Aspects of Personal Data Protection from State and Citizen Perspectives – Case of Georgia

Mariam Tsulukidze, Kartin Nyman-Metcalf, Valentyna Tsap, Ingrid Pappel, Dirk Draheim

Aspects of Personal Data Protection from State and Citizen Perspectives – Case of Georgia

Mariam Tsulukidze[1], Kartin Nyman-Metcalf[2], Valentyna Tsap[2(✉)], Ingrid Pappel[2] and Dirk Draheim[2]

[1] Information Systems Group
Tallinn University of Technology, Tallinn, Estonia
Akadeemia tee 15a, 12618 Tallinn, Estonia
{mariam.tsulukidze@taltech.ee,valentyna.tsap,ingrid.pappel,dirk.draheim}@taltech.ee
[2]e-Governance Academy
Rotermanni 8, 10111 Tallinn, Estonia
katrin.nyman-metcalf@ega.ee

Abstract. This paper aims to investigate the process of personal data protection in Georgia within the frame of e-governance, 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. The potential of proper data protection to act as the enabler of e-governance services success is also evaluated. We explore the defense mechanisms of Georgian governmental entities by conducting interviews with seven experts from the Personal Data Protection Inspectorate and other public entities handling citizens' data. We study citizens' perception of data safety and the citizens' knowledge of existing monitoring mechanisms through analysis of over 400 responses that we have received to our survey. We also analyze and assess the influence of these factors on the success of e-governance and its broad diffusion. Finally, guidelines and recommendations are formulated for raising citizens' awareness on the data protection mechanisms to be used in future theoretical and practical considerations.

Keywords: e-government, personal data protection, citizens' awareness, Georgia.

1 Introduction

A recent resolution by United Nations titled "The right to privacy in the digital age" [14] has 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. Resolution stressed the importance of government commitment to guarantee citizen data privacy. It encouraged member

states to take active measures for establishing digital environment which will be reflecting internationally recognized fundamental rights and freedoms of individuals.

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 European Union.

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 data privacy requirements. 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 between governments, businesses, and citizens. 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, we are aiming to investigate how Georgian government entities are adapting to the new data protection approaches in practice on the premise that achieving high security standard is vital to successful implementation of e-governance. We will examine the current state of electronic databases in Georgian public institution to find out whether they comply with internationally accepted standards and guidelines. Furthermore, we will look into citizens' level of awareness about data protection mechanisms and, additionally, try to better 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.

To address named matters and specify the scope of this paper, below-presented questions have been formulated:

RQ1: How are Georgian government entities adopting to current data protection approaches in practice?

RQ2: 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?

We proceed as follows. In Sect. 2 we explain the methods we have used within this research. Sect. 3 elaborates on the theoretical concepts that support personal data protection. In Sect. 4, we discuss the importance of interconnections between Data Protection and e-Governance. Sect. 5 reports on our findings and is divided into two subsections that reflect state and citizen perspective. Sect. 6 serves as a field for discussion and analyses the outcomes. The paper is summarized with a conclusion in Sect. 7.

2 Methodology

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. We have used expert interviews conducted with state officials to investigate practical adaptation of data protection

mechanisms by Georgian governmental entities. Online surveys have been distributed for understanding citizens' perception of personal data safety and their awareness of existing monitoring mechanisms.

Seven expert 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.

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.

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.

3 Theoretical Background

This section portrays an overview of restricted access theory of privacy which is considered suitable 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.

The origins of restricted access theory can be traced back to 1980s' in the hypotheses of authors such as A. Allen [1] and R. Gavison [6] however, it was only in later works of J. Moor [9], [10] 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" [10] 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 [9].

Restricted access approach suggests creating different zones of protection for each private situation to ensure that personal information is only accessed by authorized 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 [11]. 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.

The given 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 [9], [10].

4 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 [7]. Third aspect and perhaps the most crucial one comes with the fact that anonymizing or pseudonymizing 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 [15].

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. Skeptical 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 [5], [8], [12].

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 [4]. 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 [3].

5 Data Protection in Georgia – Results

This section presents our finding with regards to the research goals we have set within this study. The Subsect. 5.1 elaborates on the details of interviews we have conducted with experts to reveal how Georgia is adapting to the new data protection standards while Subsect. 5.2 gives a comprehensive analysis of citizens' surveys responses that reflect level of their awareness on data protection mechanisms.

5.1 State Perspective

This subsection 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 experts. In order to evaluate to what extent Georgian governmental entities have managed to implement 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. 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).

Personal Data Protection Inspectorate 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. The conducted interviews covered all these activities and the outcomes were coded into six categories each of which is elaborated below.

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.

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, [16] 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.

Data Exchange. 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.

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".*

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 the 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."

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.

Filling Systems Catalogues. Filing systems catalogues are electronic documents published on the web-page of Personal Data Protection Inspector's Office 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 mistakes, organizations are instructed to correct erroneous entries before they are made available to the broader public.

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. For instance, 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.

5.2 Citizen Perspective

After having scrutinized security features of governmental databases in preceding subsection, users' perception of data safety in Georgian public sector will be evaluated below.

Overall 419 responses were received which serve to bring light to citizens' awareness level about data protection mechanisms employed in public sector (See Table 1).

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. Below the interview questions are presented:

Cumulative analysis of responses to the first, fourth, seventh and eighth questions suggest that while the majority of the respondents are 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, dominant replies to these questions have indicated 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 lesser 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 [4].

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.

Table 1. Survey results.

Please specify your age					
18-25	26-35	36-45	46-55	56-65	66 <
125	91	71	58	44	30
Do you know how is your personal data stored in state institutions? On paper or electronically?					
Yes, in both forms	Yes, electronically	Yes, on paper	I don't know because it is not important for me	I don't know	
223	72	13	16	95	
Which form would you prefer for your personal data to be stored in state institutions from the security perspective?					
Hard to choose because neither are safe in my opinion	On paper as I consider it to be safer	They are both safe in my opinion	Electronically as I consider it to be safer	Other	
202	27	86	95	9	
Which sector to you trust more to process your personal data lawfully, public or private?					
Public organizations	Private organizations	Neither protect as they should	I don't know	protect	
141	29	156	62	31	
How well-aware are you of the mechanisms used for keeping your data safe at public organisations?					
Very well aware	Somewhat aware	Somewhat aware but it would like to know more	Not at all aware, it's beyond my sphere of interest	Other	
19	61	197	139	3	
Do you trust state institutions that they are processing your data in a good faith?					
Yes, absolutely	I trust them but it would be better to also monitor it	I don't trust them because I have no way of monitoring	I don't trust them because of other reason		
41	219	136	23		
What do you consider to be the biggest issue when it comes to processing your data electronically by the state?					
State entities failing to adhere to data safety regulations	Officials have possibility to view my data	State giving my data to third parties	Systems are not secure enough technially	Other	
54	110	88	155	12	
Do you know that from any state organization you can inquire to whom your data has been disclosed? Have you ever submitted such request?					
I knew by I've never made an inquiry	I didn't know but I might use it further	I didn't know, unlikely with use it further	I knew and inquired before		
153	210	42	14		
Have you heard of the Office of Personal Data Protection Inspector and its functions? Have you ever used its services?					
I knew and used them before	I knew but never used them	I didn't know, unlikely with use them further	I didn't know but I might use them further		
15	218	52	134		
Have you had an experience of public institution violating data protection standards? (disclosed your data, refused to correct inaccurate recordings etc.)					
Yes, I have experienced it myself	No, an I've never heard of anyone with this experience	No, but I heard of people who have	Other		
7	214	193	5		
Do you support implementing new e-solutions in Georgia such as e-voting of e-prescriptions for instance?					
I support and would become a user	I support but I'm not sure if would use them myself	I don't support since e-systems are not transparent	I don't support due to lack of safety guarantees	Other	
189	43	50	126	11	
Which factor would you say has the biggest potential to increase citizens' trust towards electronic services in Georgia?					
Increasing data protection standard by Government institution	Increasing computer literacy and access to internet across the whole country	Informing citizens regarding existing safety mechanisms	Enabling citizens to monitor the way government treats their data	Other	
140	60	152	61	6	

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 [8].

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. 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 skepticism towards state capability to provide adequate protection for their personal data makes them reluctant to use e-services [5]. 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. Analyzing 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.

6 Outcomes and Discussion

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 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.

7 Conclusion

Empirical data gathered from the interviews with state officials allowed a thorough investigation of matters posed in the first 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, 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. List of these issues include: absence of necessary legal requirements to guarantee 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 and lack of system accountability component within state databases. All these factors place 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 (RQ1).

Formulating the response to the second 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 (RQ2).

Limitations of the presented study concern nonprobability sampling methods which were chosen for identifying studied subset of Georgian citizens. 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. Since it aims to gather a preliminary overview of the observed phenomenon, while making generalizations might be desirable, it is still a secondary consideration for this type of research [13].

Increasing importance of personal data security creates myriad of possibilities for future research on this topic, especially along the lines of newly emerged 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 sufficient empirical evidence accumulates 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. Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield, 1-25.
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. Available: https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22014A0830(02) [Accessed: 11-Jun-2019].
3. Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), 165-176.
4. 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.
5. 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.
6. Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471.

7. Järvsoo, M., Norta, A.,Tsap, V., Pappel, I., & Draheim, D. (2018). Implementation of information security in the EU information systems: an Estonian case study. Challenges and Opportunities in the Digital Era: *17th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2018, Kuwait City, Kuwait, October 30 - November 1, 2018, Proceedings. Ed. Al-Sharhan,Salah A.; [et al.]*. Cham: Springer, 150−163.
8. 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.
9. Moor, J. H. (1991). The ethics of privacy protection. *Library Trends*, 39, 69-82.
10. Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, 27(3), 27-32.
11. Reidenberg, J. (1997). The use of technology to assure internet privacy: Adapting labels and filters for data protection. *Texas Law Review, 3(2),* 553.
12. Tsap, V., Pappel, I., & Draheim, D. (2017). Key Success Factors in Introducing National e-Identification Systems. In: *Proceedings of FDSE'2107 - the 4th International Conference on Future Data and Security Engineering, Ho Chi Minh City, Vietnam, November 29 - December 1, 2017, Proceedings.* Eds.: Dang, T.; et al. Cham: Springer, 455−471.
13. *Sue, V. M., & Ritter, L. A. (2012). Conducting online surveys. Sage publications, 33-35.*
14. United Nations, General Assembly. [2014]. Resolution A/RES/69/166 on the Right to Privacy in the Digital Age. Available: https://undocs.org/pdf?symbol=en/A/RES/69/166 [Accessed: 11-Jun-2019].
15. Wu, Y. (2014). Protecting personal data in e-government: A cross-country study. *Government Information Quarterly*, 31(1), 150-159.
16. 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.