its widespread application throughout the country and hinder broad diffusion of e-governance in Georgia.

6.3 Questionnaire limitations

Both interviews and questionnaires represent data collecting methods for qualitative case study and therefore, share number of limiting factors for their outcome validity and reliability. To avoid reciting determinants which were already evaluated in 5.3 sub-section of this paper, the current focus will be shifted towards representativeness of samples and generalizability of findings in case of questionnaires as numerous peculiarities of the named method make these two aspects rather intricate and challenging to tackle.

Population (objects of interest) for this study equals to Georgian citizens hence, conducting a census by collecting opinions from every single one of them was neither feasible nor practical within the frames of this research. Therefore, the decision was made to adopt sampling technique which is very often used in social sciences to gather viewpoints from limited subset/sample of the entire population and study their empirical diversities instead, in order to get insights into the opinions of the whole population in question [98].

To achieve the needed level of representativeness and permit generalization of findings sociological theories recommend applying probability sampling techniques for identifying subset to be studied for the research. Probability sampling methods ensure that subgroup of study participants is assembled randomly so that everyone within the population (in our case Georgian citizens) would possess the same non-zero chance of being picked as respondent [99].

Within the frames of this study however, nonprobability methods have been chosen. Convenience sampling which was applied for selecting study participants included collecting data by posting the questionnaire on social media platforms and spreading it via electronic channels of communication. Therefore, responses had been gathered only from those who were conveniently available and willing to participate. Such non-systematic approach to respondent recruiting limits sample representativeness and impedes generalizing outcomes to the entire population however, it can be justified by exploratory nature of this study. V. Sue and L. Ritter claim that using nonprobability samples is appropriate for the purposes of exploratory research since it aims to gather a preliminary overview of the observed phenomenon and while making generalizations might be desirable, it is still a secondary consideration for this type of research [15]. Academic articles recommend several measures to compensate for generalizability limitation of questionnaire which have been applied in this case as well, including:

- Selecting a sample within the limits of 30 to 500, but no more than 10% of the studied population – sample size for this study amounted to 419 respondents which meets the named criteria
- Using multiple sources of data to allow outcome verification – questionnaire outcomes have been validated by the similar pattern of findings from interviews, which represented the second source of data for this research [100].

7 Conclusion and Summary

Looking back at the development history of the right to privacy shows that the emergence of the notion to protect personal space of an individual is strongly linked with technological advancements. As automated tools for personal data processing grow in capacity and intrusiveness, privacy-enhancing legal and technological mechanisms also appear to maintain the equilibrium. This stands true for publicly-held personal data processing and e-governing initiatives as well, since maintaining adequate protection for citizens' data is an indispensable feature of successful e-services.

In response to the first question which was posed within the frames of this research number of available legal and technological tools have been reviewed which are predisposed to assert the proper level of information privacy. GDPR, principles for personal data processing, multiple conventions and cross-country agreements as well as national legislations have been introduced and analysed as legal guarantees for data protection. Furthermore, technological tools which allow practical realization of these legal principles have been evaluated including access control and audit trail logging mechanisms. They were discussed in more detail from the technical angle and further exemplified by describing the case of Estonia, which stands among the most advanced e-states with highly efficient digital governance.

Considering all the above-mentioned in combination with presented restricted access theory of privacy leads to the conclusion that currently available legal and technological mechanisms prove capable of guaranteeing sufficient protection for individuals' personal information within the frame of e-governance, if/when they are implemented properly. As theory suggested, these mechanisms need to be used for establishing protected zones of privacy within state databases to maintain adequate safety level for citizens' personal information (RQ1).

Empirical data gathered from the interviews with state officials allowed a thorough investigation of matters posed in the second question of this research. Georgian public sector has shown significant effort towards getting compliant with internationally accepted data security standards. Several positive reforms have been made in this regard during the current decade, be it adopting the law on personal data safety or implementing technological solutions for establishing secure and interoperable state network.

However, a number of pertinent issues still prevail from legal as well as technological perspective which prevent Georgian public sector from harvesting the benefits of the secure digital environment. Failure of existing law in force to guarantee desired level of safety for personal data, unsatisfactory level of technological security in majority of state entities, absence of proper access control policies and audit trail monitoring mechanisms, disregard of information privacy by public servants together with lack of system accountability component within state databases places data security in Georgian public sector at its preliminary stage of development. As this research has indicated Georgian governmental entities still have not adapted to the number of suggested data protection approaches which continues to hinder country's association with EU standards and its values (RQ2).

Formulating the response to the third question of this research called for gathering first-hand empirical data from citizens by the means of online questionnaires. Interpreting their outcomes has led to the conclusion that knowledge of existing data protection mechanisms and practical monitoring tools is rather limited and fractional for a sizable number of polled citizens. However, both sources of data used for this research have confirmed growing interest of the public in matters related to personal data protection which has the potential to serve as the catalyst for future improvements in this regard.

According to the survey outcomes concerns related to personal information safety in public sector seem to have a certain deterrent effect on respondents' willingness to utilize e-services. While such apprehensions are unlikely to exclude usage of digital services entirely they prove capable of impeding board diffusion of e-governing initiatives among the citizens of Georgia (RQ3).

Main insights gathered within the frames of this research suggest that state entities need to prioritize achieving personal information security for e-services they offer. At the same time, considerable attention must be paid to increasing level of citizens' awareness on monitoring mechanisms at their disposal. Below-presented recommendations were formulated to suggest solutions for current challenges and facilitate accomplishing responsibilities state of Georgia has undertaken by Association Agreement with EU.

- Implementing legislative amendments to include clear-cut obligations for data controllers on matters such as introducing a written policy on information security or enforcing access control mechanisms, in order to harmonize existing law in force with internationally accepted standards and guidelines
- Elaborating centralized governmental strategy for incorporating technological mechanisms such as audit trail logging in electronic databases to accelerate reforms

and guarantee homogeneity of personal data protection across the whole public sector

- Fostering interoperability and creating protected data exchange channels in between governmental institutions to ensure secure circulation of citizens data between state institutions
- Adhering to the concept of 'privacy by default' while building digital infrastructure for e-services and improving work ethics of the public servants with respect to citizens' personal information privacy by the means of thematic training together with continuous monitoring of their activities inside personal information databases
- Providing citizens with tools for direct and real-time monitoring of how their personal data is being handled by various public entities as it was shown on the Example of Estonia to increase the element of system accountability
- Conducting active information campaigns to raise citizens awareness on matters related to personal information processing and monitoring tools at their disposal in order to refute existing misconceptions and invoke public trust towards digital data processing in public sector.

The right to privacy and personal data protection have entered the limelight with recent years' technological advancements. In modern information society these fundamental rights are being interpreted more and more broadly to protect a bigger segment of individuals' lives from unjustified invasion. Such increasing importance of personal data security creates myriad of possibilities for future research on this topic, especially along the lines of newly emerging General Data Protection Directive. Since the presented case was limited to exploring the current state of personal data safety in Georgian public sector, future research should be conducted on the effects of GDPR on non-EU countries as directive comes into full force and sufficient empirical evidence will accumulate for observation and analysis.

Further explanatory research can also be conducted for understanding reasons behind the problems which were exposed by this study. As a logical continuation of presented work, it would provide generalizable explanations for issues such as citizens' distrust and resistance to digital data processing in public sector.

References

[1] United Nations, General Assembly. [2014]. Resolution A/RES/69/166 on the Right to Privacy in the Digital Age.

[2] Association agreement between the European Union and the European Atomic Energy Community and their Member States of the one part and Georgia, on the other part. Opened for signature 27 June 2014, [entered into force 1 July 2016]. OJ L 261/4.

[3] United Nations, Economic and Social Affairs Department. e-Government Survey 2016. Available: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf [Accessed: 21-Apr-2018].

[4] Kvizhinadze, A. (2014) "სეკულარიზმის კრიზისი საქართველოში "[The crisis of secularism in Georgia] Available: https://www.radiotavisupleba.ge/a/25286765.html [Accessed: 21-Apr-2018].

[5] Chelidze, K. (2011). "ID ბარათი: ნეგატიური დამოკიდებულება უსაფუძვლო არაა"[ID card: Negative attitude is not unfounded]. Available: http://www.ambioni.ge/id-barati-negatiuri-damokidebuleba-usafuzvlo-araa [Accessed: 21-Apr-2018].

[6] Chankotadze, A. (2013) "ID ბარათები: საფრთხე პირადი თავისუფლებისთვის" [ID cards: threat for personal freedom] Available: http://liberali.ge/articles/view/3150/ID-baratebi--safrtkhe-piradi-tavisuflebistvis [Accessed: 21-Apr-2018].

[7] Given, L. M. (Ed.). (2008). *The Sage encyclopedia of qualitative research methods.* Sage Publications.

[8] Creswell, J. W., & Creswell, J. D. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

[9] Recker, J. (2012). *Scientific research in information systems: a beginner's guide.* Springer Science & Business Media.

[10] Tracy, S. J. (2012). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact.* John Wiley & Sons.

[11] Grunig, J. E. (2002). Qualitative methods for assessing relationships: Between organizations and publics.

[12] Yin, R. K. (2013). *Case study Research: Design and Methods*. Sage publications.

[13] Hox, J. J., & Boeije, H. R. (2005). Data collection, primary versus secondary. *Encyclopedia of Social Measurement*, 1, 593-599.

[14] Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering*, 14(2), 131.

[15] Sue, V. M., & Ritter, L. A. (2012). *Conducting online surveys*. Sage publications.

[16] Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. *Qualitative Social Research*, 11(2).

[17] Evans, J. R., and Mathur, A. (2005). The value of online surveys. *Internet research*, 15(2), 195-219.

[18] Regulation (EU) 2016/679 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 and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[19] Directive 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L119/89.

[20] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[21] Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Review*, 24(6), 508-520.

[22] Charlesworth, A. (2017) Watching the Watchers: CCTV, the GDPR and the third wave of Data Privacy Regulation. White Paper, Cloudview (UK) Limited.

[23] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705.

[24] Koščík, M. (2017). The Impact of General Data Protection Regulation on the grey literature. Paper presented at 9th conference on grey literature and repositories. (p. 64).

[25] Hornung, G. (2012). A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft of 25 January 2012. *SCRIPTed*, 9(1), 64.

[26] O'Brien, R. (2016). Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business Information Review*, 33(2), 81-84.

[27] Google Spain SL v. Agencia Espan˜ ola de Proteccio´n de Datos (AEPD) [2014] Case C-131/12, EU Court of Justice.

[28] Svantesson, D. J. B. (2015). The (uncertain) future of online data privacy. *Masaryk UJL & Tech.*, 9, 129.

[29] Vasiliu, I (2017). Work in the transition period for a successful implementation of the data protection package. Presented at the E-volution of Data Protection conference, plenary session II, Tartu, Estonia. Materials available: https://www.just.ee/en/e-volution-data-protection-conference [Accessed: 21-Apr-18]

[30] Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, 26(3), 213-228.

[31] Greenleaf, G. (2015). Global data privacy laws 2015: 109 countries, with European laws now a minority. *Privacy laws & Business International report*, 133, 14-17.

[32] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 6(2), 77-78.

[33] Emerson, T. I. (1979). The right of privacy and freedom of the press. *Harvard Civil Rights-Civil Liberties Law Review*, 14, 329.

[34] Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. University of North Carolina Press.

[35] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

[36] Glancy, D. J. (1979). Invention of the Right to Privacy, *The. Ariz. L. Rev.*, 21(1).

[37] Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1-22.

[38] Baghai, K. (2012). Privacy as a human right: a sociological theory. *Sociology*, 46(5), 951-965.

[39] Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield.

[40] Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471.

[41] Moor, J. H. (1991). The ethics of privacy protection. *Library Trends*, 39, 69-82.

[42] Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, 27(3), 27-32.

[43] Reidenberg, J. (1997). The use of technology to assure internet privacy: Adapting labels and filters for data protection. *Texas Law Review*, 553.

[44] Wu, Y. (2014). Protecting personal data in e-government: A cross-country study. *Government Information Quarterly*, 31(1), 150-159.

[45] Beldad, A., van der Geest, T., de Jong, M., & Steehouder, M. (2012). A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government information quarterly*, 29(1), 41-49.

[46] Jho, W. (2005). Challenges for e-governance: protests from civil society on the protection of privacy in e-government in Korea. *International Review of Administrative Sciences*, 71(1), 151-166.

[47] Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, 27(6), 2233-2242.

[48] Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), 165-176.

[49] Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. *Business process management journal*, 11(5), 589-611.

[50] Kunis, R., Rünger, G., & Schwind, M. (2007). A new model for document management in e-Government systems based on hierarchical process folders. Paper presented at the 7th European Conference on E-Government, Academic Conferences Limited, (p. 229).

[51] Council of Europe. [1981]. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series 108.

[52] Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. 01248/07/EN, WP 136.

[53] Olteanu, M., & Homeghiu, F. M. (2012). Protection of Personal Data–actual and proposed issues. *EIRP Proceedings*, 7.

[54] Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16). Springer Science & Business.

[55] Jaffer, J. (2010). The mosaic theory. Social Research: *An International Quarterly*, 77(3), 873-882.

[56] European Union, Charter of Fundamental Rights of the European Union. [2000]. OJ C 364/1.

[57] Council of Europe., & Council of Europe. [1952]. The European convention on human rights. Strasbourg: Directorate of Information

[58] The United Nations, General Assembly. [1948]. Universal Declaration of Human Rights. Paris.

[59] McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1), Available: https://doi.org/10.1177/2053951716686994 [Accessed: 21-Apr-18]

[60] Nyman-Metcalf, K. (2014). *The future of universality of rights. In Protecting human rights in the EU* (pp. 21-35). Springer, Berlin, Heidelberg.

[61] Greenleaf, G. (2017). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. *Privacy Laws & Business International Report*, 145, 10-13.

[62] Kiškis, M., & Petrauskas, R. (2003). E-Governance: two views on legal environment. Paper presented in International Conference on Electronic Government (pp. 407-412). Springer, Berlin, Heidelberg.

[63] Nyman-Metcalf, K. (2014). *e-Governance in Law and by Law. In Regulating eTechnologies in the European Union* (pp. 33-51). Springer, Cham.

[64] Fisher, E., Pascual, P., & Wagner, W. (2010). Understanding environmental models in their legal and regulatory context. *Journal of Environmental Law*, 22(2), 251-283.

[65] Kennedy, R. (2015). E-Regulation and the Rule of Law: Smart Government, Institutional Information Infrastructures, and Fundamental Values, *Information Polity*, 21, 77-98.

[66] ECtHR, Taylor-Sabori v.the United Kingdom, [2002] No. 47114/99.

[67] ECtHR, Khelili v. Switzerland, [2011] No. 16188/07.

[68] Wuermeling, U. U. (1995). Harmonization of European Union privacy law. *J. Marshall J. Computer & Info. L.*, 14, 435.

[69] Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. 00569/13/EN, WP 203.

[70] Forgó, N., Hänold, S., & Schütze, B. (2017). *The Principle of Purpose Limitation and Big Data. In New Technology, Big Data and the Law* (pp. 17-42). Springer, Singapore.

[71] Article 29 Data Protection Working Party. Opinion 05/2014 on anonymisation techniques. 0829/14/EN, WP 216.

[72] Article 29 Data Protection Working Party. Opinion 3/2010 on the principle of accountability. 00062/10/EN, WP 173.

[73] პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიში (2018) [Annual Report of Personal Data Protection Inspector] Available: https://personaldata.ge/manage/res/images/2018/angarishi/angarishi_2017.pdf [Accessed: 21-Apr-18]

[74] Chuanfan, L. (2010). Research on role-based access control policy of e-government. Paper Presented at E-Business and E-Government 2010 International Conference. (pp. 714-716). IEEE.

[75] Kalam, A. A. E., Baida, R. E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., ... & Trouessin, G. (2003). Organization based access control. In Policies for Distributed Systems and Networks. (pp. 120-131). IEEE.

[76] Niu, Z., Zhou, K., Feng, D., & Yang, T. (2010). Access Control Lists for Object-Based Storage Systems. *Chinese Journal of Electronics*, 19(3).

[77] Salunke, D., Upadhyay, A., Sarwade, A., Marde, V., & Kandekar, S. (2013). A survey paper on Role Based Access Control. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(3), 1340-1342.

[78] Peng, Y., Song, Y., Ju, H., & Wang, Y. (2014). OB4LAC: an organization-based access control model for e-government system. *Applied Mathematics & Information Sciences*, 8(3), 1467.

[79] Haguouche, S., & Jarir, Z. (2014). Managing Heterogeneous Access Control Models Cross-Organization. Paper presented at International Conference on Risks and Security of Internet and Systems. (pp. 222-229). Springer, Cham.

[80] Jiang, K., & Cao, X. (2011). Design and implementation of an audit trail in compliance with US regulations. *Clinical Trials*, 8(5), 624-633.

[81] Söderström, O., & Moradian, E. (2013). Secure audit log management. *Procedia Computer Science*, 22, 1249-1258. Available: https://doi.org/10.1016/j.procs.2013.09.212 [Accessed: 21-Apr-18]

[82] Yavuz, A. A., & Ning, P. (2009). Baf: An efficient publicly verifiable secure audit logging scheme for distributed systems. Paper presented at the Computer Security Applications Conference. (pp. 219-228). IEEE.

[83] Kuna, H. D., García-Martinez, R., & Villatoro, F. R. (2014). Outlier detection in audit logs for application systems. *Information Systems*, 44, 22-33.

[84] King, J., & Williams, L. (2012). Secure Logging and Auditing in Electronic Health Records Systems: What Can We Learn from the Payment Card Industry. Paper presented at 3rd USENIX conference on Health Security and Privacy (pp. 13-13). USENIX Association.

[85] Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). *Towards a novel privacy-preserving access control model based on blockchain technology in IoT. Europe and MENA Cooperation Advances in Information and Communication Technologies* (pp. 523-533). Springer, Cham.

[86] Kalvet, T. (2012) Innovation: a factor explaining e-government success in Estonia, Electronic Government, *An International Journal*, 9(2), 142–157.

[87] Anthes, G. (2015). Estonia: a model for e-government. *Communications of the ACM*, 58(6), 18-20.

[88] Murumaa-Mengel, M., Laas-Mikko, K., & Pruulmann-Vengerfeldt, P. (2015). I have nothing to hide": A coping strategy in a risk society. *Journalism, representation and the public sphere*, 194-207.

[89] Martinovic, I., Kello, L., & Sluganovic, I. (2017). Blockchains for Governmental Services: Design Principles, Applications, and Case Studies. Working Paper Series No.7. Centre for Technology and Global Affairs. Available: https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf [Accessed: 21-Apr-18]

[90] Sihvart, M. (2017) Blockchain – security control for government registers. E-estonia. Available: https://e-estonia.com/blockchain-security-control-for-government-registers/ [Accessed: 21-Apr-18]

[91] Margetts, H., & Naumann, A. (2017). Government as a platform: What can Estonia show the world. Research Report. Available:

https://www.politics.ox.ac.uk/materials/publications/16061/government-as-a-platform.pdf [Accessed: 21-Apr-18]

[92] Kütt, A., & Priisalu, J. (2014). Framework of e-government technical infrastructure. Case of Estonia. Paper presented at the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[93] საქართველოს კონსტიტუცია [1995]. [Constitution of Georgia] Parliament of Georgia. Tbilisi.

[94] საქართველოს ზოგადი ადმინისტრაციული კოდექსი [1999] [General Administrative Code of Georgia] Parliament of Georgia. Tbilisi.

[95] საქართველოს კანონი პერსონალური მონაცემების დაცვის თაობაზე [2011] [Law of Georgia on Personal Data Protection] Parliament of Georgia. Tbilisi.

[96] საქართველოს მთავრობის დადგენილება №64 [2012] სახაზინო (საბიუჯეტო) დაწესებულებებში საქმისწარმოების ავტომატიზებული სისტემის მინიმალური სტანდარტის დამტკიცების შესახებ [№64 Decree of the Government of Georgia on Approving Minimum Standard for Automated Document Management Systems in State Budget Institutions]. Government of Georgia. Tbilisi

[97] Brink, H. I. L. (1993). Validity and reliability in qualitative research. *Curationis,* 16(2), 35-38.

[98] Gobo, G. (2004). Sampling, representativeness. *Qualitative research practice*, 435.

[99] Best, S. J., Krueger, B., Hubbard, C., & Smith, A. (2001). An assessment of the generalizability of Internet surveys. *Social Science Computer Review*, 19(2), 131-145.

[100] Alreck, P. L., & Settle, R. B. (1995). *The Survey Research Handbook: Guidelines and Strategies for Conducting a Survey*, 2E. Edition, Chicago.

Appendix 1 – Interview at the Office of Personal Data Protection Inspector

For the purposes of this research first interview was conducted with the representative of Personal Data Protection Inspector's office in Georgia. The precise list of matters covered during the interview is displayed below. An exhaustive overview of the gathered data has been presented in Chapter 5 of this study. The detailed transcript of the conversation is stored with the author of this thesis and can be presented upon request.

- Filing system and filing systems catalogues registers. Which public institutions are obliged to maintain them, established standard and procedure for their maintenance. The frequency of filling out these catalogues for public institutions
- The main channel for data exchange in between various public institutions. Role of internal document flow systems, conventional methods or other forms of electronic communications for personal data exchange within the public sector. A common set of rules applicable to exchanging sensitive personal data in between institutions
- Criteria for assessing data safety level by Personal Data Protection Inspector for both paper-based and digital data repositories. The commonly accepted standard of safety
- Electronic databases and their technical capability to register public servants' access to the citizens' personal files. Access trail logging, so-called electronic footprint mechanism. Approach taken by Georgian legislation regarding mandatory nature of implementing automated logging mechanism. Its practical implementation and the overall situation in Georgian public sector in this regard
- Legal perspective of access control mechanisms and their implementation in state organizations. If state organizations operate by creating a list of employees with clearance to access citizen's personal data or such information is usually accessible by every employee. Mechanisms state organizations implement to

avoid unlawful access to the personal data by third persons during electronic processing of the data

- Usage of electronic document flow systems in public institutions, what is current situation, amount of institutions which prefer traditional forms of personal data processing (only on paper) if any and established standard at Inspectors' office for monitoring institutions where personal data is processed on paper. Applied means to control/restrict using and viewing personal data content by unlawful persons for such cases
- The most problematic issues when it comes to electronic processing of personal data in Georgian public sector from the experience of Data Protection Inspectorate. Types of law infringements encountered most frequently in practice
- Citizen cooperation with the Personal Data Protection Inspector's Office. The frequency of citizen inquiries to public institutions regarding a type of data stored there about them and institutions/public servants that have access to it. Responses to such inquiries from state officials, the technical capability of public institutions (their electronic systems) to provide an automated answer to such requests
- Matter of implementing a higher standard of personal data protection by state institutions and its potential to increase citizens' trust towards e-governance and government in general
- Most effective methods for increasing citizens' awareness on the importance of personal data protection. The overall standard of personal data protection currently in public sector. Possible tendencies for its increase and factors which have contributed to such tendency
- Influence GDPR has on Georgian legislation and practice for the time being - if any at all

Appendix 2 – Interviews with data controllers from public sector

With the intention to collect primary data from data controllers in Georgian public sector, six additional interviews had been conducted with the representatives of four different organizations for this research.

1. Interview – Representative of Educational Resource Centre – Audio recording 05.01.2018
2. Interview – Representative of Public School – Audio recording 05.01.2018
3. Interview – Representative of Public School – Audio recording 05.01.2018
4. Interview – Representative of Social Service Agency – Audio recording 16.01.2018
5. Interview – Representative of Public Service Development Agency – Audio recording 19.01.2018
6. Interview – Representative of Public Service Hall – Audio recording 20.01.2018

List of discussed topics was the same for all these interviews and is now presented below. Detailed written transcripts have been made depicting all the conversations and can be presented upon request.

- Types of personal data processed by the organization and the course of its collection. Employed means for storing citizens' personal information and the environment in which processing takes place, digital or paper based
- Data access policy among employees and its technological realization. List of employees with clearance to access citizens' personal data files (if any) and its implementation in practical administrative maintenance on a day to day bases
- The current state of electronic databases used within the organization, their technical capability to register public servants' access to the citizens' personal files (create automated logs). Any other employed means for depicting which

employee has accessed specific profile of data subject, when, for how long and for what purpose

- Established protocol for exchanging personal information with other public institutions, most frequently employed means of communication to fulfil data requests
- How well-aware citizens are of the form in which their data is kept within the named institution. Citizen requests regarding the list of information public entity in question owns about them or regarding the list of public servants which have accessed his/her personal file. Technological capability of the institution to give out such information if/when requested. Established protocol for answering such inquiries
- Protecting mechanisms of employed software within the organization. Applied means to prevent unauthorized persons from accessing internal databases. Adhered standards for guaranteeing an adequate level of personal data protection

Appendix 3 – Results of the questionnaire

The questionnaire was created with the purpose to assess citizens' point of view and awareness level regarding employed security mechanisms for protecting their personal information by the state. Participants were recruited by posting the survey on social media platforms and sending it to the direct contacts and contacts of acquaintances, as well as spreading it via email lists and other means of peer to peer digital networking. Data collection took place from February 9 until March 25, 2018. Comprehensive analysis of the questionnaire outcomes has been presented in Chapter 6 of this research. Results are displayed below in the form of descriptive statistics.

Do you know how is your personal data stored in state institutions? On paper or electronically?

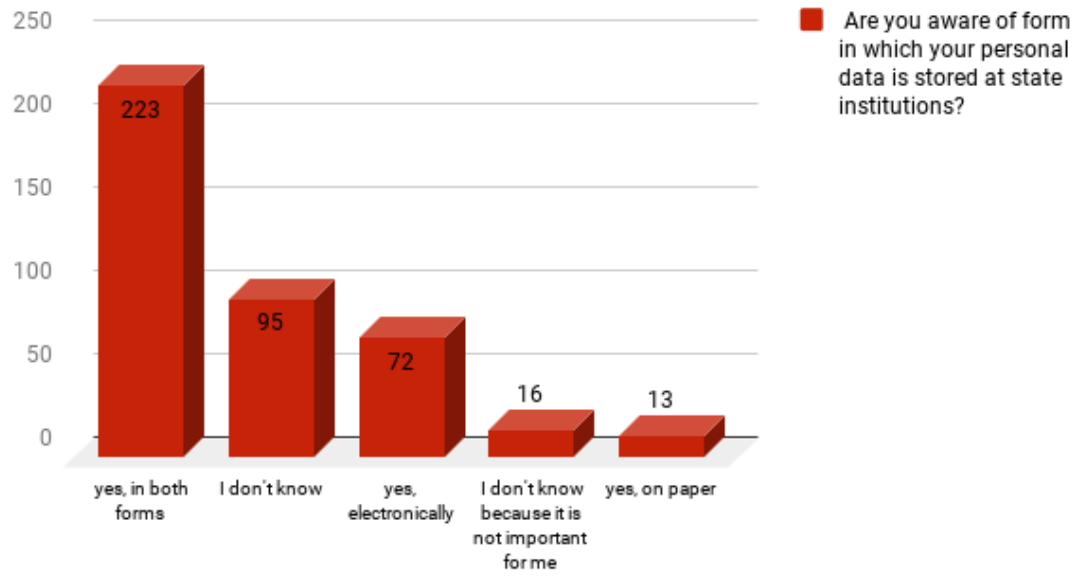

Figure 1. Answers to Question 1.

Which form would you prefer for your personal data to be stored in state institutions from the security perspective?

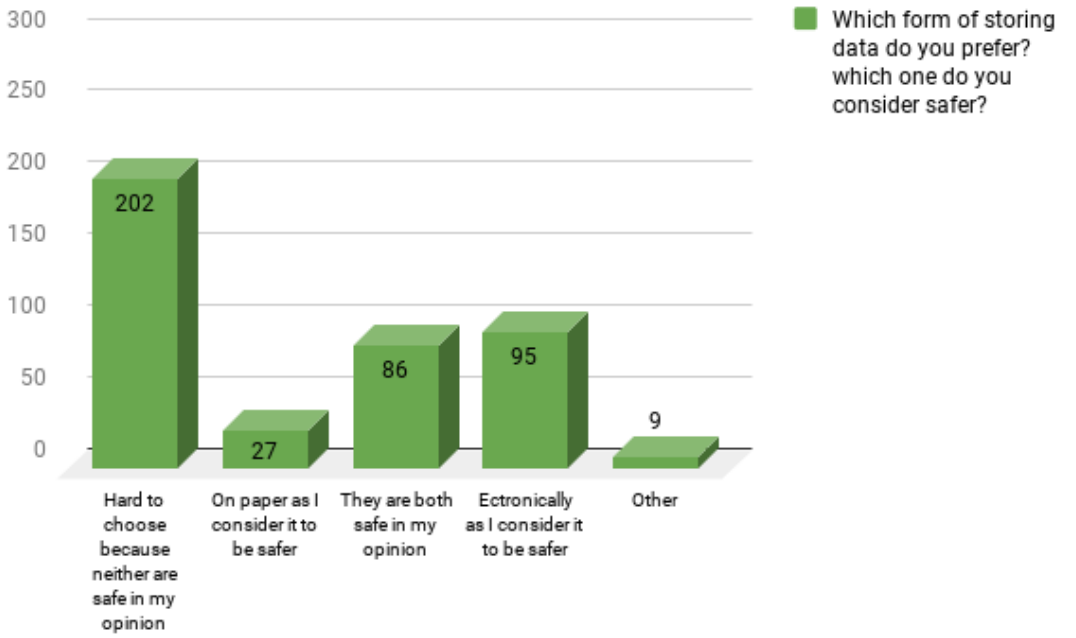

Figure 2. Answers to Question 2.

Which sector to you trust more to process your personal data lawfully, public or private?

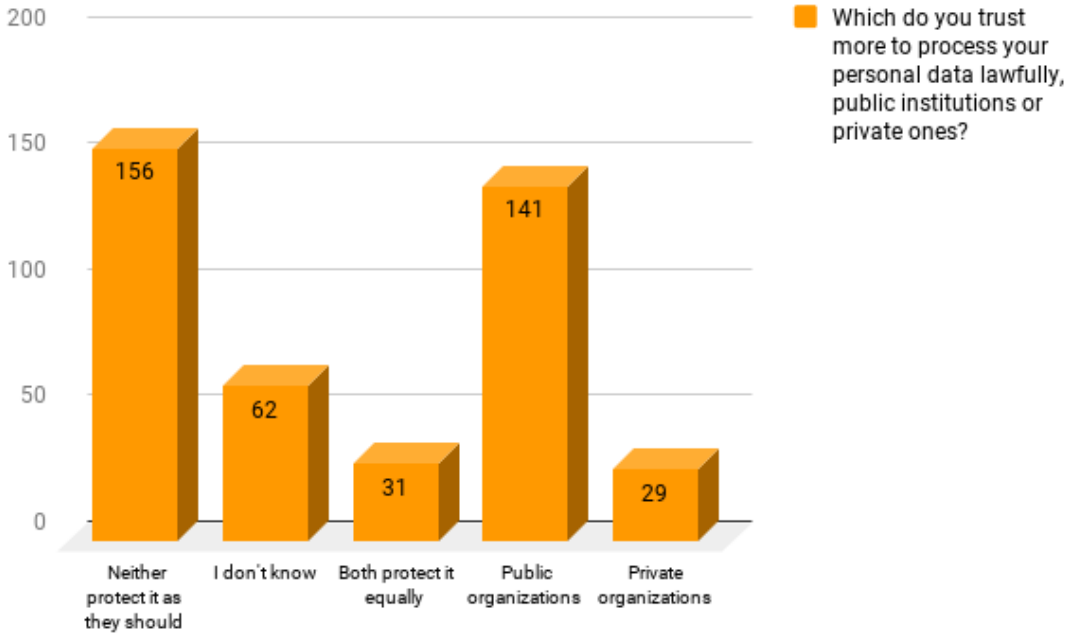

Figure 3. Answers to Question 3.

How well-aware are you of the mechanisms used for keeping your data safe at public organisations?

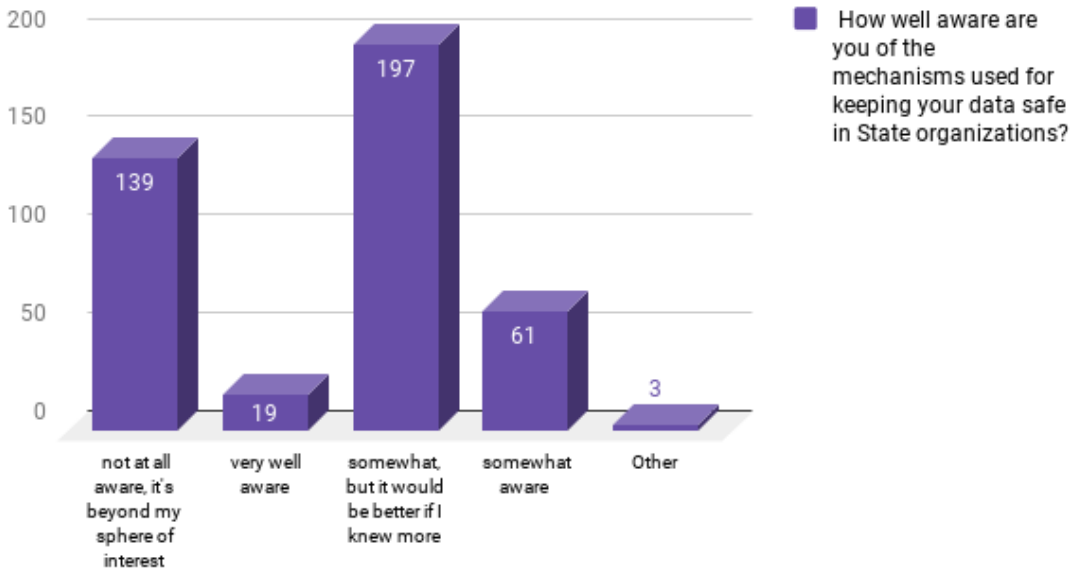

Figure 4. Answers to Question 4.

Do you trust state institutions that they are processing your data in a good faith?

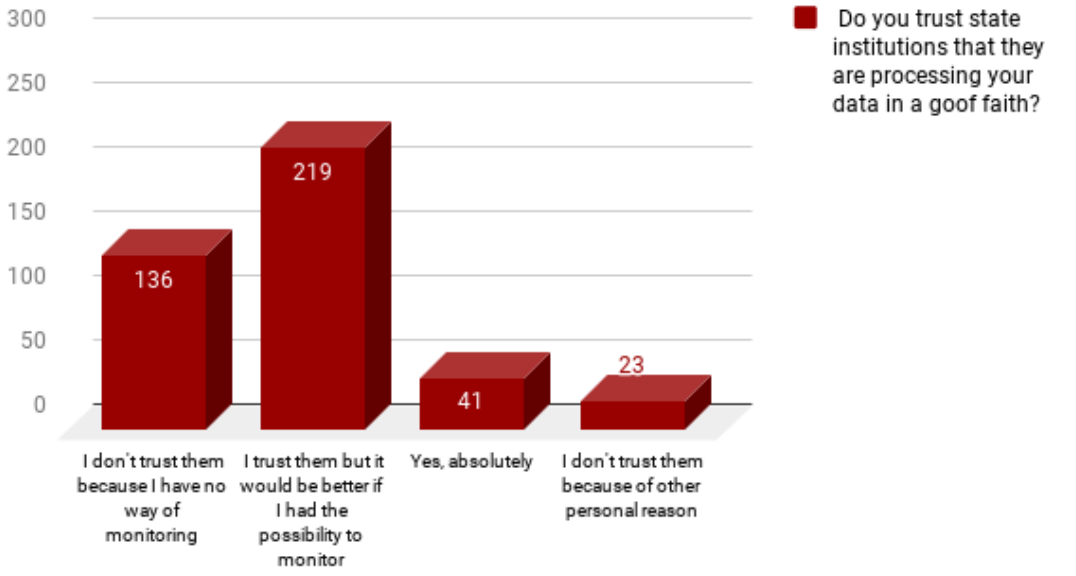

Figure 5. Answers to Question 5.

What do you consider to be the biggest issue when it comes to processing your data electronically by the state?

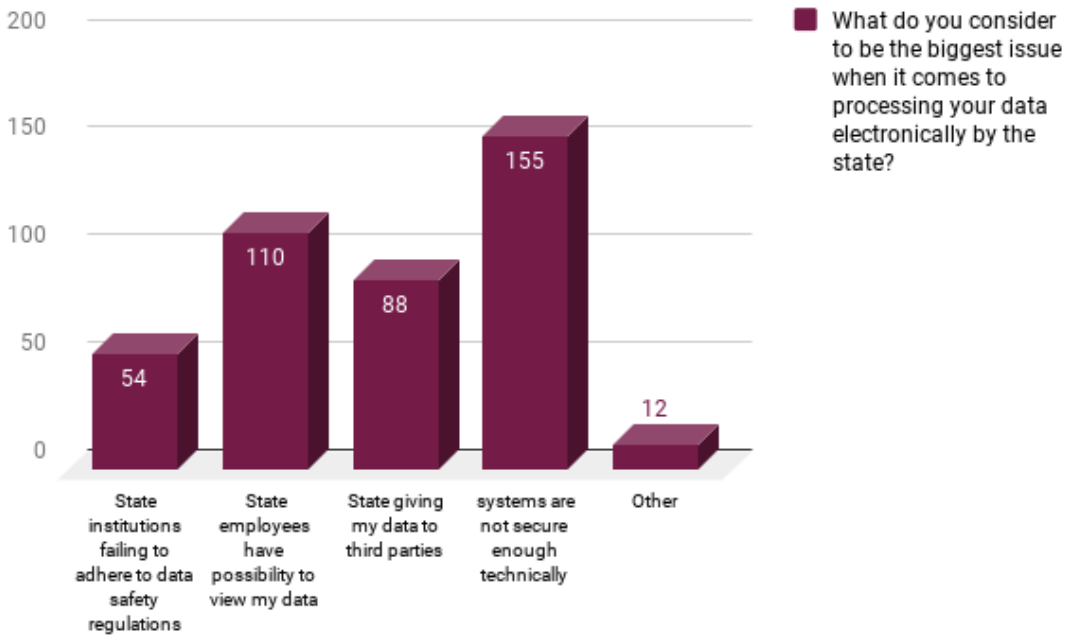

Figure 6. Answers to Question 6.

Do you know that from any state organization you can inquire to whom your data has been disclosed? Have you ever submitted such request?

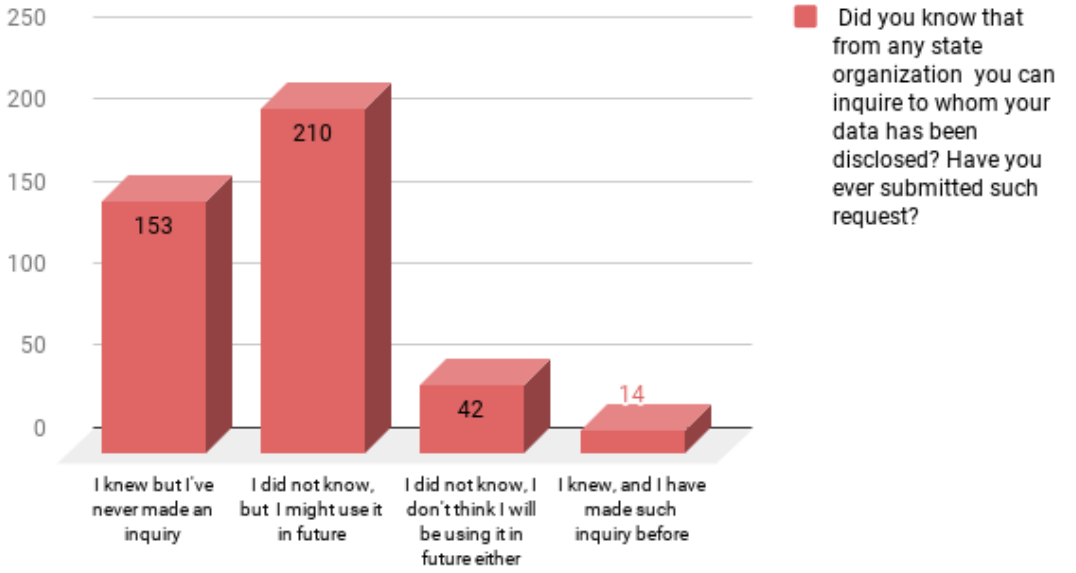

Figure 7. Answers to Question 7.

Have you heard of the Office of Personal Data Protection Inspector and its functions? Have you ever used its services?

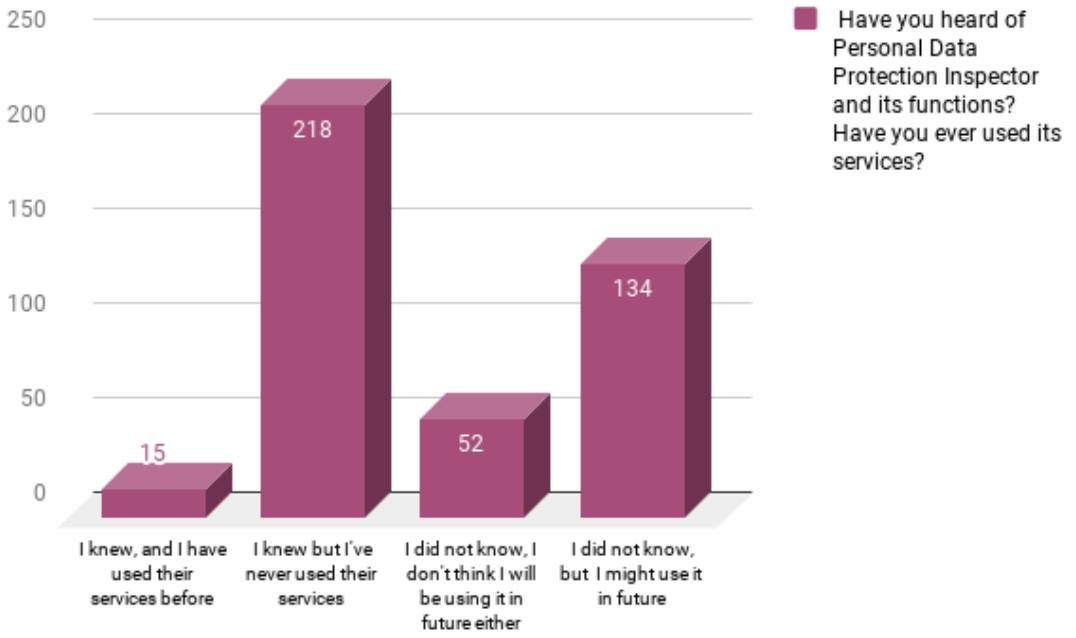

Figure 8. Answers to Question 8.

Have you had an experience of public institution violating data protection standards? (disclosed your data, refused to correct inaccurate recordings etc.)

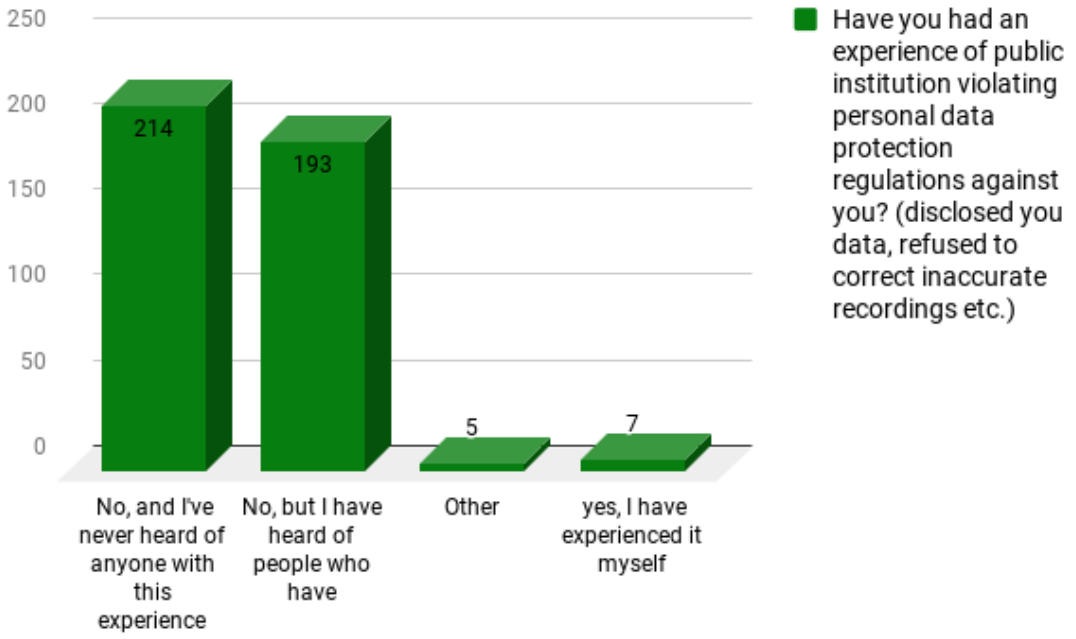

Figure 9. Answers to Question 9.

Do you support implementing new e-solutions in Georgia such as e-voting of e-prescriptions for instance?

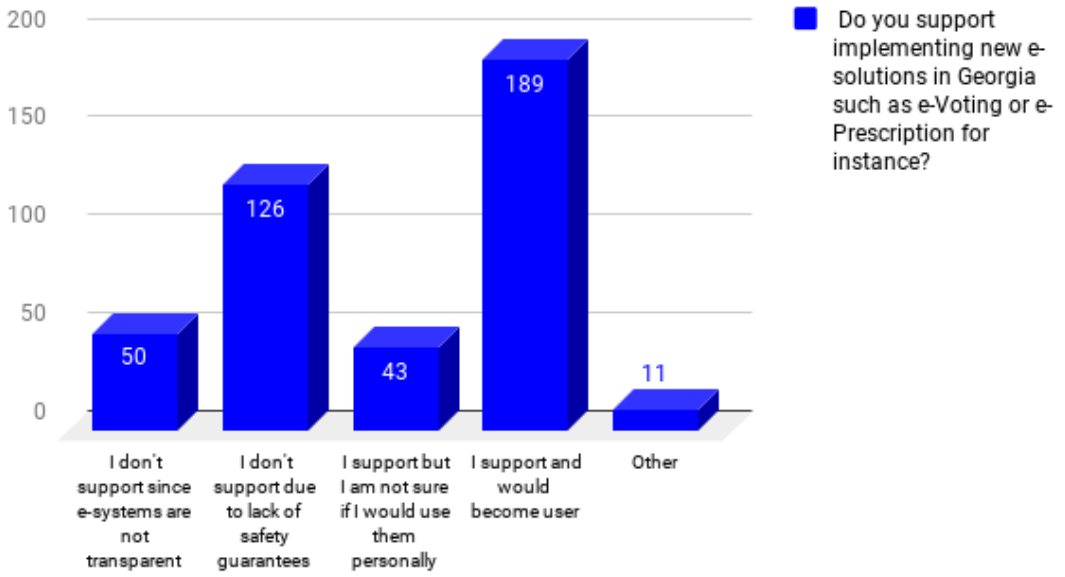

Figure 10. Answers to Question 10.

Which factor would you say has the biggest potential to increase citizens' trust towards electronic services in Georgia?

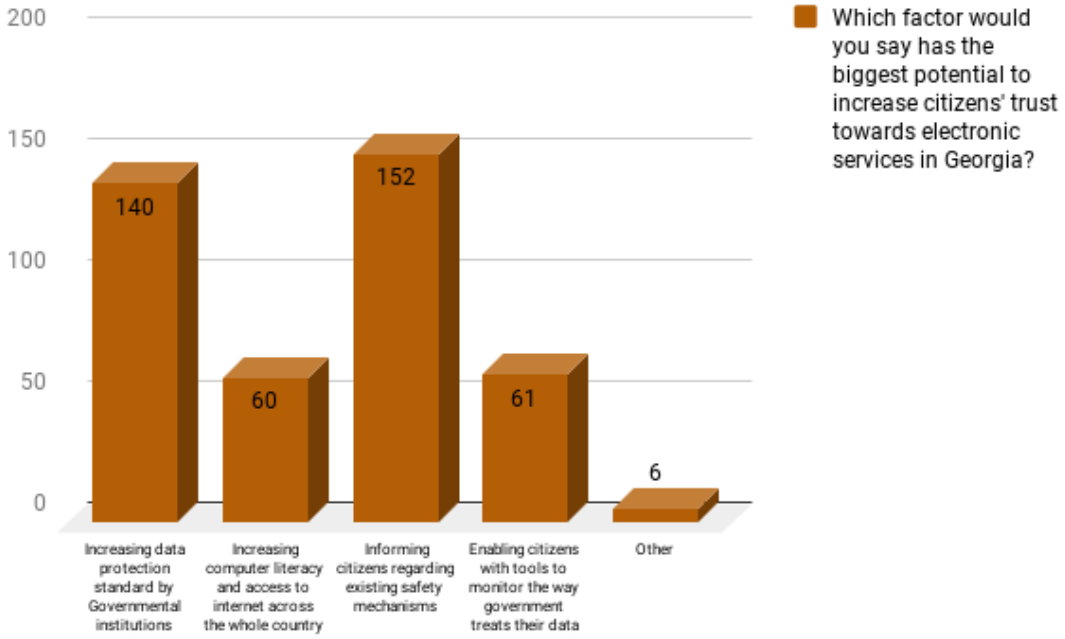

Figure 11. Answers to Question 11.

Please specify your age

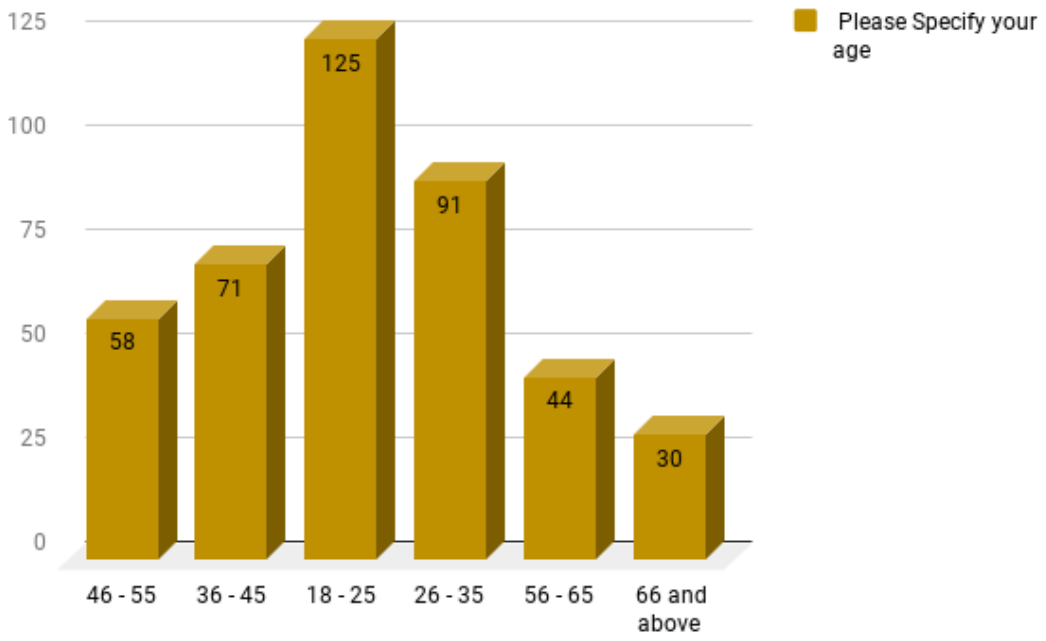

Figure 12. Answers to Question 12.