TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Tatiana Iovu 186359IVGM

E-Governance Services Development and Data Protection – International Approaches and National Decisions. Case Study: The Republic of Moldova.

Master's thesis

Supervisor: Katrin Nyman-Metcalf

Co-Supervisor: Karin Oolu

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Tatiana Iovu 186359IVGM

E-riigi teenuste arendamine ja andmekaitse-rahvusvahelised lähenemisviisid ja riiklikud otsused. Moldova Vabariigi näitel.

Magistritöö

Juhendaja: Katrin Nyman-Metcalf

Kaasjuhendaja: Karin Oolu

Tallinn 2020

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: Tatiana Iovu

06.05.2020

Abstract

In developed economies, emerging innovations play a key role in fostering social integration, productivity, and progress. More and more governments nowadays begin to implement the Information and Communication Technologies for the intercommunication with the citizens and the Republic of Moldova is one of those countries. The e-Governance Technologies and Services Development in Moldova started in 2010, the Personal Data Protection legislation foundation was laid with the first Constitution of the Republic of Moldova, made a significant leap in 2011 with the Law no. 133/2011 on the protection of personal data, based on the European Union Directive 95/46 and still under development at the moment, because even after the General Data Protection Regulation has entered into force, amendments were adopted to the law, but the foundation was not changed. That area is one of the main research topics of this thesis, what changes have happened over the past 10 years, and to what extent has it affected the legislation on personal data protection? And in what manner governmental institutions are readjusting to the e-Services quality requirements and the rules on personal data protection? Another area of interest for this research is the citizens of the Republic of Moldova, their preparedness, and willingness to adapt to the new e-Reality. At the beginning of the research is already known and understandable, that e-Services are not popular among the citizens of Moldova, and services lack qualitative promotion and marketing. What are the main reasons for that, when Moldova has one of the best Internet coverages in Europe?

This is an interdisciplinary case study with the elements of quantitative and qualitative analysis. The research includes practical parts, that provide the analysis of the citizens' and state's perception regarding the digitalization of the governmental services and the legal framework of personal data protection.

Keywords: e-Governance, e-Services, legal framework, personal data protection, citizens' level of awareness, citizens' level of trust, MConnect, the Republic of Moldova.

This thesis is written in English and is 49 pages long, including 7 chapters and 15 figures

List of Abbreviations

APEC	*Asia Pacific Economic Cooperation*
CBPR	*Cross-Border Privacy Rules*
EaP	*Eastern Partnership Countries*
eID	*electronic Identity Card*
EU	*European Union*
GDPR	*General Data Protection Regulation*
ICT	*Information and Communication Technology*
IoT	*Internet of Things*
NCPDP	*National Centre for Personal Data Protection*
OECD	*Organization for Economic Cooperation and Development*
RQ	*Research Question*
SDG	*Sustainable Development Goals*
UN	*United Nations*

Table of Contents

List of figures

1 Introduction

Governance e-Transformation in the Republic of Moldova was launched in 2010 and since then, Moldova is a bright example in demonstrating how e-Governance services can provoke progress. The Republic of Moldova took the implementation of e-Governance solutions as a tool to execute the UN Sustainable Development Goals (SDGs)[1] and serves as a good example for other UN member states, which just started the implementation of e-Transformation.

The ICT development, specifically in the governmental area goes hand-in-hand with the privacy and personal data protection. Personal Data is any information associated with an identified or identifiable natural person (the subject of personal data). An identifiable person is a person who can be identified directly or indirectly, in particular, by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Article 12 of the Universal Declaration of Human Rights treats privacy as a distinct human right. It states that "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence… Everyone has the right to the protection of the law against such interference or attacks"(Universal declaration of human rights, 1948). In legal terms, privacy is not an absolute right. It can be restricted by certain reasons, for example, to protect national security or public safety, or, if it conflicts with other rights. Data privacy is not the same as data protection. The second one implies the way the third parties handle the information they hold about us, how it is collected, processed, stored, and used. In other words, data privacy is a broader aspect and data protection is one corner of it. While data protection is more defined, than privacy, how it is applied legally can still greatly vary based on which country you are considering.

The digitalization era has shown new ways of collecting, accessing, analyzing, and using data, often across multiple borders and jurisdictions. One of the big challenges is the systematic collection of personal data(any structured set of personal data that is accessible according to certain criteria, centralized, decentralized or distributed on a functional or geographical basis) and personal data processing (any operation or set of operations performed on personal data, both automated and non-automated, such as collecting, recording, organizing, storing, restoring, adapting or changing, extracting, consulting, using, disclosing by transfer, distribution or provision of other access, grouping or combination, blocking, deletion or destruction) by the government. ICT development now enables the government to monitor our transactions, conversations, and the

[1] Sustainable Development Goals of the United Nations. UNDP Moldova
https://www.md.undp.org/content/moldova/en/home/sustainable-development-goals.html
(Accessed on 19.03.2020)

locations we visit. In some countries private companies are legally required to store personal data locally for a longer period, making it easier for governments to get information on their citizens. The development of e-Governance technologies and services in the Republic of Moldova happened swiftly, the framework was created just in 4 years. It is of great importance to understand, how the legal framework of e-Governance in Moldova was developing alongside will all the services. The Republic of Moldova has a goal to become the European Union (EU) member state, which means that they need to have a long-term plan, regarding the e-services development for compliance with all the European standards regarding the software processes and quality assurance, legal framework, cross-border data transmission, and The General Data Protection Regulation (GDPR, Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data). Alongside GDPR, European Convention on Human Rights, the Fundamental Charter of Human Rights became the foundational pillars for the legislation of the Republic of Moldova, due to the vision to become an EU-member state. The detailed description of the requirements can be found in the European Union – the Republic of Moldova Association Agreement (EU and Republic of Moldova, 2014). ICT and e-Governance can be considered a very legal-sensitive topic, especially in the case of the Republic of Moldova, where the legal framework in this sphere is still under development (Nyman-Metcalf & Repytskyi, 2016).

2 Thesis motivation

The main goal of this research is to understand on what level the personal data protection is at the moment in the Republic of Moldova if it meets the GDPR requirements, how is it evolving, the specific directions and what are the hindrances for the future improvement. The main measurable will be the GDPR because Moldova has signed the Association Agreement with the EU, back in 2014 and this document contains a set of recommendations and regulations, that Moldova agrees to follow and fulfill. The main focus is to research whether the legal framework for personal data protection was built in line with the European legislation and how governmental entities have updated their policies and agendas for full compliance. The right to protect personal information is one of the main and fundamental rights, which is increasingly important nowadays. The development of e-Governance Technologies and Services and its legal framework have not been developed simultaneously in Moldova and that became a reason for gaps in data protection regulations.

The Republic of Moldova began the implementation of e-Governance and personal data protection solutions also based on 2 other main legislations, that are important for the Republic of Moldova as a potential EU member state. The documents are the Charter of Fundamental Rights of the European Union[2] and the European Convention on Human Rights[3]. For this reason, the failure of the Republic of Moldova to adequately take into consideration data protection is very important, as this detracts from a good example it could otherwise show others. When new electronic services are developed, the legal framework for these programs should be developed simultaneously. Otherwise, the new risk may occur, for example for the protection of personal data, or it may be difficult to develop effective laws, which are not overlapping or contradicting existing ones.

The outcome of this Master's thesis will be the analysis of the legal framework of e-Governance Services in Moldova and its evolution, along with the e-Services, recommendations for governmental, non-governmental and private organizations for full compliance with data protection regulations, analysis of the experiences of other countries, and unions. The legal framework of e-Governance stands for a broad system of rules that governs and regulates decision making, agreements, laws in the area of implementation of e-Governance services, and the legislation build around it and the citizens' data protection.

Personal data should be at least as secure in the e-World, as in the traditional one since E-Governance does not leave a choice for citizens, meaning sharing their data is a must. It is necessary to evaluate the development of e-Services and legal framework for those and personal data protection of the citizens. By investigating what gaps there are in these specific areas it will be possible to suggest solutions to the Republic of Moldova, but also, that will be relevant for other countries that go through similar development and meet resembling hindrances.

This research will become a significant contribution to the academic collection of the e-Governance system and the Legal Framework of Personal Data Protection of Moldova because at the moment there is a very low number of such studies.

2.1 Research questions and tasks

RQ1. How has the e-Governance system in the Republic of Moldova transformed over the past 10 years and to what extent has it affected the legislation on personal data protection?

[2] Charter of Fundamental Rights of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (Accessed on 19.03.2020)

[3] European Convention on Human Rights. https://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed on 19.03.2020)

The Republic of Moldova has established the right for privacy not so long time ago, starting from the moment the first Constitution of independent Moldova was introduced, in 1994[4]. Since then it was acknowledged as a fundamental human right. Starting with the introduction of the electronic data, the tempo of the development of the legal framework of the citizens' data protection has increased. The transition from the old school paper-based documents and face to face service delivery to online is happening till today and it is not clear when it will reach the maximal possible automation level. To understand how the future of e-Governance and Data Protection in Moldova will appear to be, it is imperative to investigate the past achievements and lapses.

RQ2. What is the level of citizens' awareness regarding e-Governance technologies development and personal data protection importance?
In the framework of this research, the understanding of the level of people's knowledge concerning their right to personal data protection and the development of the electronic and online service will be studied. The level of citizens' awareness and trust towards government is crucial for answering this question. People might be cautious about providing their data to third parties, different online platforms, businesses, and other various vendors. But how citizens feel about government storing, analyzing, and accessing their data; do they consider governmental entities more or less trustworthy, compared with the private ones? The government must have a clear understanding of that problem to have an efficient e-Service design and implementation. When people don't know their rights, abuse of those rights is inevitable. If we will take EU citizens as an example, in the year of the GDPR adoption, 2016 and before it entered into force, only third of Europeans were aware of the national public authority, that is in charge of their data protection, 15% only felt that they had complete control over their data (Bu-Pasha, 2017). To answer this question is needed to figure out, on which level the citizens of the Republic of Moldova are.

RQ3. How are the governmental entities adapting to the standards of e-Services quality and Personal Data Protection regulations?
To conclude this question, it is needed to analyze whether the most powerful governmental authorities are functioning in line with all the technological and legislative changes. The Republic of Moldova has signed the Association Agreement with the European Union in 2014; multiple rules, standards, and recommendations in the area of e-Governance and Personal Data Protection have been included in the agreement. To see the progress of the Republic of Moldova in those

[4] First Constitution of the Republic of Moldova. http://www.ccrm.md/constitutia-republicii-moldova-din-29071994-1-92 (Accessed on 26.02.2020)

areas, especially in the past 10 years after the very beginning of the digitalization in the country and 6 years after signing the agreement with the EU will be conducted the qualitative analysis of the national legislation and its implementation.

Research Tasks 1. Literature review for analyzing main data protection regulations and legal frameworks of e-Governance in different countries during various time frames.
Research Task 2. To evaluate citizen's level of awareness regarding the provided e-Services and their level of knowledge regarding their data protection rights via qualitative and quantitative methods, by distributing surveys among the citizens, that represent different age groups.
Research Task 3. Analyze the approach of the Government of the Republic of Moldova towards the adaptation of security features towards data protection via qualitative methods, conducting interviews with experts in the field of governmental e-Services and Data Protection.
Research Task 4. Propose a set of recommendations for enhancing data protection standards and increasing citizens' knowledge in the area of e-Services and ways of taking control over their data.

2.2 Research design and methodology

Consequently, a systematic literature analysis is a piece of work to its terms that can answer far wider issues than any simple empirical study will ever do. Nonetheless, systematic literature reviews are placed at the peak of the pyramid over many research designs as it can produce extremely relevant functional connotations (Siddaway, 2014).

For this study, mixed research methods were applied. To analyze the evolvement and current state of the e-Services, the legal framework of e-Governance and the level of citizens' involvement in the processes and their knowledge in the field, providing recommendations to the governmental organizations that are at the beginning of the e-Governance development and to the Governmental organizations of the Republic of Moldova, this approach was the most efficient. In the interest of delivering unbiassed recommendations, it is essential to look at the current state from two viewpoints: governments and citizens. Information may be retrieved qualitatively in this kind of study, but it is also quantitatively evaluated using quantities, ratios, estimates or other statistical analyses to evaluate connections. Furthermore, qualitative research is more systematic and also requires a diverse array of data from multiple channels to obtain a broader understanding of the stakeholders, particularly their opinions, experiences, and perceptions. To provide exhaustive research on the topic, after setting all the research questions and tasks, to determine the level of the citizens' awareness of e-Governance services and their rights on Personal Data Protection, the quantitative research took place. In the case of the current study, the quantitative research was the best solution because it provides the most up-to-date information and methods of getting it are tailored to answer a specific set of questions and collect the empirical data regarding the specifically defined objects instead of referring to already existing, but outdated data, that only partially can provide the necessary answers.

As the primary step of the quantitative research, a survey was conducted and shared out via social media, e-mail lists, and personal messages. The aim was to cover 5 age groups, all of the respondents were in the range of 18 to 55+ years old, to evaluate which age groups are more prepared and comprehend the necessity for changes in the e-Governance and Personal Data Protection systems in the Republic of Moldova. Surveys were published in 3 languages: English, Russian, and Romanian, to give all the citizens and permanent residents the deepest understanding of the stated issue. Despite the fact, that the surveys were distributed only via online channels, it is beneficial, due to the fact, that it was also possible to reach also the citizens of the Republic of Moldova, that are located abroad. In the very beginning, all the respondents were informed, that their answers and opinions are anonymous, secure, and will be used for this research only. Except for multiple-choice questions, there was one open-ended question, that asked the respondents to suggest which services would be most useful for them to have online. Survey research takes advantage of quantitative screening and survey format to test public preferences with numerical accuracy. It aims to include responses to questions like "How many people feel a certain way?" Survey research helps to do correlations among categories. It presents forecasts from a trial that can be linked to confidence for the overall population (Sukamolson, 2007).

Qualitative research was utilized to collect the adept opinion via face to face, semi-structured interviews; some of the questions were used in every interview and the rest varied based on the area of the interviewee’s expertise. Some of the interviews were conducted in English, some in Russian or Romanian. All of them were transcribed, the Russian and Romanian ones were also translated into English, all of them were coded in the end. Qualitative research is mainly aimed to comprehend the organizational processes and not on predicting outcomes and outputs (Lee, 1999). This approach is beneficial for applying it to detect the gaps in online governmental services and spot the breaches in Data Protection law and its implementation by all the actors. Qualitative study is reflected through simple language, while the quantitative study is demonstrated through numerical and mathematical models. Qualitative research involves small sample sizes, while quantitative research is focused on the study of the big numbers.

The qualitative analysis relies on upon opportunistically or deliberately selected cases while quantitative analysis utilizes random sampling (Green, 1999). Qualitative analysis also focuses on specific individuals, incidents, and circumstances, linking itself to an analytical style. Quantitative analysis is far more inclined to concentrate on characteristics that can be expanded to a broader population. Qualitative research serves as a preferred approach to investigate, interpret, and evaluate new phenomena via analytical and conceptual study.

This work will provide new perspectives regarding the protection of personal data, citizens; knowledge in this area, and awareness regarding the e-Governance services and solutions, possible alternatives, and recommendations to current hindrances will be proposed with a view to setting out grounds for future amendments.

3 Literature review

Privacy became a more significant human value during the period of the industrial revolution. By the end of the nineteenth century, learned justices in the United States discussed it, arguing that "the right to be let alone ... secures the exercise of extensive civil privileges" (Warren et al., 1890). Historical and in some cases philosophical discussions of privacy could be found in (Seipp, 1978), (Schoeman, 1984), (Bennett & Grant, 1999). The dominant approach to privacy is to perceive it as a fundamental human right. It is expressly recognized in the key international instruments, the Universal Declaration of Human Rights (UDHR, 1948) at Article 12, and the International Covenant on Civil and Political Rights (ICCPR, 1976), at Article 17, which use the same form of words: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence ... Everyone has the right to the protection of the law against such interference or attacks.”

The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals about the processing of personal data and the free movement of such data places itself squarely in this tradition in declaring at the outset that its objective is to "protect the fundamental rights and freedoms of natural persons and in particular their right to privacy concerning the processing of personal data" (EU 1995, Article 1.1). The GDPR was developed as a substitute for the 1995 Data Protection Directive, which serves as the basis for a legal framework in multiple countries within and outside the EU and is of great importance for the Republic of Moldova. The difference between regulation and directive is that the first one provides standards for the member stated, based on the countries that are supposed to create and update their legislation for compliance. The regulation is a unified code of laws, which stay above all the EU national legislation (Robinson et al., 2009). Unlike its predecessors, which was incorporated into law separately by each state as they deemed appropriate, GDPR is being compulsory in its totality and expressly accessible to each state within the European Union.

There has therefore been some degree of a drift towards a perception of privacy as an economic right. This is consistent with business interests because it enables administrative efficiency to be valued very highly when balanced against privacy, and hence to force more substantial compromise than would be feasible if privacy were regarded as a human right. There are several variants to the economic rights school of thought, which grant more or less freedom to the individual, and less or more power to organizations that handle data about them. First of all nowadays, in the past decade, authors have looked into the initiation and starting development and evolution of e-Governance (Freitag & Traunmüller, 2009), different countries have "jumped" on the e-Governance trend in different timeframes and often, the countries, that have started the development of certain technologies later, than others, have made more significant progress, compared to the first ones (Nyman Metcalf & Repytskyi, 2016), (Kerikmäe, 2014). Multiple authors have looked into the variety of disciplines that e-Governance consists of, computer science, information sciences, administrative and organizational sciences, sociology, and political science (Hans J. Scholl, 2015).

E-Governance is extremely sophisticated in promoting accountable, accessible, inclusive, transparent, and reliable public services that provide citizen-centered results. Now, there are tendencies in the deployment of e-Services, particularly in the fields of healthcare, school, and decent jobs, while access to the most fragile is increasing. (United Nations, 2018). Another set of documents, that serve as a foundation for personal data protection overall are the EU Charter of Fundamental Rights of the EU (Charter of Fundamental Rights of the European Union, 2016) and the European Convention on Human Rights (European Convention on Human Rights, 1953). According to J. Lee, e-Governance is the metaphor for the last stage of e-Government development (Lee, 2010). That means, all the conclusions and main metamorphosis will be happening in the framework of the e-Governance itself.

This compelling contribution explores and addresses the varying definitions of the importance of protecting personal data. In the context of data privacy law, it follows their alleles, stressing that those are at least to some degree rooted in specific national solutions (González Fuster & Gutwirth, 2013). The explanation for this is that search results, data web sites, and social networking platforms that have claimed control of the information they receive may understand that they have to ensure that they adopt best practices in the way they obtain and utilize the specific data (Rees, 2014). The principles of e-Governance are based on pillars, that are similar for every government, that is planning to implement this innovation. In the case of international organizations, it would be relevant to refer to two main, the United Nations (UN) and the Organization for Economic Cooperation and Development (OECD), (Riley, 2003).

Next principles unite those two organizations regarding the e-Governance development:

1. Citizen-centric design for every service;
2. Clarity and level of understanding of the services;
3. Assurance of citizen’s rights for access, privacy, and confidentiality for all.

One of the first outspoken declaration for the rights for privacy states that: “It is not, however, necessary, to sustain the view that the common law recognizes and upholds a principle applicable to cases of invasion of privacy, to invoke the analogy, which is but superficial, to injuries sustained, either by an attack upon reputation or by what the civilians called a violation of honor; for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration“ (Goldsmith et al., 1890).

Despite the past years and industrial development, these words haven’t devalued. And the rest of the researches, conducted on personal data protection is based on these principles. The fundamental legislation in this area was the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data, adopted by the Council of Europe on January 28, 1981, and subsequently supplemented by a protocol on the powers of supervisory bodies and cross-border data transfer. Based on the provisions of this Convention at the national level, European countries have adopted separate laws on the regulation of personal data (Савельев, 2018). A study conducted in 2009 by the Microsoft Research state that even anonymized data shared on the Internet can disclose people’s identities. Just based on private Google queries, we can see, that it’s easy to establish it based on their location requests, symptoms research and sometimes, people also google search themselves (Korolova et al., 2009). On the importance of the citizens’ trust aspects and worries regarding the technical development in the digital age, we can refer to K. Nyman Metcalf, “In many countries, a majority of people still feel that electronic data is more vulnerable than paper-based data; to some extent, this may be a generational issue, but there are also other reasons. The new operations that can be performed thanks to electronic data and automatic data processing, such as face recognition or, generally, the compilation of enormous amounts of data that at least in practice would be impossible to do manually, do entail new risks.” (Nyman Metcalf, 2014).

Some of the fundamental objectives of data gathering and distribution were the value of assurance, to be a person's defined freedom to transmit a piece of limited information concerning them in absolute conformity with a specific necessity. Throughout the Big Data era, the primary focus is on information recycle, because all data obtain true value regardless of circumstances. It applies to information possibly related to citizens' details which could potentially classify as personal data.

There has to be intangible importance in this kind of information recovery. Statistics on customer transactions also permit targeted advertising, and also research and analysis, as well as consumer situation predictions. More and more information a company owns, the worse the potential it has in the deployment of Data analysis techniques to identify different types that could be essential for management decisions (Савельев, 2018).

During the previous 10 years, the data protection laws amount has increased the most, compared to the other 3 decades (Greenleaf, 2015). According to the study, from 2010 to 2015, 29 laws have been issued, 2000-2010 - 39 laws, 1990-2000 – 20 laws, previous decades 9 and 12; almost a mathematical progression. That we can see, the legal development was happening all along with the improvement of tech-savviness.

4 International Approaches to e-Governance Services development and Data Protection

In the following chapter review of the e-Governance services evolvement and its legal framework, with the accent on Personal Data Protection legislation will be made. Based on the analysis of various regional developments, it would be possible to observe some worldwide tendencies, patterns, and the most and least successful examples to make recommendations.

4.1 GDPR

The General Data Protection Regulation is the main document that regulates the citizen’s data protection all across the European Union states and also in other countries in cases when they deal with the EU citizens’ data. The GDPR is a so-called replacement for the Data Protection Directive, which was the main regulation policy for data for 20 years, from 1995, which the same as GDPR was an essential part of the EU privacy protection and human rights legislation. The GDPR is an important and necessary “upgrade” in this area, regarding the tech-boost that happened in those 20 years and affected all the processes, regarding collecting, processing, retaining, and analyzing data (O’Brien, 2016; Safari, 2017). Advancement of technology and globalization has formed many various challenges when people protect their freedom to protect sensitive information that they have, experienced in the EU overall. Private data is migrating easier due to modern technologies, private companies, and government authorities, that use private data way more, compared to 10 years ago and people have become more transparent with their private data. GDPR also creates an essential part of a legal structure inside the data community.

A single data privacy approach, implemented in the EU via the General Data Protection Regulation, which seeks to consolidate and clarify fragmented laws currently enforced at the state level. Such a statute helps to identify proactive science and development by specifying standards of legal and pragmatically appropriate conduct in the data protection context. These data are progressively gathered and distributed through developing ICTs, sparking a need for acute evaluation (Jasserand, 2018). Due to the likelihood of individual negligence of the possible applications and meaning of personal information, and the questionable security provided by the right to liberty from surveillance, it does seem reasonable to propose measures to safeguard security outside the requirements of the Law. Although the legislation codifies concepts of "equal data" that restricts the contact among data trustees and authors, providing that reasonable consent processes are adopted and that data mining has a specific intent and objective, such concepts do not seem to resolve the above-mentioned concerns. (Koguchi, 2020)

According to Article 5 of GDPR, there are six data protection principles:

1. Lawfulness, fairness, and transparency

   A regulation update is covering the data breach part. In case a data breach is discovered, the data controller must notify about it both the supervisory authority and the data subject. It concerns not only EU bodies, but also all the entities outside of the European Union, that hold or process the data of the EU citizens (O'Brien, 2016).
2. Purpose limitation

   This particular principle is about the usage of data. In case it was collected for the analysis of the usage of public services in a country, it cannot be used for any other purposes, researches, analysis. This is the phenomenon of "repurposing the data", a growing phenomenon, its consequences are irreversible, in case the data was collected for marketing purposes and it is being used, for example, for law enforcement (Jasserand, 2018).
3. Data minimization

   This principle sets a limitation on the amount of data that can be held or processed. In the sense, that if a marketing agency providing ads needs to know only the gender or age, that is illegal for them to get any kind of the medical data of that data subject. Regarding the state authorities, medical institutions are not allowed to access data subject's criminal records, etc.
4. Accuracy

   This principle might be most relevant to the healthcare system. In case that data is not up-to-date, or redundant, it can cause complications for the patient, in the case when mid-diagnosis was not replaced with the final diagnosis.

5. Storage Limitation

   The right to be forgotten is the piece of legislation that assists data subjects in having control of their data. Anyone can contact the data processor or the data controller and request the deletion of their data. In the majority of the cases that is exactly what will follow, but there is also a "reserve" from the requirement to forget. According to the Articles 17.3 and 89 of the GDPR, the personal data can be kept in case of need for archiving, if it can carry some public interest, or in need of establishment or defense of the legal rights (Politou et al., 2018)
6. Integrity and Confidentiality

   Article 5.1(e) obliges all organizations public and private to take all the necessary measures, to provide full data protection and privacy from damage, destruction, or unauthorized or illegal data processing (IT Governance privacy team, 2017).

When analyzing experiences of other countries, we can make a solid conclusion, that GDPR is the brightest example and reference for other countries, when developing their national or regional policies and legislations on personal data protection. GDPR cannot be called only an unrivaled European Policy, because this regulation is of a worldwide meaning.

Within the European Union countries have the free movement of people, goods, and information. Based on that, the cross-border data exchange became reality and all the queries can be answered with high speed. Based on Chapter 5 of GDPR, data can be transferred to third countries and international organizations by request. Article 45 states that the European Commission, first of all, has to evaluate the third party based on a wide spectrum of criteria for compliance, will gauge the level of adequacy of protection in a certain country/organization, and based on those procedures will make a verdict.

4.2 Asia Pacific Economic Cooperation

Beginning with the Asia Pacific region and APEC (Asia Pacific Economic Cooperation) countries, we could follow a tendency of creating a similar system to the European Digital Market. accountability, data minimization, the right to be forgotten, data protection by design and data proportionality (M. James Daley, 2015).

The development and launching of APEC's Cross-Border Privacy Rules Framework became the turning point for the whole region. In 2011, it was processed and accepted by the APEC leaders[5]

[5] Cross Border Privacy Rules System http://cbprs.org/about-cbprs/ (Accessed on 25.02.2020)

and became a bright example for other world regions. The core policies, rules, and guidelines of the Cross-Border Privacy Rules (CBPR) have been under the process of intense evolution from 2004 until the year 2015 (Fletcher, 2015).

The main outcomes for the CBPR must be:

- Data subjects' (consumers') absolute trust in the cross-border data transmissions systems
- Guarantee that there will be no irrational hindrances to cross-border data exchange yet at the same time providing the confidentiality of the personal data of their residents at home and globally, in coordination with foreign entities (Ibid.).

Another important change for the region was the declaration in July 2018 of an "equivalence" treaty[6] involving Japan and the EU. As the GDPR drives EU data privacy requirements increasingly higher, conclusions of suitability continue to be more out of scope for APAC regimes, even with the area's rapid rate of regulatory change. "Equivalence" arrangements whereby the non-EU authority decides to implement EU data security requirements to private data transferred from the EU could well be the way ahead, rendering the innovations in Japan essential to monitor.

Nevertheless, more relevant to the development of legislation in the Asia-Pacific area is the idea of much more competition for data security in the area as people are rapidly engulfed in a modern digital world introduced on by the wide usage of cell phones and the advent of the IoT. At about the same time, the area's authorities are working together towards digital identification systems and more aggressive solutions to electronic monitoring. In this context, the GDPR principles illustrate the potential necessity for more security laws in the area (Hogan Lovells, 2019).

APEC's experience and case studies can be useful for the current implementation of the legal framework of e-Governance and Personal Data Protection for the Republic of Moldova, but also the Eastern Partnership region.

4.3 Eastern Partnership countries

For all 6 countries of the Eastern Partnership (EaP) (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine), Estonia was the main role model regards to the development of the e-Services and as much as possible, of the legal framework of e-Governance, based on the initial existing legislation on the country level. All countries are connected with the common USSR past, communist systems. The transition from previous regimes to democratization was not smooth and time-wise pretty tightened. Bureaucracy still can be considered a major problem in the existing

[6] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the EU. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data (Accessed on 1.03.2020)

governmental systems and major development of e-Governance systems should serve as a breakthrough. The expression "open government" may not see the government as a set of administrative and technological tools, but rather a unique government system of public administration. An open government is conceptualized, on the one hand, as transparency and usability of information on the operations of administrative organs, and, on the other, as involvement and presence of citizens in the system of government administration, such as foundational security of civil rights. Therefore, it could be said the perception of e-Governance has progressed from the public service provision and the performance of state functions in digital form to a structure of open government frameworks and concepts.

At the moment, the EU-Council of Europe Framework Partnership Program (PCF) aims to establish and provide a comprehensive knowledge base and capabilities to create the potential of authority in six Eastern Partnership countries to bring regional policies into effect. Its aim is also to introduce them to the criteria of the Council of Europe and the European Union in the areas of the protection of human rights, democracy and the rule of law, as well as the development of living standards[7]. The main focus of the EU in the EaP countries in the prevention of cybercrimes and increasing the level of cybersecurity, which is tightly connected with the citizens' data protection. The agreement, between EU and the EaP countries, documented in the Declaration of the Second EaP Ministerial Meeting on the Digital Economy (October 2017, Tallinn). One of the most important factors is to deploy more efforts in line with EU security practices to facilitate the advancement of regional cybersecurity systems and national logistical Computer Emergency Response Teams[8]. By helping recipient states concentrate on mutual concerns, a regional strategy has the arcanist between participating countries, thereby fostering extra security, sustainability and development, in the region, while enabling for bilateral initiatives to tackle state-specific needs.

Georgia, Moldova, and Ukraine have implemented regional cybersecurity policies, but only Georgia and Ukraine have departmental control divisions. Risk assessment units are in Azerbaijan, Belarus, and Georgia. A communication point for global cooperation has been established for purposes in Azerbaijan, Belarus, Georgia, and Ukraine. The essential security of assets is tackled only in Belarus and Georgia. CERTs or analog agencies are developed in Azerbaijan, Belarus, Georgia, Moldova, and Ukraine[9]. These steps are the most common for the region and demonstrate to be the most effective to tackle the problems in the entire region.

[7] Council of Europe. Partnership for Good Governance. https://pjp-eu.coe.int/en/web/pgg2/home (Accessed on 3.05.2020)

[8] Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/c_2018_8184_f1_annex_en_v1_p1_1000418.pdf (Accessed on 1.05.2020)

[9] Ibid.

4.4 Case of Estonia

The main reasons for Estonia's success in electronic development are the general agreement between the driving forces of Estonian society. Thanks to this agreement, political leaders had a desire to develop this direction, although it requires financial costs and resources. The initiative came from both the public and private sectors, but the government also played an active role. Other reasons for success lie in the fact that Estonia, a small country, is located not far from Finland, one of the leaders in the movement towards the information society. But the main factor, perhaps, was the desire of society to find the possibility of rapid development.

The role of the national e-Development strategy in Estonia was fulfilled by a document entitled "Principles of Estonian information policy"[10], which clarified and streamlined thinking in this area. It was considered, that the information society as a comprehensive concept, abandoning a purely technological approach to this concept and then the government's role was determined, the fact of what place government occupies is very important. The first and most important thing that the government must do is to provide support for the movement towards the information society. Then - to provide conditions in which the information society can develop. Estonia set the primary goal - to achieve equitable and affordable access to information and communication technologies (ICT) for everyone, regardless of geographical location, and to ensure the active provision of information by the government - that is, to make the state open (Anthes, 2015). As for the coordination of all these efforts, for many years Estonian government did not have a special state body in this area. And now, when these issues are coordinated by the Ministry of Economics and Communications, many consider this situation to be not very convenient. It was called the "soft coordination" of government initiatives, if only because no one knew what needed to be done, and naturally did not want to take risks when making decisions. "A big challenge in developing governmental e-Services is keeping them decentralized for security while preserving cross-application compatibility"(Anthes, 2015).

Based on facts and multiple studies, 3 main pillars of the Estonian e-Services are X-Road, eIDs, and eesti.ee, the threshold of all the other services. The biggest benefit of the X-Road is the fact, that the system is entirely distributed, when many mistakenly consider it being centralized one(Margetts & Naumann, 2017). In Estonia, all government services have an e-Service feature. Electronically signed documentation must be recognized by all Local and state departments, public law entities, as well as private arbitration individuals conducting public law roles. Via eesti.ee platform every citizen can check, which governmental authority has accessed their data and based

[10] https://ega.ee/wp-content/uploads/2020/01/Eesti-infopoliitika-p-hialused.pdf

on that information build causal relationships; if any of the accesses cause suspicion, every citizen is free to investigate the case.

Estonian citizens today can vote from their computers, and dispute tickets for parking from anywhere. It is possible via the "once-only principle" that states that no specific bit of information is to be submitted repeatedly. Applicants have their data — earnings, loans, investment — pulled from somewhere in the system instead of having to "prepare" a loan request.

Regarding the legal framework of e-Governance, since the very beginning, Estonia was not trying to think through a set of laws, that will be actual for the next 30 years. Vice versa, they concentrated on the legislation step by step. Estonia has embraced the fact, that trust is the main pillar and the legal framework will be a tool to strengthen it, and GDPR is one of the main contributors. The legal framework in Estonia from the outset was structured to consider e-Governance as an element of governing, but as least additional regulations as necessary; some anticipate Estonia to create an impressive amount of e-Governance policies, this isn't the scenario (Nyman Metcalf, 2019). The failure to develop special regulations makes sure that advantages of e-Governance will percolate the state's constitutional and organizational structure and that e-Services are incorporated into the federal rules regulating the numerous services. The legal structure includes unique rules, centered on a legislative requirement to define appropriate requirements for a portability program.

Regarding the Personal Data Protection Estonia, the most recent law is the Personal Data Protection Act[11], which came into force at the beginning of 2019. Articles 24 and 25 are of great importance for the further analysis of the legislation of the Republic of Moldova; Right of data subjects to obtain information and personal data concerning them and Right of data subjects to request rectification and erasure of personal data that have been introduced to the legislation of the Republic of Moldova not a long time ago (see Chapter 5.2).

5 National Decisions - Case study of the Republic of Moldova

The following chapter will be analyzed the current state of e-Governance system on its legal framework with the main focus on the Personal Data Protection legislation and their evolution. Likewise, the activity and role of the National Centre for Personal Data Protection will be evaluated; all the theoretical conclusions will be affirmed or abnegated by the expert opinion of 5 specialists from the Republic of Moldova, who's daily job directly or indirectly is dependent on the aspects, that are listed above.

[11] https://www.riigiteataja.ee/en/eli/523012019001/consolide

5.1 Political Situation in the Republic of Moldova

The Republic of Moldova has not seen a stable political power for decades. In 2019 Moldova has combated the oligarchy, via extremely difficult measures. Starting with 2016, the Republic of Moldova has a new president, Igor Dodon, the former leader of the Socialist Party[12]. This was the first time since 1996, the direct election of the President happened, applying the two-round system. Moldova is a Unitary, Semi-Presidential Republic with a Parliamentary System. Until the end of 2016, when Socialist Party leader Igor Dodon took the first direct presidential election in the Republic of Moldova on the 13th of November and the national mood again swung more towards a balance among pro-European and Eurasian orientations, Moldova was one of the pioneers of the European integration among the post-Soviet countries. The Republic of Moldova was the first to get a visa-free regime with the Schengen countries after the Baltic states in April 2014.

During Mr. Dodon's Presidency time, he was temporarily suspended from his position, six times by official decision of the Constitutional Court of the Republic of Moldova, while the authority was delegated to the President of the Parliament – Adrian Candu. This kind of opposition between the President and the Parliament was continuous and started changing in the second half of 2019. "Igor Dodon - informal leader of the pro-Russian Party of Socialists has been openly zig-zagging towards EU, visibly tempting to combine pro-Russian sympathies with pro-EU pragmatism. Considered as a hardline critic of the EU, Igor Dodon started gradually to separate his rhetoric into negative and pragmatic opinions." (Cenușa, 2019).

To provide a practical example of critical political instability in the country, we can look into the Parliamentary elections in 2014. The Socialist party, who first got into parliament and immediately received 25 seats. The power coalition retained its main positions, the speaker was Andrian Candu, close to V. Plahotniuc, but failed to agree on the appointment of the Prime Minister. Firstly, the Liberal Party of Mihai Ghimpu began to demand more ministerial seats for itself than angered the coalition partners. Secondly, the candidate nominated by liberal democrats Prime Minister Yuri Leanca received approval only from the Liberal-Democratic Party and Democratic Party. As a result, they had to ask the Communists for help, and a strange minority coalition formed when the Democrats and liberal Democrats made decisions and divided their portfolios, while the Communists helped them without entering the ruling circle. After almost 3 months of negotiations, the government of Kirill Gaburich was formed.

However, this cabinet lasted less than four months - on June 12, K. Gaburich resigned. Apparently, he realized that they were going to make him a look guilty in the case of the stolen billion from

[12] Election Guide. Democracy Assistance & Election news. Republic of Moldova http://www.electionguide.org/elections/id/2990/ (Accessed 15.03.2020)

the state budget (Mocanu, 2017) and decided not to play along with the oligarchs. The acting Prime Minister became Natalia German. After a month and a half of consultations, on July 30, a new prime minister was elected - Valery Strelets, but he was not destined to sit in a chair even for 100 days: on October 29, the government was dismissed by the votes of socialists, communists, and democrats. Another acting the premiere was George Brega. Thus, in 2015 in Moldova, there were two Prime Ministers - Gaburich and Strelets, which together held out just 225 days, and three acting Prime Ministers - Leanca, German, and Brega (Vardanyan, 2016).

The current situation and the continued partnership with the EU rely on the wide range of political after-electoral alliances that can emerge along with several specific scenarios. Outcomes, whereby pro-Russian socialists take over the government or an alliance, are renegotiated between the new governing party and the Socialists are similarly conceivable. The least likely is to unify all pro-EU powers that have joined the elected legislation (Cenușa, 2019).

5.2 Evolution of the Personal Data Protection and Interoperability law in the Republic of Moldova

One of the most significant factors, that is influencing the legislation of the Republic of Moldova is the Moldova-European Union Association for Agreement, signed in June 2014. It states that the legislation of Moldova is supposed to go "through the approximation of its legislation to that of the European Union" (EU and Republic of Moldova, 2014), Article 1, paragraph 2f, and Article 22 and 30 of the same document. Article 22 covers the expected outcomes of Moldova-EU cooperation regarding the e-Governance. Both parties aim to develop an effective system of cross-border information exchange between the EU member states and the Republic of Moldova, business-wise, Article 28.

Specific national legislation:

- Constitution of the Republic of Moldova, Article 28, "The state shall respect and protect the private and family life".
- Law on personal data protection of 15.01.2007 (abrogated)
- Law nr. 133 of 08.07.2011 on Personal Data Protection, that covers both public and private sectors.
- Law nr.208 of 21.10.2011 on amending and completion of some legislative acts.
- Law regarding the 2013-2018 data Protection strategy of 10.10.2013

Governmental decisions:

- Governmental Decision on the Requirements on Personal Data Security of 14.12.2010
- Governmental Decision on the Register of Personal Data Controllers of 15.05.2012

- Governmental Decision on approval of the Reform Action Plan on the modernization of public services, for 2017-2021[13]

The national law on Data Protection and Interoperability was developing since 2007. The first difference that we find is already in the first articles of these variants of laws (2007 and 2011), namely, Article 2 part 4, paragraphs of the new law expands the areas, that not covered by the law, namely: the processing and cross-border transfer of personal data related to those responsible for committing crimes of genocide, war crimes and crimes against humanity or with victims of such crimes. We can say that the basis of this amendment includes rules that ensure the protection of the dignity and freedom of each individual. In their totality, fundamental rights form the basis of the legal status of an individual.

Next, we consider article 3 of both versions of this law, which discusses the basic concepts, keywords, with the assistance of which we can correctly interpret this law. The 2011 version expanded its article with such concepts as - controller, processor, depersonalization of personal data, personal data accounting system. We can conclude that time does not stand still, and there is a development of technologies and methods for processing personal data. With the successful launch of the e-Governance services in Moldova, the upgrade of the legal frameworks is an inevitable process. We also draw attention to the legal framework of the new law, namely the Convention for the Protection of the Person in Connection with the Automatic Processing of Personal Data, the Additional Protocol to the Convention.

We see the following improvement of the law in article 4(d), namely, this paragraph deals with the correctness and accuracy of the data - accurate data are updated if necessary. Inaccurate or incomplete data, for the purposes for which they were collected or for which they were subsequently processed, should be deleted or corrected. There is no such clause in the 2007 version, therefore, the issue of inaccurate data remained controversial, and non-specific data were stored anyway, and the public authority could be misleading. And the storage of personal data for longer periods for statistical purposes or theoretical or scientific research is subject to safeguards in the processing of personal data provided for by the rules governing these areas, and only for the period necessary to achieve these goals. Compliance with and enforcement of the provisions of paragraph one is the responsibility of the controller. This is also an innovation, since in the law of 2007 this term did not exist, and accordingly there was no clear delineation of responsibilities of persons who process personal data.

[13] Resolution Nr. 966 from 08/09/2016 on approval of the Reform Action Plan on the modernization of public services, for 2017-2021 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=366273&lang=2 (Accessed on the 01.03.2020)

Both versions of the law regulate the processing of personal data, Article 6. This process is carried out by the consent of the subject of personal data. However, in the new version of the law, innovation was the introduction of a new category of subjects and the protection of their rights. We are talking about the processing of personal data of special categories of persons (incapable or partially incapable) and cases where this processing is prohibited. So, the processing of special categories of personal data is prohibited, except when: the subject of personal data has given his consent. In the event of incapacity or limited legal capacity of the subject of personal data, the processing of special categories of personal data is carried out only with the written consent of his legal representative; processing is necessary in order to fulfill the obligations or special rights of the controller in the field of labor law, provided that it is carried out in compliance with the guarantees provided by law, and also taking into account that any disclosure to third parties of personal data processed for these purposes can only be carried out if the availability of the relevant legal obligation of the controller; processing is necessary to protect the life, physical integrity or health of the subject of personal data or another person, if the subject of personal data is physically or legally unable to give his consent; processing refers to data, that was voluntarily and explicitly made publicly available, by the subject of personal data; processing is necessary to determine, exercise or protect the rights of the subject of personal data in court; processing is necessary in order to ensure the security of the state, provided that it is carried out in compliance with the rights of the subject of personal data and other guarantees provided for by this law. In all other cases, it is prohibited if there is no written consent of the official representative, guardian, or trustee.

Also, an innovation was article 7 of the new law, which regulates the processing of personal data regarding health status. This article states that derogations from article 6 are possible if the processing is required for preventive medicine, establishing a medical diagnosis, providing medical care or treating a subject of personal data or managing health services operating in the interests of the subject of personal data, the processing is required for public health protection. Medical workers, health care facilities and their medical personnel may only process personal data regarding health conditions without the permission of the National Center for the Protection of Personal Data, only if the processing is necessary to protect the life, physical integrity or health of the subject of personal data. If these goals relate to other persons or society as a whole and the subject of personal data has not given express written consent, the permission of the Center must be obtained in the manner prescribed by law.

Article 8 regulates the processing of personal data regarding criminal penalties, coercive procedural measures or sanctions for offenses; it can only be carried out by public authorities or under their control within the limits of the powers granted and per the conditions established by laws governing these areas. The old version of the law did not give us a clear understanding of how and by whom the data are processed during criminal proceedings. The register of forensic and criminological information is maintained by the Ministry of the Interior.

Another innovation in the new law was the processing of personal data from data with an identifier function. Processing of the state identification number (IDNP) of an individual, fingerprints, or other personal data performing the function of a general-purpose identifier may be carried out under one of the following conditions, the data subject has given his consent; processing is expressly provided for by law. This change is a consequence of the development of technologies used in the forensic identification of progress in the field of registration in information systems, etc. An interesting change in Article 10 of the new law, which states that the provisions of Articles 5, 6 and 8 do not apply in cases of the processing of personal data carried out exclusively for journalism or the purpose of artistic or literary creation if the processing relates to data voluntarily and explicitly made publicly accessible by the subject of personal data or closely related to the status of the public figure of the subject of personal data or the public nature of the actions in which he is involved, following the Law about freedom of expression. In this case, the rights of journalists, public figures are protected, but only if this information is obtained for literary creation and is related to the publicity of the subject.

The old law completely lacks the provisions of Articles 12-17. The new law regulates informing the subject of personal data (if personal data is collected directly from the subject of personal data, the controller or processor must provide, except when he already has it, the following information:

- the identity of the controller or, if any, processor;
- purpose of processing the collected data;
- additional information, such as recipients or categories of recipients of personal data;
- the availability of access rights, interference with data and objections, as well as the conditions for the exercise of these rights; whether the answers to the questions with which the data are collected are mandatory or voluntary, as well as the possible consequences of refusing to answer.)
- the right to access personal data, any personal data subject has the right to receive from the controller upon request without delay and free of charge: confirmation whether or not the data related to it has been processed, as well as information about the purposes of the processing, categories of data used, recipients or categories of recipients to whom the data are disclosed;
- personal data message that is the subject of processing, as well as any available information about their origin, in an accessible form and in a manner that does not require additional equipment for understanding;

- information on the principles of the mechanism used in any automated processing of data relating to the subject of personal data;
- information on legal consequences for the subject of personal data arising as a result of data processing;
- information on the procedure for exercising the right of intervention concerning personal data, the right to intervene concerning personal data. Any subject of personal data has the right to receive from the controller or processor upon request and free of charge: correction, updating, blocking or deletion of personal data, the processing of which is contrary to this law, in particular, due to the incomplete or inaccurate nature of the data;
- notification of third parties to which personal data are disclosed about transactions performed under paragraph (a), except in cases where such notification is impossible or requires a disproportionate effort in comparison with the legitimate interest that may be infringed, the right of the subject of personal data to object. The personal data subject has the right at any time to free of charge, on a justified and legal basis related to his private situation, objection to the personal data relating to him becoming a subject of processing

  unless otherwise provided by law. If the objection is justified, the processing performed by the controller cannot further affect this data. The subject of personal data has the right at any time and without any justification to object free of charge that his data be processed for direct marketing purposes. The controller or processor must inform the subject of the right to object to such use before disclosing personal data to third parties.
- A person may be affected by the decision indicated in paragraph (1) if: the decision is authorized by the law establishing measures to ensure the legitimate interests of the subject of personal data; the decision was made during the conclusion or execution of the contract, provided that the request of the personal data subject for the conclusion or execution of the contract was satisfied.
- Access to justice. Any person who has suffered damage as a result of the illegal processing of personal data or whose rights and interests guaranteed by this law are violated, has the right to apply to the court for compensation for material and moral damage.

One of the distinguishing features of the new law is the entire 5th chapter, which is fully devoted to controlling in the field of personal data protection. This article clearly describes the responsibilities of controllers in the processing of personal data - notification of the Center (controllers directly or through processors are required to notify the Center before processing personal data intended to serve a single purpose. Processing of categories of personal data other than those for which notification is made is carried out when subject to a new notice, Article 23 of the law governs the contents of this notice, what it should include), preliminary verification (if based on Upon notification, the Center will establish that the processing falls into one of the categories defined in paragraph (2), and within five days after the notification is submitted, it orders that a preliminary check be carried out without fail, which the controller or processor will inform. Article 24 governs which processing operations personal data that are subject to preliminary verification - operations to process special categories of personal data, as well as genetic and biometric data and data that allow you to determine the geographic location of persons, including for scientific research; operations to process personal data using electronic means designed to evaluate certain personal aspects, such as professional competence, reliability, behavior, etc. operations on the processing of personal data by electronic means in accounting systems designed to make certain private automated decisions in connection with the analysis of creditworthiness, financial and economic situation, acts that may result in disciplinary, criminal or criminal liability of individuals, etc.)

Permission for the processing of personal data within seven days after the completion of the preliminary audit, the Center decides on the issue of permission or refusal to issue permissions for operations specified in paragraph (2) of Article 24. Verification of the legality of the processing of personal data, (Verification of the legality of the processing of personal data (hereinafter - verification) is carried out to comply with the controller and processor with the requirements and conditions provided for by this law). Procedure filing complaints and their consideration by the Center (this procedure is enshrined in Section 27 of the Law and indicates that the subject of personal data, believing that the processing of his personals does not comply with the requirements of this law, in the 30-day at a reasonable time from the moment of detection of a violation, it can file a complaint with the Center). Register for the filing of personal data controllers, with a specific purpose of accounting for the processing of personal data, the Center creates and maintains a register for the registration of personal data controllers, which should contain the information specified in paragraph (2) of Article 23. If any changes regarding this information shall be notified to the Center within five days, which shall make appropriate entries in the register of personal data controllers.

Chapter 4 of the law of 2007 and chapter 6 of the law of 2012 are devoted to the Confidentiality and security of the processing of personal data. They practically do not differ, however, the new law includes provisions regarding non-disclosure of professional secrets, so the management of the Center and its employees are obliged to ensure non-disclosure of professional secrets regarding confidential information to which they have access, even after completion of labor activity. This introduction is considered to be a very important aspect since professional secrecy, in this case, acts as an independent object of the law, and the institution of legal protection should be more developed. Despite the fact, that not all the citizens have eIDs at the moment, there is an option of checking which governmental entities have accessed citizens' data. The electronic service "Viewing information on accessing personal data" is provided free of charge to citizens of the Republic of Moldova, holders of electronic identity cards, or another public key certificate.

The service allows the applicant to view the information on the operators who processed personal data and the time of their processing (from the registers held by the IP "Public Services Agency": State Register of Population, State Register of Drivers and State Register of Transport). When providing the service, the provisions of the legislation of the Republic of Moldova are observed, which specify that any subject of personal data has the right to obtain from the operator, upon request, without delay and free of charge:

- confirmation that personal data are or are not accessed by the controller (authority);
- the authorities that accessed the data;
- date of accessing the data.

As a subject of personal data, every citizen has the right to address directly to the authority that processed the data to exercise the right of access, opposition, and intervention, in the order provided by art. 13, 14, and 16 of the Law of the Republic Moldova on the protection of personal data[14].

The information displayed does not contain data (actions) on the processing of personal data, carried out in the context of actions to prevent and investigate crimes, enforcement of convictions, and other actions in criminal or misdemeanor proceedings, for national defense, state security and maintaining public order.

For additional information, citizens can address a written request to the Public Institution "Public Services Agency". The results of the security audit in the personal data information systems are presented for the last two years.[15] The deadlines for storing audit data on accessing information resources through automated information systems are established for 2 years according to the Decision of the Government of the Republic of Moldova no. 112/2010 on approving the Requirements for ensuring the security of personal data when processing them in personal data.

[14] Law on personal Data Protection of the Republic of Moldova. https://www.legis.md/cautare/getResults?doc_id=121238&lang=ro (Accessed on 24.04.2020)

[15] Public Service Agency of the Republic of Moldova. Viewing information on accessing personal data. http://www.e-services.md/?q=ro/content/vizualizeaza-informatia-privind-accesarea-datelor-cu-caracter-personal (Accessed on 20.04.2020)

5.3 Interview outcomes. Promotion of e-Governance Services

When analyzing all the interviews, a pattern was disclosed. All of the experts in the field of e-Governance services and Data Protection have mentioned, those e-Services are not promoted enough in the Republic of Moldova. It is a well-known and proven fact, that e-Governance services cause an immense increase in transparency. In the case of the Republic of Moldova, the government is afraid of transparency. As the former Ministry of Foreign Affairs of Moldova Senior Legal Adviser stated:

"...many Ministries were deprived of the opportunity to set tariffs themselves or came up with various certificates, they issue these certificates only for themselves in the framework of their organization. Imagine, I need to access a service, coming to a Ministry and I am told to bring a certain paper. Where from? From the same department, in the same Ministry. It was a war with let's say, hidden corruption, money sharing. This system is disappearing. Some Ministries reserved the right, exclusive right, of access to information. There is no centralized service to obtain information on citizens, for example, to obtain a criminal record. You need to contact a specific organization and just recently that organization stopped taking money for this service. Now it has stopped because they do not do the work, they just maintain the base, that is, put information there".

We can see, that introduction of the e-Governance services is undoubtedly useful for the country in general, firstly, for the citizens, secondly for the fulfilments of the commitments, undertaken in the relation with the Moldova-European Union Association agreement in 2014 and thirdly, to combat the latent corruption, that is still present in some of the governmental institutions. The fact of not having a centralized system of data storage and exchange was confirmed with interviewee number 3. There is an existing data interoperability system in Moldova, MConnect, created in 2014, but as demonstrated in practical examples it is not effective, as it claims to be. MConnect is the technical and informational foundation of every other online governmental service. At the moment, 28 governmental entities are fully connected and using MConnect in their day-to-day activities for the data exchange[16]. It is stated, that any of the governmental entities can be allowed to connect to the main interoperability system, just by following next rules: a) The applicant must describe in as much detail as possible the context in which the data is to be consumed, but also the actual data sets that will be subject to interoperability through MConnect. b) Refer to the regulatory framework of the information system that will consume the requested data (the act by which it was established, created the information system, the technical concept of the system, the rules of operation of the system). c)In the chapter on legal arguments, exact references to the provisions of

[16] MConnect Moldova. https://mconnect.gov.md/#/ (Accessed on 2.04.2020)

legislative and normative acts are required, which enable the institution to consume the requested data. d) If the data to be exchanged is personal data, then this initiative must be notified to the National Center for Personal Data Protection, the applicant must be registered in the Register of personal data operators.[17]

Another technologic platform, that is novel too much of the countries, but actively used in Moldova is MCloud. Several organizations use common applications that are housed in a single data center using cloud technology. The officials just need to connect the internet wire to access them, no servers, and necessary storage space. Public officials are required to log in using a Cloud service, customizes the account, and operate with data. Institutions can benefit from a range of Cloud applications, including custom ones. To streamline spending on IT services, the government has introduced a popular technology platform, known as MCloud. This platform aims at promoting government spending and strengthening data centers in a shared management process. Thus, costs are reduced considerably, officials' work is more productive and, eventually, better public services are provided.

MSign is a governmental service, that provides an opportunity to apply any type of electronic signatures and verify the originality and authenticity of another digital signature. That could be done on the MSign official website[18], after choosing the "Sign" option and uploading the document, the user has 3 ways of signing the document: Mobile Signature, Digital Signature (via MoldSign Server) and National eID (See annex #).

Governmental online payment service launched in 2013 – MPay, an information tool with which various online services can be paid. Although MPay is primarily aimed at public sector electronic services, it can also be used for commercial services. MPay makes it possible to pay for services through several payment methods such as bank cards, payment terminals, e-banking systems, and cash payments. In the case of cash payments, citizens who do not have access to the Internet can go to the counters of connected banks or the Post Offices of Moldova. The beneficiaries of the MPay service are, first and foremost citizens, those who pay for public services, but also the representatives of the business environment, who in their commercial activity need to receive payments for the services provided, but also to pay for the services consumed. Cardholders can make electronic payments for the payment of public services.

Promoting the services, that lack user-centric design will not bring any specific results, especially, when the alternative of old-school services is still present. Citizens and businesses can be motivated to be the partakers of the e-Governance services benefits, via receiving cost and time-

[17] Ibid.

[18] MSign online service. https://msign.gov.md/#/ (Accessed on 15.04.2020)

efficient services. Even, while the paper-based documents could be issued old-school way, the online services have to be provided 10 times faster and 10 times cheaper. More than half of the population of the Republic of Moldova is not aware of the e-services, and as with the use of the computer and the Internet, the young age, the urban environment, the higher education level, as well as the high-income level are the characteristics associated with a higher rate of access to public services through the Internet. According to the interviewee from the e-Governance Agency of Moldova:

"Our citizens do not know about the existing electronic services and besides, they do not know how to use these services. And who should be responsible for promoting these services? Perhaps the responsibility should be on those who launched these services. Unfortunately, our mentality assumes that someone created this project, invested money in it, launched it, and does not care about the rest. But implementation should not be the last action point, but the initial. And here we get a big problem because marketing does not want to work. From this point of view, Estonia is a good example for us. We have long been negotiating with colleagues from the Estonian Academy of e-Government, in which we discussed prospects and said that technologically Moldova is ahead of Estonia. But what we cannot catch up with Estonia is the question of how to promote services so that people would like to eat this sweetie in the form of electronic services."

Compared to 2016, the number of citizens, accessing public services online has increased only with 4.5%, up until 15.4% in 2019. The most visible benefit for 42.3% of the population, as a result of the Government Services Modernization Reform, is to reduce the number of visits to public institutions needed to benefit from a service. Each third respondent believes that the implementation of the Reformation will eliminate corruption at the level of service provision. A quarter of the interviewees mentioned the reduction of costs and the duration of service provision(e-Governance Agency of the Republic of Moldova, 2020).

Before changes, that were described previously, all governmental authorities must be using only electronic means of communication and data exchange; all civil servants must be aware of the services and know using those. The fact, that one wheel in the big system can stop its harmonious work and development. As stated by 2 interviewees one minister, just by having a very strong will of not using the state's e-Services can stop the whole Ministry from using them.

A very interesting aspect is the technical audit of the data processors, individual or legal entity of public or private law, including a public authority and its territorial units, which, on behalf of or in the interests of the controller, processes personal data at its direction. Here is the experience of the e-Governance Agency of Moldova Representative:

"We do not have the right to observe this. We manage a data exchange platform. So, when the organization is connected to this platform, we see that the analysis is being done. And the

organization provides certain information, that is, what kind of data they need access to. When they are asked what data they need access to, another question arises, what is the organization's motive for accessing this data. Is there, for example, a Government Decision, or is there another need. And of course, an in-depth analysis is carried out, arguments are given whether an organization needs this data. The process of integrating an institution or an information system of a given organization does not occur through the MConnect platform. Further, the organization's employees do not have direct access to the MConnect platform, they have access to a system implemented through the MConnect platform. Employees have access exclusively to the data requested by this organization. And in no case do they have access to all other data. There is another MLog system that registers and processes all data requests at the level of each organization individually. When we have an MCabinet (personal account) in which every citizen can track what his data has been requested. For what purpose, when, who requested the data - all this will be displayed. We do not have the right to prohibit access to data when documented for what purpose the data is needed. Certain contracts or decisions that allow the processing of the data."

Some of the public authorities are refusing to get accustomed to the progressive ways of e-Governance. There is a practical instance, the National Centre for Personal Data Protection of Moldova refuses to accept any documents, with digital signatures. While some of the public and private agencies are trying to keep pace with the current progress, it is still needed for them to go back to the old ways and tools. Referring to what former ambassador of Moldova to Estonia stated:

"If I am writing to them a letter with a digital signature and they are not responding to me, the Agency is violating my rights. We should look at the situation from this perspective, but not from the perspective of their plans; it is not about are they willing to accept such documents, or no, they are obliged to. Let us keep to this perspective".

Regarding the legislation on Data Protection in the Republic of Moldova, even compared to the EU's GDPR, Moldova still has a very strong legislative foundation, in some areas it is even stricter. As the previous interviewee said:

"In some specific cases, under the idea of personal data protection a lot of data is not being disclosed, but de facto it should be public; it is the matter of the interpretation of the law."

So, simple citizens not always get the importance of their personal data and what it can mean for unauthorized access to it. They see themselves insignificant in a global picture, but people with some bigger so-called "power" such as business owners, politicians are overprotective of their data and do everything possible not to disclose their connections to some other businesses, their incomes, and their possessions. As the interviewee contributed to this matter:

"Once politicians understand, that e-Governance solutions are diminishing their ways of influencing, they start to oppose it. "

To combat that increased volumes of power in the hands of politicians and take away their monopoly rights to opposing e-Governance development, was created the National Centre for Personal Data Protection of the Republic of Moldova.

5.4 The role of the National Centre for Personal Data Protection of Moldova

The legal framework of data protection in the Republic of Moldova is undoubtedly solid, because it inherited its foundation from the European GDPR but started developing years before, which is confirmed by the former Deputy Chief of the Directorate-General for Supervision and Compliance at the National Centre of Personal Data Protection: "The Republic of Moldova, signed the European Convention No. 108 back in 1998 if I am not mistaken, but only started to apply this Convention in 2008 when the National Center for the Protection of Personal Data was created and the first Law No. 17 was adopted in 2007 on the protection of personal data. Since 2008, they began to directly apply this law in practice. And the biggest emphasis and the greatest attention was paid specifically to public services, the public sector. That is, at first the Center began to adapt this processing of personal data precisely in public services so that public services were an example for the private sector."

The majority of citizens do not tend to show a profound understanding of their personal data, based on the results of the survey (described in a detailed way in the next paragraph), opinions if the experts, statistics provided by the NCPDP (See annex 13). The first action point that can be taken, to combat unnecessary personal data access by unauthorized users, is to raise awareness and eliminate the knowledge gap regarding personal data protection rights. Regarding the unnecessary personal data access by unauthorized users, the former Deputy Chief of the Directorate-General for Supervision and Compliance at the National Centre of Personal Data Protection mentioned:

"The most common violations are the collection of personal data unnecessarily. There are simply a lot of public services when an employee thinks that he takes an important position and he is allowed to. He can go in, check his relative, neighbor, and any other. There have even been cases when money was paid for it. For the prosecutor to check on a person and to sell these documents, which he took from the register to his relative, who, in turn, will sue this person. The data is worth it. At the moment, personal data has the highest cost that can be. And in most cases, these government officials use their authority to check, issue information, make a fake document, change some data in the register."

Regarding the citizens' knowledge gap, the NCPDP started taking action in 2019. Multiple events were organized in different cities, for different age groups with the main goal of raising awareness

in this area and not only for citizens but also for civil servants. During 2019, were published 129 press releases, article,s and announcements on the official page of the Center (NCPDP, 2019).
Another hindrance, that stops center from the active development and alignment of all the decision-making processes in the lack of staff. Based on the analysis of the recent court decisions taken by the NCPDP, inconsistencies can be found in decisions, taken in very similar cases. While analyzing the official website of the center www.datepersonale.md, we can see, that the names and the contacts of the employees are not published there. The inconsistency in taken decisions can be one of the main reasons for that. But still, if we will go on some social media platforms like Facebook or LinkedIn, some of those employees will mention their workplace on their pages. All of the e-Governance processes are mainly partially automated now in the Republic of Moldova. Most of the services still require the intervention of multiple actors to perform in till the end and lacks efficient ways of monitoring who is having access to the data and what changes are being performed. That creates some gaps and new places for corruption. One of the example cases described by the interviewee:

"For example, the same cases when only one letter was changed in the Criminological Register, where all criminal cases are kept, a lot of money can be paid to change one letter, and if one letter is changed, this person is no longer listed. Later, in case an official check will be made and enter some last name, for example, remove the last letter U from the name of Chobanu, then the information will not show that he has any offenses. Additionally, public services do not have the means to apply the principles to the protection of personal data in practice, because, for example, the same programs, applications that are being developed, they do not always apply these principles immediately. In Moldova, they often work based on old programs, old ones 15-20 years ago there was nothing to protect personal data".

One of the most recent cases of the incorrect handling of the citizen's data happened during the COVID-19 outbreak in the Republic of Moldova, on the 9th of March 2020, the President, Igor Dodon, during the press-conference disclosed some personal data about the citizen, that brought the first case of coronavirus in the country[19]. The legislation regarding the protection of personal data concerning the patient concerned has been violated because public authorities of different levels have revealed in several public speeches a series of unique identifiers of the targeted natural person such as first name, last name, age, sex, double citizenship, name of the hospital and the locality from abroad where the patient was addressed, airline and the date the person took a flight, the specific medical conditions: diabetes mellitus, grade 2 overweight, and hypertension but also bilateral bronchopneumonia; the name of the hospital in which she was admitted to the Republic

[19] News Maker Moldova, news portal. https://newsmaker.md/rus/novosti/dodon-nazval-imya-zhenschiny-zarazhennoy-koronavirusom-imel-li-on-na-eto-pravo/ (Accessed on 20.04.2020)

of Moldova. With the identifiers spoken in public, according to the data from the State Register of Population, there are 162 persons with similar information, previously it was stated by multiple news portals that the number of such persons is approximately 500 (Ibid.). Therefore, namely the addition of the person's name and surname led to the identification of the natural person and the violation of the right to the protection of personal data and the right to the confidentiality of medical data. The civil society was expecting the reactions and some penalties towards the President for such actions, but there was no follow up reaction from the NCPDP. This type of behavior ignores the Article 16(2) of the Constitution of the Republic of Moldova: All citizens of the Republic of Moldova are equal before the law and the authorities, regardless of race, nationality, ethnic origin, language, religion, sex, views, political affiliation, property status or social origin.

A different organization, that is also responsible for the information security in Moldova is the security and Intelligence service of the Republic of Moldova (SIS). The main focus of the organization is: "Efficient protection of fundamental rights and freedoms of citizens, society and state against risks and threats to state security, promotion of democratic values and national interests of the Republic of Moldova"[20]. In some governmental organizations, personal information can be kept in print out versions, in folders, and any of the workers' offices or sometimes visitors would be able to access this information without any hindrance (More details in interview nr 2). This shows a lack of understanding of what data protection is, what the principles are that should guide it, and why it is important.

6 Citizens perception - Case study the Republic of Moldova

In this chapter, the author is presenting the analysis of the citizens' knowledge in the area of the e-Governance services and their rights on Personal Data Protection in the Republic of Moldova. The case of this country is different from many others; usually in democratic societies citizens are the ones requesting changes and improvements, in the online interaction with the governmental authorities, but in Moldova, the government has to be looking for ways to attract citizens' attention towards novel solutions.

[20] Security and Intelligence service of the RM. https://www.sis.md/en/content/mission-vision-and-values (Accessed on 24.04.20

6.1 Citizen’s perception of e-Governance Services development and Personal Data Protection

To complete a thorough analysis and to make a conclusion based on the RQ2, a survey was composed and shared out online, via social media posts, personal messages, e-mail invitations, diaspora groups on Facebook, among the citizens and permanent residents of Moldova. From the 26th of March 2020 till the 4th of April 2020, 293 respondents have shared their opinions and experiences based on 11 multiple choice and one open-ended question. It allowed getting a clearer picture of citizens’ level of trust towards the governmental institutions and government in general, their knowledge regarding rights on personal data protection, and the development of e-Governance services in Moldova. The survey was presented in 3 languages, English, Russian and Romanian to allow both citizens and permanent residents of the Republic of Moldova to share their opinion and make sure, that all of the respondents have a clear understanding of the questions, addressed to them. The survey was anonymous, the respondent’s data was not disclosed, and they have been informed about it before beginning the survey. After, based on the language preference, the respondents have been asked to pick their age group: 148 respondents are 18-25 years old, 77 are in the second age group 25-35, the third age group 35-45 consists of 43 respondents and 25 of survey participants are 45-55+ years old. Youth tends to adapt faster to the current tech-savviness, use the technology and internet more, and knowing the major age group, that participated in the survey helps with its outcomes; same with the field of activity of the respondents.

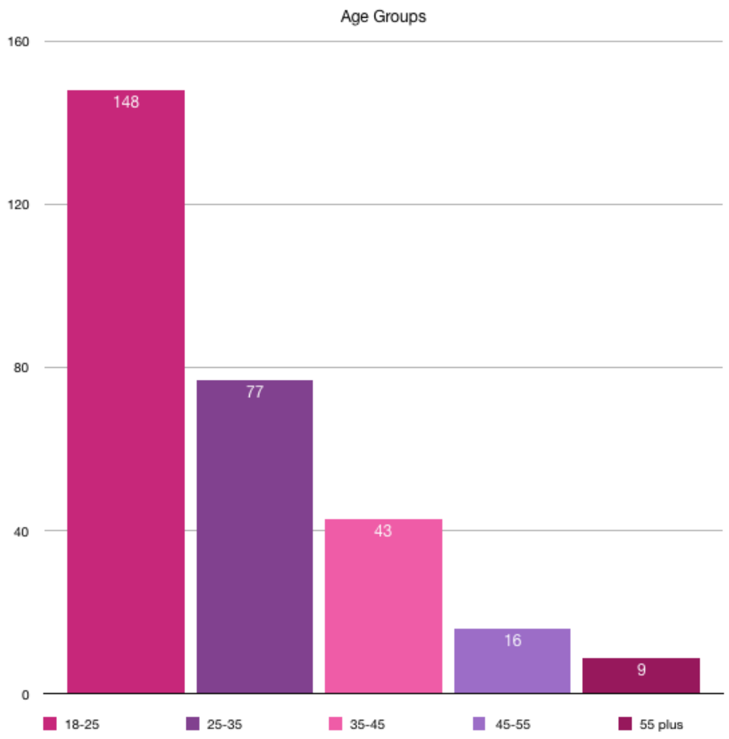


Figure 1. Answers to the survey question number 1.

Based on the field of activity is also possible to conclude which groups tend to adapt to the changes faster, who is better informed regarding the novel services, and who finds them more beneficial.

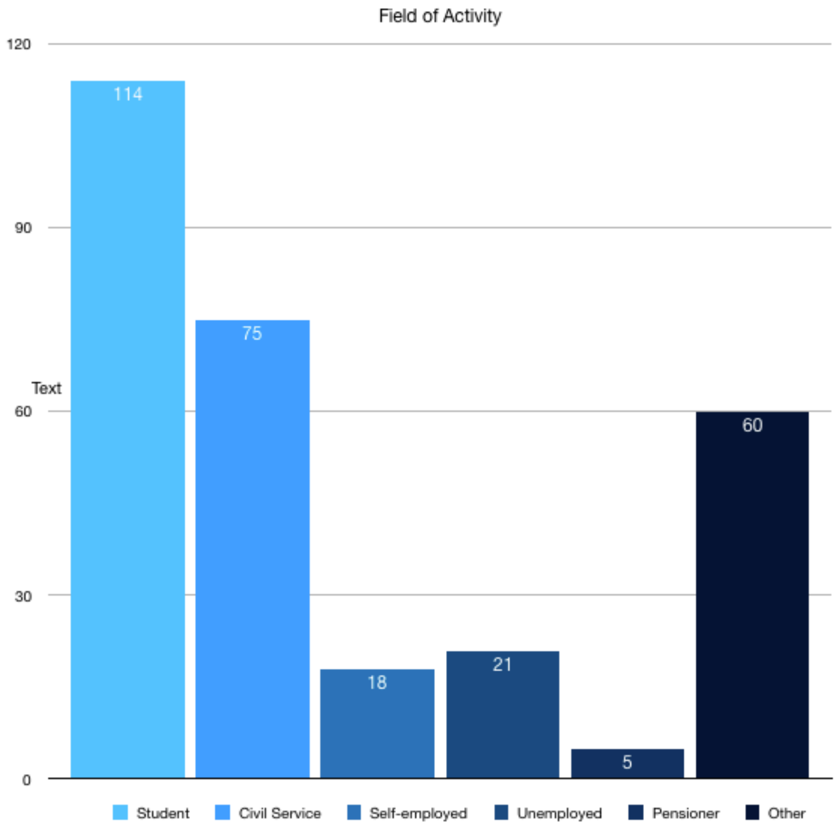


Figure 2. Answers to the survey question number 2.

Firstly, respondents were asked to describe their level of trust towards the governmental institutions. The majority, 152 respondents have partial trust, only towards some of the entities, 15 did not trust them in the past, but regain the trust now. When 104 of responses supported the fact, that there is no trust towards governmental institutions, only 10 respondents trust them completely and 12 respondents found it complicated to find an answer and chose the option “Other”.

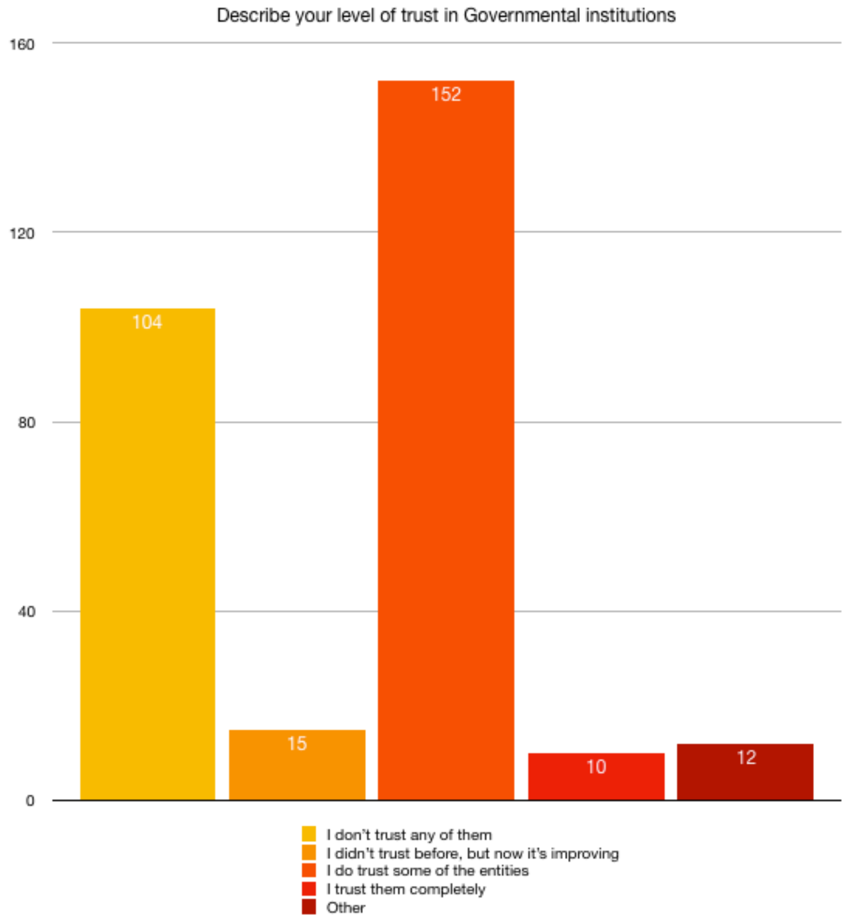


Figure 3. Answers to the survey question number 3.

The next question revealed, that 119 respondents do not know in what format (on paper or electronically), governmental institutions store their data, 12 respondents do not consider the knowledge about that important. 22 respondents state, that their data is kept on paper only, 47 – only in electronic format. And only 93 respondents know that data can be stored in both formats.

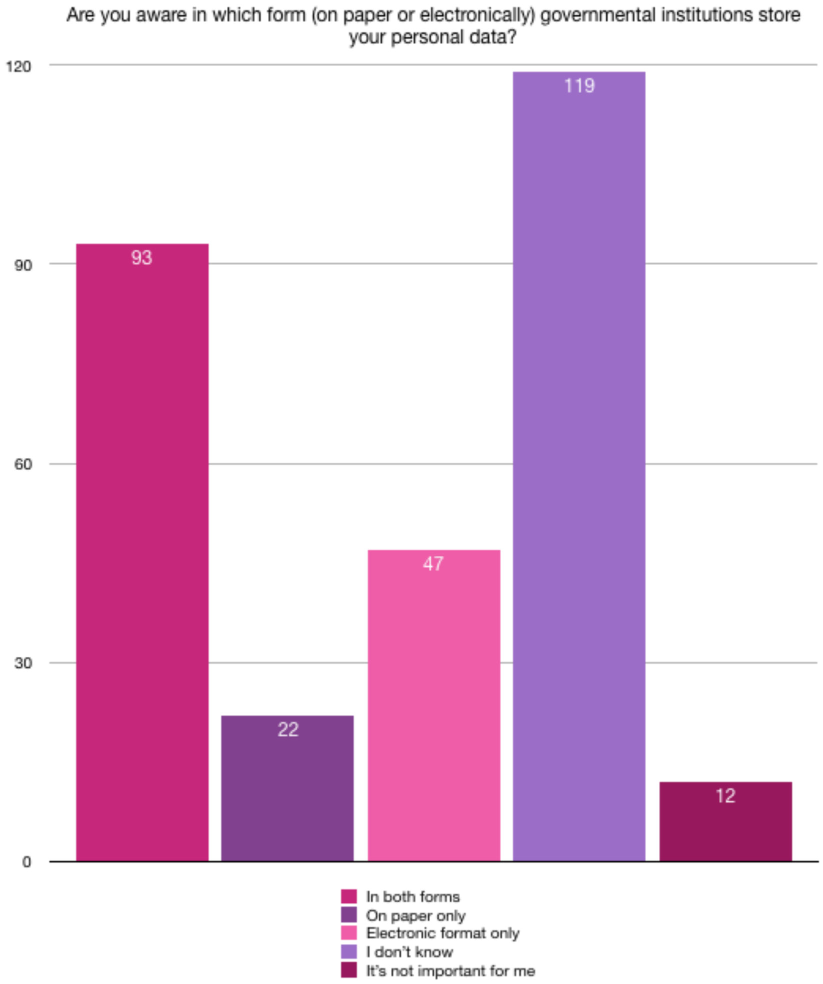


Figure 4. Answers to the survey question number 4.

Regarding the safety of the data stored electronically, or on paper, 103 respondents find electronic data storage safer than on paper, 38 – vice versa. 96 respondents consider both variants safe, 55 – consider none safe and 1 finds it complicated to give a precise answer and goes with the variant "Other".

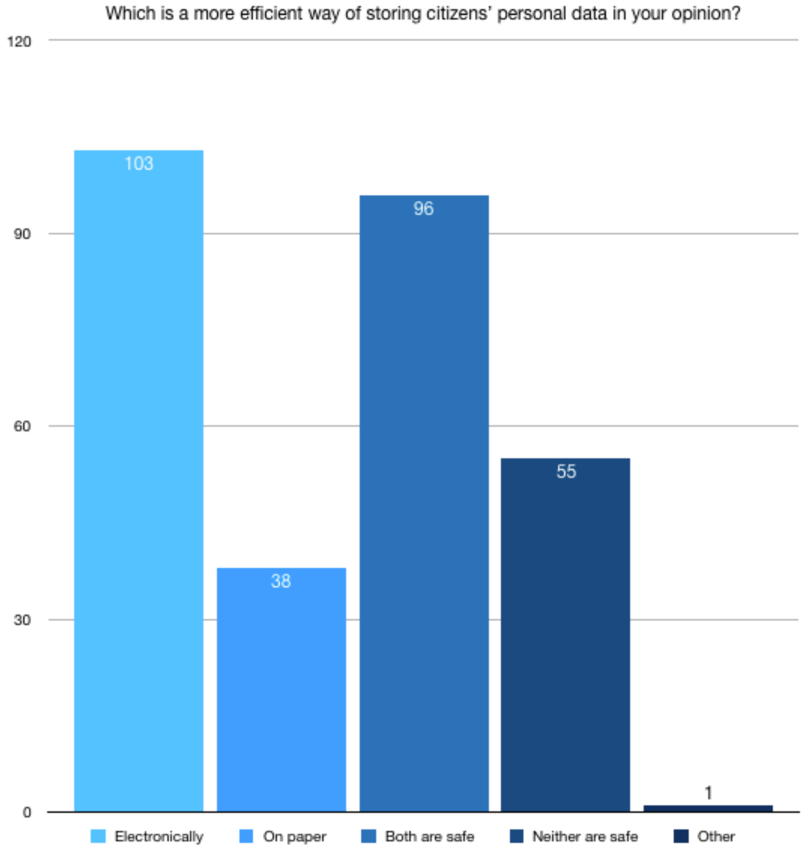


Figure 5. Answers to the survey question number 5.

With the view on the responsibility of public and private institutions with the protection of citizens' data, the majority of the respondents consider, those private organizations are more responsible, 40 say that public. 66 respondents think, that both protect it on the same level, 61 – that both are not serious in that area, 25 respondents don't have an answer on the question.

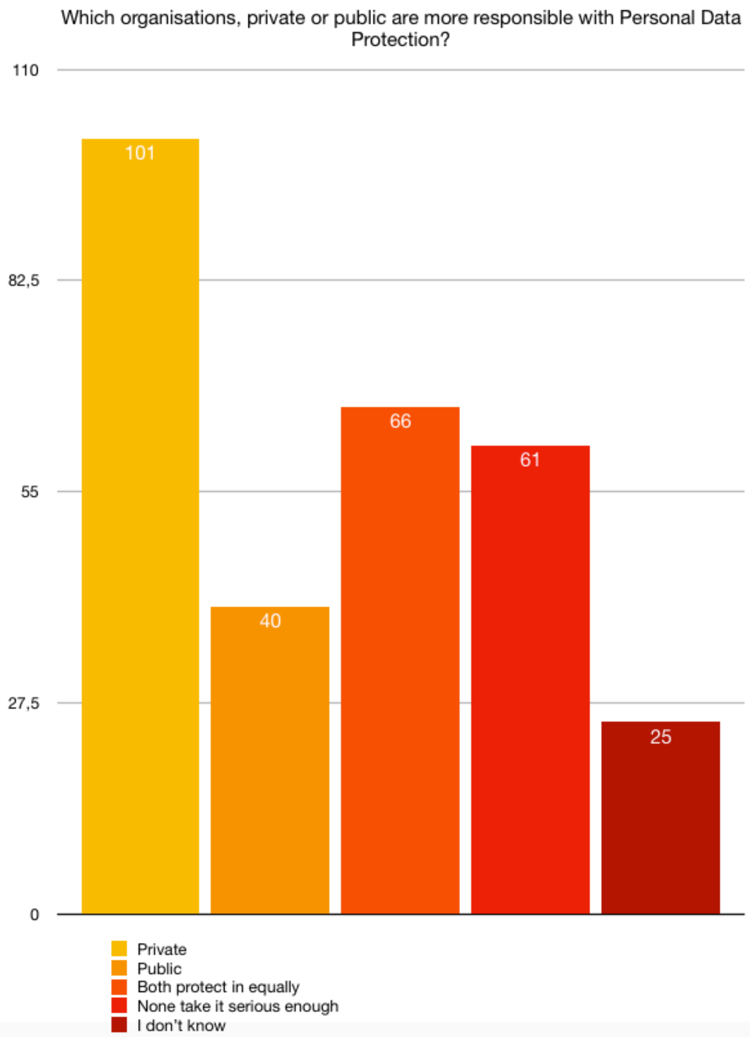


Figure 6. Answers to the survey question number 6.

The next question regarding citizens' is the biggest issue in personal data processed by the government is lack of assurance in the diligent following of data protection regulations – 125 respondents, 85 consider that technical solutions used by governmental organizations are not up to the required security standards. 38 responses are in support of the idea, that governmental organizations can share their data with third parties, 36 do not like the fact, that all civil servants have access to their data and 12 of the respondents found it complicated to respond.

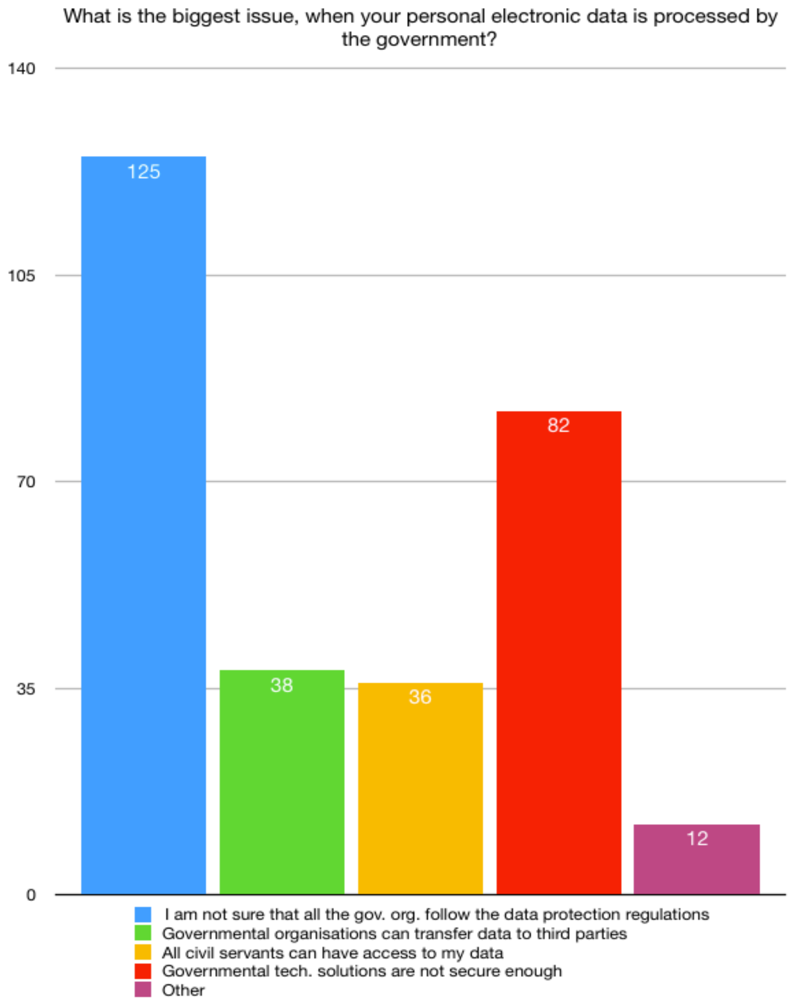


Figure 7. Answers to the survey question number 7.

Still, on the wave of understanding citizens' level of trust towards the government, they were asked to reply, whether they trust in how government utilizes their data. Almost the absolute majority, 146 respondents cannot trust them if they do not have an opportunity to monitor who accesses their data. At the same time, 103 responses tell, that it is possible to trust, but it would be beneficial to monitor who is accessing the data. The last two options have the same number of respondents, 22, some of them trust the government with the utilization of their data without monitoring who is accessing it, and some do not trust in any circumstances.

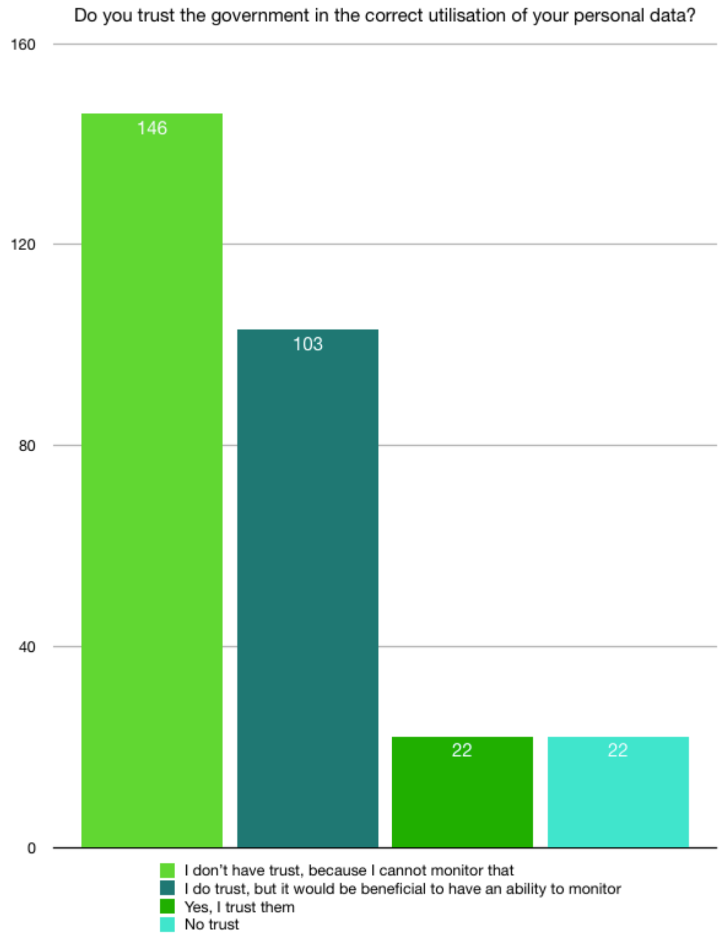


Figure 8. Answers to the survey question number 8.

The next question is in a way connected with the previous one, but it is more direct and precise, regarding citizens' awareness regarding their right to know to whom their data was disclosed, only 2 answer options were given. 171 respondents know about their rights and the rest, 122 never knew about it before this survey.

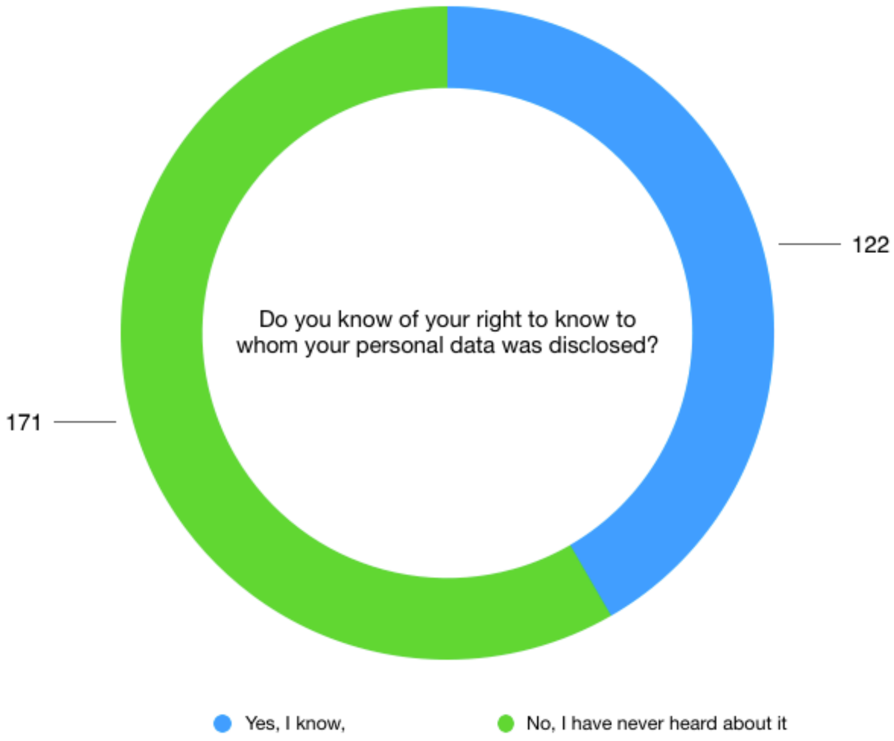


Figure 9. Answers to the survey question number 9

“Have you ever heard of National Centre for Personal Data Protection? Have you used their services?’’. 108 respondents know about the center, but only 17 have used their services before. The number of the respondents, that never knew about the National Centre for Personal Data Protection before the survey, but they might use their services in the future. While 48 of the respondents never heard of the NCPDP and do not think that will ever need their services.

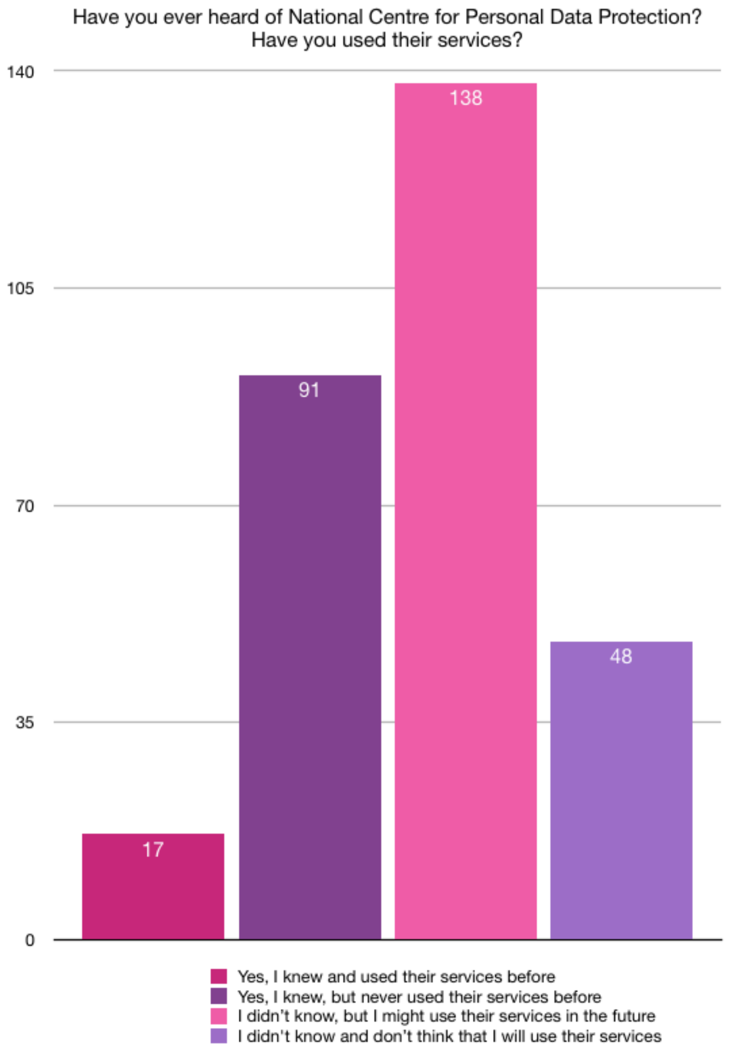


Figure 10. Answers to the survey question number 10.

Second to the last question was regarding citizens' perspective on the transition of the governmental services online and its effect on transparency. In the opinion of 77 respondents, e-Governance systems are not transparent. 98 citizens like this idea and it will help them trust the government. The majority of responses confirm the statement, the implementation of this idea is not useful yet, first of all, the technical literacy of the population has to be taken care of.

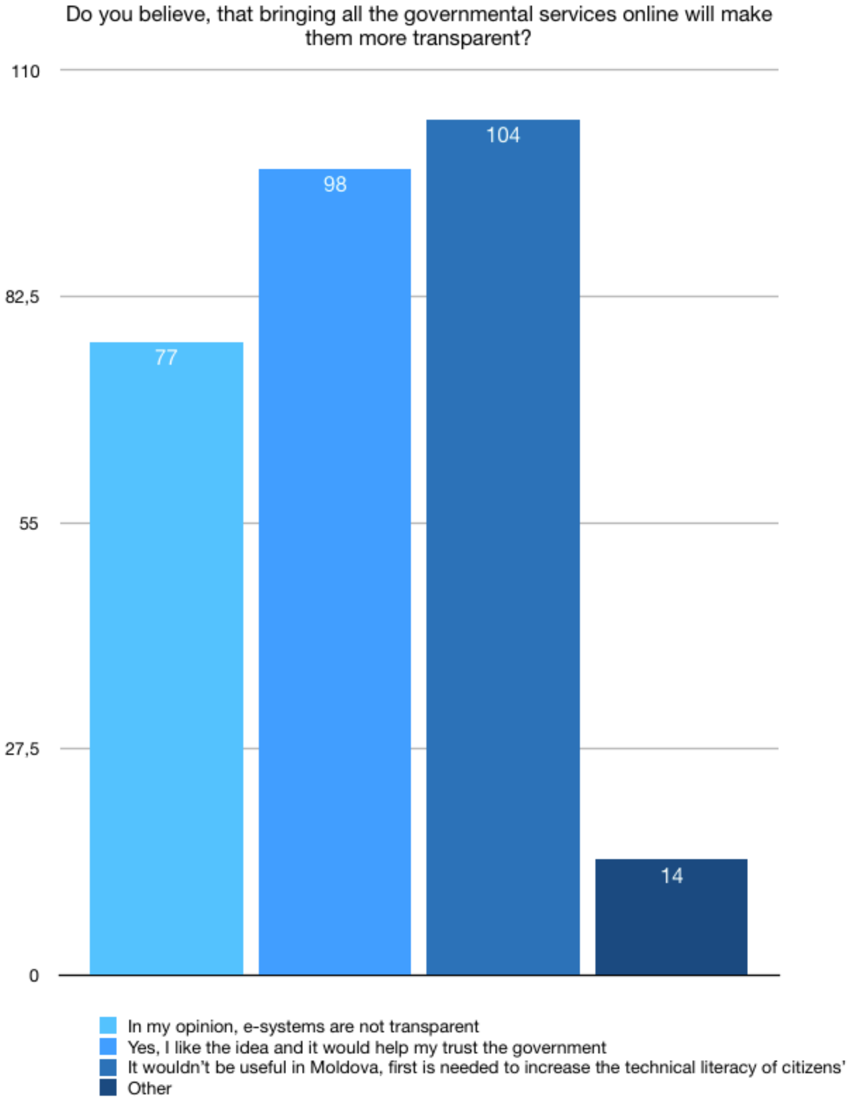


Figure 11. Answers to the survey question number 11.

The last question was open-ended, the respondents were asked to suggest, which governmental services they would prefer to see online. Most of the suggestions included already existing services, like e-Civil Status, online payments for utilities, etc. One of the suggestions stated, that it would be beneficial to bring all of the services online, up to the moment when the final signature has to be attached. That variant could have been a working scenario, but in Moldova, there is a functioning digital signature, which can be procured and has to be renewed once a year. This feedback also signifies that people are not aware of having an option of the digital signature.

The leader of suggestions, which is novel for the Republic of Moldova were medical services, like e-prescriptions, possibility to make doctor appointments online, definitely connected to the COVID-19 outbreak. The government has introduced one novel solution at the very beginning of the state of emergency: citizens could check if their health insurance is still valid, in opposite case they could proceed with the payment online via the MPay service. Another suggestion was about the payment of the monthly public transportation subscription. This suggestion demonstrates, that people become less afraid of the online payments because such fear still exists among the citizens, that can be also confirmed with the suggestions regarding the online banking, coming from the elderly citizens, even though the suggestion is not directly connected to the services, provided by the government.

It was also mentioned, that all the services, connected to the identity verification documents, visas and residence permits, which are presented online only partially, some of the procedures still would have to be done physically, and brought online after.

6.2 Survey context

Based on the precedent theoretical background research, conducted in chapters (…) to get the factual proof and foundation for the conclusions of this research, the outcomes of this survey are backed up with the National Survey, conducted by the e-Governance Agency of the Republic of Moldova (e-Governance Agency of the Republic of Moldova, 2020)

The survey reveals the citizens' level of trust towards the government at the present moment, based on the questions number 3, 6, 7, and 8. The response to those questions demonstrates to us a clear picture of a big trust gap between citizens and governmental institutions; people would prefer private organizations to the public in personal data protection. In the case, the government would provide citizens with a solution to monitor who is access their data and then, they would find it easier to establish trustworthy bilateral relations. Referring to question number 8, we can see, that lack of trust also comes from the lack of transparency. Citizens do not know what measures the government takes to protect their electronic data and there is no access by everyone information, that government is sharing, which technical solutions are used, without provoking any future threats regarding cybersecurity. It might seem hopeless to establish that trust, that a democratic government should require based on question number 3 we can see, that the absolute majority of the citizens still have doubts about some of the governmental entities, possibly based on their previous experiences. Establishment of a trustworthy government-citizen relationship is crucial in the democratic society and the improvement and promotion of online governmental services would be very efficient in this specific area.

Regarding the citizens' awareness of their rights for controlling the personal data and how the government treats and stores their data, we can find answers, backed up with statistics in questions number 4, 9, and 10. Only 41.7% of the respondents know about their right control to whom is disclosed their data, while 58.3% have never heard about it. Regarding people's comprehension of the data storage methods, 40.6% do not know in what format their data is stored, which signifies, that there is a lack of mass communication from the government with the citizens. This type of information can be spread via various channels, such as TV, social media, lectures at schools, universities, public and private offices.

Concerning the National Centre for Personal Data Protection, average citizens know very little about it. 63.4% know nothing about the existence of this center, but the majority of them see the possibility of adding towards their services. The minority of the respondents found it necessary to use their services in the past and 31% is simply aware of the Centre’s functions. The last number can be and must be increased, by applying the same measures as in the case with the citizens’ rights on personal data protection and control.

For the fullness of the survey, it was highly necessary to be aware of the citizens’ enlightenment of existing e-Governance services and people’s readiness to move fully to receiving services online. 35.4% of the respondents agree with the fact, that some citizens still lack even basic technical literacy and it is understandable, in 2019 only 64.7% have a computer/laptop in their house, and half of these people do not have enough resources to procure one. But the situation with the internet coverage is pretty impressive, 93.4% have internet access at home and 74.7% have it on their smartphones (e-Governance Agency of the Republic of Moldova, 2020).

The very last question of the survey was open-ended, respondents were asked to share their opinion on which governmental services it would be useful to have online. While some suggestions were very progressive: i-Voting, e-Tax, e-School/University, e-Prescriptions and many other, signifies, that part of the population is interested in the experiences of other countries in this sector and they are supporting the idea of the system’s upgrade.

The second part of the answers is suggesting the services, that already have become e-Services in the Republic of Moldova, such as online payments for utilities and internet, eID, criminal record, e-Visa, and many other (Figure 12). That confirms, that all existing e-Government services are underpromoted among all the citizens' age groups. Also, there are several opinions, that the existing e-Services are not user-friendly. Services significantly lack the user-centric design. Another point is accessing e-Governmental services while being abroad. As it was also covered in the first interview, with the former ambassador of the Republic of Moldova to the Kingdom of Netherlands, it is very challenging for citizens, who are being abroad on a long-term basis to access any of the e-Services in case of need or urgency. There are 4 possible authentication methods, that are represented under MPass service, which was introduced on the 1st of March 2019[21]. To have access to it, citizens can use:

- Mobile Signature

[21] https://mpass.gov.md/login?lang=en

- Electronic Signature (via MoldSign Server)
- Electronic Identity card
- 2-Step Authentication

All of these authentication steps require prior preparation step from the end-user side, which are impossible to perform while being abroad, as also covered in the interview number one. Based on the feedback of the workers of the Public Service Agency of Moldova, electronic identity cards are mainly issued to legal entities.

Despite these difficulties, it was brought to the attention by former ambassador of the Republic of Moldova to the Republic of Estonia, that not every authentication method can give you access to all of the online governmental services (See chapter 5.3).

The survey was limited, by having to be spread only via online channels, due to the quarantine in the Republic of Moldova, starting on the 11th of March till the 15th of May. That made number of older respondents significantly lower, compared to the younger respondents.

7 Summary, Conclusion and Recommendations

Regarding the first question, the Republic of Moldova has a solid foundation: the legal framework of Personal Data Protection and interoperability are designed in agreement with the EU standards, except one component, that must be altered. Law no. 133/2011 on the Protection of Personal Data is based on Directive 95/46 because at the development and implementation stage, in 2011 there was only the Directive when the GDPR was approved in 2016. The Republic of Moldova has to take notice of this fact and enhance the legislation based on the most recent legislation to be able to compete with the standards. Especially, when 2 draft laws were already elaborated that come to transpose the GDPR: the Law on personal data protection and 2. the Law on the National Center for Data Protection. These laws are being examined since November 2018, when the first reading happened and the date for the second reading is not yet announced. It is very important to understand that in the case of personal data matters substance, not the form. It is important to take into consideration, the type of information, the message it conveys and how sensitive is this information. The key is the content, and not the form it possesses.

All the governmental agencies that are responsible for attaining excellent results in these areas.

The imperative result, that has to be obtained will emerge from the work with the citizens. In a democratic society, the majority of the changes have to come from the "foundation" of the government or other words from the people. Citizens have to be requesting the services, that will assist them in establishing a trustworthy and efficient communication with the government. Secondly, electronic data is intangible. However, it is necessary to have a positive use of technology; if a citizen's information was accessed, a footprint must be left behind for traceability and accountability. Taking Estonia as an example, every citizen can check whenever their data are being accessed by any public or governmental authority. At the moment, in Moldova, a very small number of citizens know about this option and have access to it.

The existing services have to be promoted and fully introduced to the citizens. Every governmental authority, that launches a service should be responsible for its promotion and focusing on user-centric design when developing a service. Not every ministry has a full team of professional marketing specialists; that is why one of the authorities has to take charge of this field and organize pieces of training and have advisors, that can help governmental institutions with the marketing strategy. One of the best candidates for taking charge of this area is the e-Governance Agency of Moldova; the expected outcomes are enhanced aesthetics, especially smartphone app utilization; enhanced web content techniques for service providers. Along with the training for marketing purposes, consultations in the areas of service development, design, and deployment are needed to focus on launching user-friendly services with citizen-centric design. The promotion of the M-Cabinet system, where all the citizens can monitor how their data is being used, will trigger the development of other services.

The e-Governance Agency of Moldova has developed an e-learning platform[22] for the civil servants. All governmental institutions should make it mandatory for the whole staff to participate in those training and prepare final tests to verify if civil servants obtained the required for their position knowledge level. Potentially, some brief online courses can be developed that will be in free access for all the citizens, and later on opening an e-Governance Technologies and Services faculty at the Technical University of Moldova.

Constant evaluation of the level of the end user's satisfaction with the quality of the provided services and with their accessibility. Accessibility is a complex issue, which also involves the citizens' access to the computer and the Internet, which is mainly problematic in rural areas. The government should take care, that in every village there must be several computers with an Internet connection, that will be available for use for all the citizens that are living there, plus at least one person in that location should be trained regarding the service usage and access.

The next essential aspect is trust, from citizens to the government, and establishing this confidence is fully state's responsibility. To lay the foundation for the trustworthy bilateral relation, the government has to start with the legal framework; it will not eradicate the "trust issues" ultimately but will contribute to settling the controversy. The next step is to educate people in this field, people cannot trust anything they do not know and comprehend. All age groups should be included

[22] e-Governance e-Learning Platform https://elearning.gov.md/ (Accessed on 20.04.20)

in the learning process: children should be taught from a very young age about safety on the internet and further, the school curriculum can introduce to them the essence of the services in depth. The elderly population must be aware and capable of managing the online services, especially the world society could experience it during the pandemic outbreak when the most vulnerable part of society has to be protected and distanced from the society as much as possible. People need help with getting rid of the fear of technological development; that can be fought with via sharing the basic cybersecurity knowledge, which also includes the security rules on social media platforms.

The Republic of Moldova tends to be a politically unstable country, based on the past 29 years of its independence. The constant change of political vector tends to make the development in all areas slow and the Agendas, that are set become inefficient. A team of specialists has to be invited once a year to evaluate the progress on the KPIs and propose what could have been done more effectively, on which aspects every institution should concentrate until the next evaluation period. The determinant of the effective shift to e-Governance is the formation of a regulatory body accountable for various elements of e-Governance. To prevent confusion and conflicts, the authority of the whole organization must also be laid down in the national legislation. One person should not have held in their hands the power to change the vector of the entire institution.

To make sure that all the citizens and residents of Moldova can get access to all of the presented online governmental services, another authentication method is required. An analog of Estonian Smart-ID or Mobile-ID technology would be beneficial, especially for the citizens, that have relocated abroad, whether temporarily, or on constant bases. A very limited number of people have obtained the eID, the Mobile Signature makes citizens tied up to his mobile number, what is extremely inconvenient, when living abroad, monthly payments for the number maintenance are required. Such a step will increase the state’s collaboration with the banks and boost the development towards a cashless society.

Moreover, on the rise of 5G technology, more private data will likely be released and handled more conveniently, more rapidly and more widely across borders. It is debatable that a more uniform nationwide data security system will help both the data controlling and data processing entities and allow people to be more knowledgeable of their responsibilities and freedoms. It is necessary to improve the level of protection, the field of cybernetics in the Republic of Moldova is not protected. We do not have rules at the government level that would establish clear requirements for those that provide electronic services, for those who receive these services, for example, banks. It is needed to establish certain limits, certain requirements for all actors who must be professional. As for cybernetics, we should develop confidence in it and all aspects of the provision of services related to it.

Overall, the chosen methods for the current study helped to get a constructive analysis of both angles: citizens and the government. Such an approach was needed to get the full picture for the current case study and provide answers to all the Research Questions. For further research would be beneficial to analyze in-depth the level of civil servants’ knowledge in the area of e-Governance and legal framework of Personal Data Protection.

Reference

Anthes, G. (2015). Estonia: A model for e-government. *Communications of the ACM*, *58*(6), 18–20. https://doi.org/10.1145/2754951

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. https://doi.org/10.1080/13600834.2017.1330740

Cenușa, D., Stercul, N. (2019). *Elections 2019 in Moldova : New Challenges and New Opportunities for Ukraine-Moldova-Romania Triangle*.

Daley, M., J. P. & P. Z. (2015). *The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Cross-Border Discovery. Gilead Sciences, Inc. T.*

e-Governance Agency of the Republic of Moldova. (2020). *Perceptii, asimilarea si sustinerea de catre populație a e -Guvernării și Modernizării serviciilor guvernamentale, Sondaj National*.

EU and Republic of Moldova. (2014). The association agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Moldova, of the other part. *Official Journal of the European Union*, *L 260/4*.

Fletcher, V. (2015). *APEC Cross-Border Privacy Rules System Policies, Rules, and Guidelines*. *5*(2013), 21–33.

Freitag, M., & Traunmüller, R. (2009). Spheres of trust: An empirical analysis of the foundations of particularised and generalized trust. *European Journal of Political Research*, *48*(6), 782–803. https://doi.org/10.1111/j.1475-6765.2009.00849.x

Glas, L. R. (2013). European convention on human rights. *Netherlands Quarterly of Human Rights*, *31*(2), 210–216. https://doi.org/10.1192/pb.27.12.463-a

Goldsmith, J., Levinson, D., Harvard, S., Review, L., & May, N. (1890). The Harvard Law Review Association. *Harvard Law Review*, *4*(5), 193–220.

González F., G., & Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law and Security Review*, *29*(5), 531–539. https://doi.org/10.1016/j.clsr.2013.07.008

Green, J. (1999). Qualitative methods. *Journal of Community Eye Health*, *12*(31), 46–47. https://doi.org/10.1177/0010414006296344

Greenleaf, G. (2015). Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority. *Privacy Laws Business International Report*, *January*.

Hans J. S., (2015). Electronic Government. Introduction to the domain. In *E-Government.*

Information, Technology, and Transformation (pp. 3–11). Routledge. https://books.google.ee/books?hl=en&lr=&id=isMqBwAAQBAJ&oi=fnd&pg=PP1&dq=e-governance&ots=aE6PiIEKJi&sig=XkYjwByO-zu_-aWtc8OBsnlGt8g&redir_esc=y#v=onepage&q=e-governance&f=false

Jasserand, C. (2018). Subsequent Use of GDPR Data for a Law Enforcement Purpose: *European Data Protection Law Review*, *4*(2), 152–167. https://doi.org/10.21552/edpl/2018/2/6

Kerikmäe, T. (2014). Regulating technologies in the European Union: Normative realities and trends. In *Regulating Technologies in the European Union: Normative Realities and Trends* (Issue April 2016). https://doi.org/10.1007/978-3-319-08117-5

Koguchi, T. (2020). *Personal Data Protection*. 165–177. https://doi.org/10.1007/978-981-15-1033-5_9

Korolova, A., Kenthapadi, K., Mishra, N., & Ntoulas, A. (2009). Releasing search queries and clicks privately. *WWW'09 - Proceedings of the 18th International World Wide Web Conference*, 171–180. https://doi.org/10.1145/1526709.1526733

Lee, J. (2010). 10-year retrospect on stage models of e-Government: A qualitative meta-synthesis. *Government Information Quarterly*, *27*(3), 220–230. https://doi.org/10.1016/j.giq.2009.12.009

Lee, J. (1999). Using Qualitative Methods in Organizational Research. *Sage Publications,* 11-35 https://books.google.ee/books?hl=en&lr=&id=ipPUy90VHfgC&oi=fnd&pg=PR13&dq=qualitative+methods&ots=o_wAtbnhg1&sig=8GQg0m1bSWSSQhQdAh5YmEmjhn8&redir_esc=y#v=onepage&q=qualitative%20methods&f=false

Lovells, H. (2017). Asia Pacific Data Protection and Cyber Security Guide 2017. *Lexology*. https://www.lexology.com/library/detail.aspx?g=6a557999-2f44-46f4-b3a2-d3c30696f281

Margetts, H., & Naumann, A. (2017). *Government as a platform*.

Mocanu, I. (2017). *The Most Important Political Events of the year 2016 in THE VIEW OF THE REPUBLIC OF MOLDOVA ' S POPULATION*. 124–133.

NCPDP. (2019). *ACTIVITY REPORT FOR THE YEAR 2019.*

Nyman-Metcalf, K., & Repytskyi, T. (2016). *Exporting Good Governance Via e-Governance: Estonian e-Governance Support to Eastern Partnership Countries BT - Political and Legal Perspectives of the EU Eastern Partnership Policy*. *Springer*, 81–100. https://doi.org/10.1007/978-3-319-27383-9_6

Nyman Metcalf, K. (2019). How to build e-governance in a digital society: The case of Estonia. *Revista Catalana de Dret Public*, *2019*(58), 1–12. https://doi.org/10.2436/rcdp.i58.2019.3316

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. https://doi.org/10.1177/0266382116650297

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law and Security Review*, *34*(6), 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rees, C. (2014). Who owns our data? *Computer Law and Security Review*, *30*(1), 75–79. https://doi.org/10.1016/j.clsr.2013.12.004

Riley, C. (2003). *The changing role of the citizen in the e-governance & e-democracy equation*. 1–111. http://www.tanzaniagateway.org/docs/Changing_role_of_the_citizen_in_the_E-governance_E-democracy_equation_2003.pdf

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European Data Protection Directive. *Rand Europe Technical Report*, *January*, 1–82.

Safari, B. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, *47*(3), 6.

Schoeman, F. (1984). *Privacy: Philosophical Dimensions* (pp. 199–213). University of Illinois Press on behalf of the North American Philosophical Publications.

Seipp, D. J. (1978). *The right to privacy in American history* (p. 212). http://pirp.harvard.edu/publications/index.html#1978

Siddaway, A. (2014). *Systematic Literature review*. *Ii*, 1–13.

Sukamolson, S. (2007). Fundamentals of quantitative research Suphat Sukamolson, Ph.D. Language Institute Chulalongkorn University. *Language Institute*, 20. https://doi.org/9781848608641

Universal declaration of human rights, 113 Radical Teacher 54 (1948). https://doi.org/10.5195/rt.2019.591

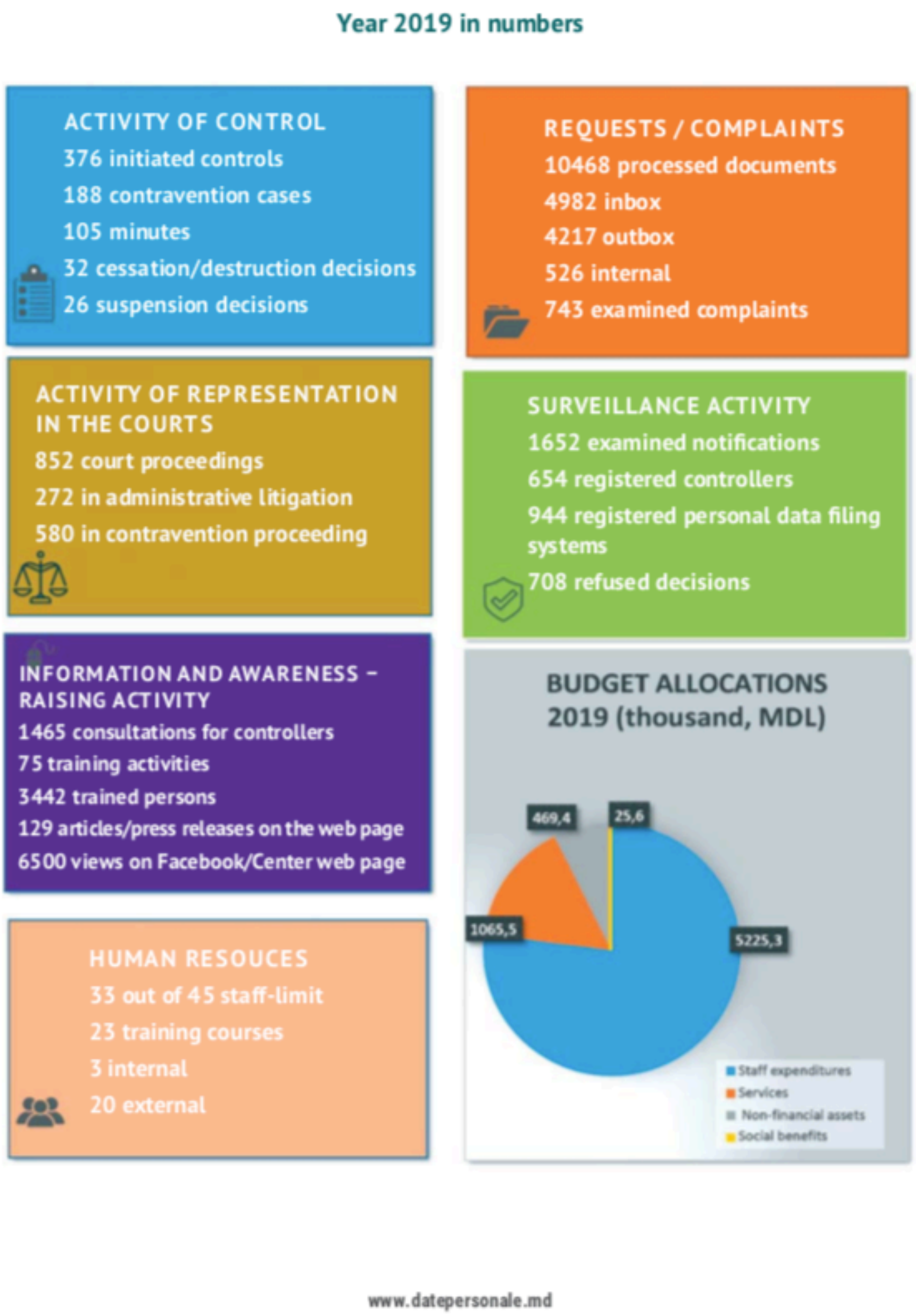
United Nations, (2018). *E-GOVERNMENT SURVEY 2018*.

Vardanyan, E. (2016). The Republic of Moldova – a hostage to geopolitics or "failed state"? *Pathways to Peace and Security*, *2(51)*, 51–70. https://doi.org/10.20542/2307-1494-2016-2-51-70

Warren, S. D., Brandeis, L. D., Review, H. L., & Dec, N. (1890). The Right to Privacy Today. *Harvard Law Review*, *43*(2), 297. https://doi.org/10.2307/1330091

Савельев, А. И. (2018). *Проблемы применения законодательства о персональных данных в эпоху Больших Данных*. https://doi.org/10.32388/022014

Annexes



Year 2019 in numbers

ACTIVITY OF CONTROL

376 initiated controls

188 contravention cases

105 minutes

32 cessation/destruction decisions

26 suspension decisions

REQUESTS / COMPLAINTS

10468 processed documents

4982 inbox

4217 outbox

526 internal

743 examined complaints

ACTIVITY OF REPRESENTATION IN THE COURTS

852 court proceedings

272 in administrative litigation

580 in contravention proceeding

SURVEILLANCE ACTIVITY

1652 examined notifications

654 registered controllers

944 registered personal data filing systems

708 refused decisions

INFORMATION AND AWARENESS – RAISING ACTIVITY

1465 consultations for controllers

75 training activities

3442 trained persons

129 articles/press releases on the web page

6500 views on Facebook/Center web page

HUMAN RESOUCES

33 out of 45 staff-limit

23 training courses

3 internal

20 external

BUDGET ALLOCATIONS 2019 (thousand, MDL)

www.datepersonale.md

Figure 12. NCPDP of the Republic of Moldova, the year 2019 in numbers.

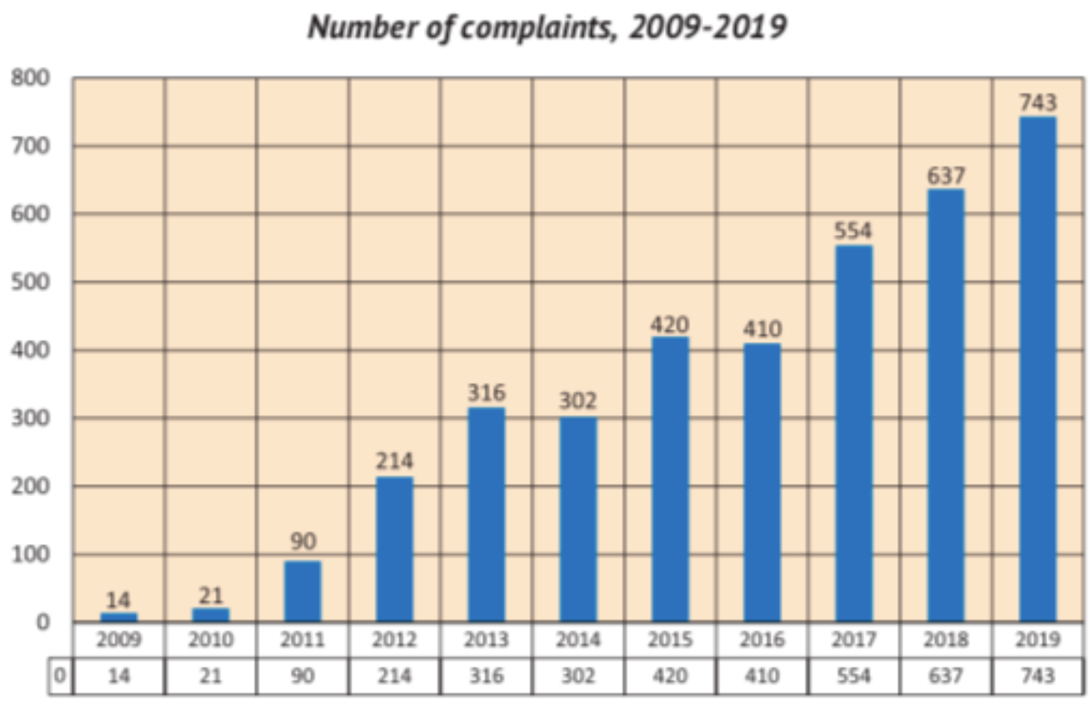


Figure 13. The number of complaints processed by the NCPDP in 2009-2019.

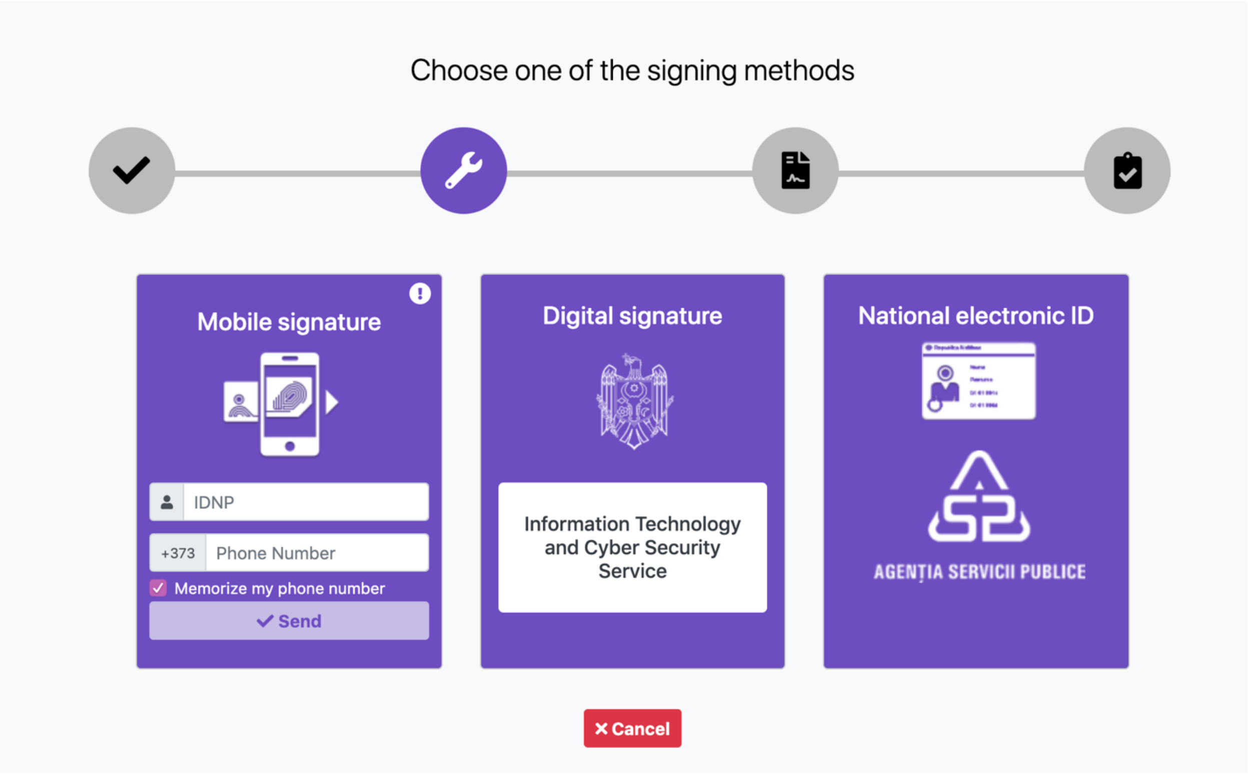
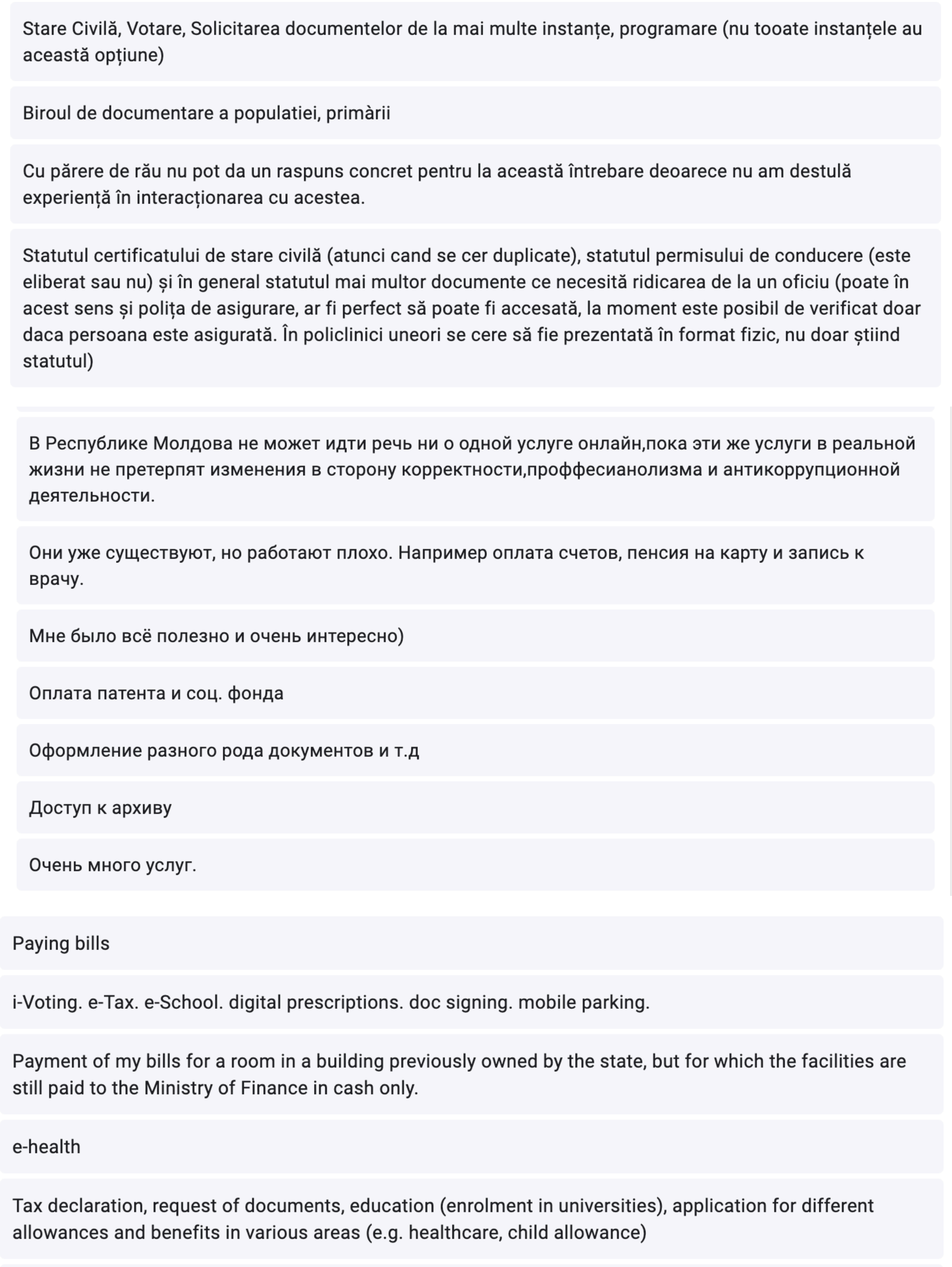


Figure 14. Authentication methods



Stare Civilă, Votare, Solicitarea documentelor de la mai multe instanțe, programare (nu tooate instanțele au această opțiune)

Biroul de documentare a populatiei, primàrii

Cu părere de rău nu pot da un raspuns concret pentru la această întrebare deoarece nu am destulă experiență în interacționarea cu acestea.

Statutul certificatului de stare civilă (atunci cand se cer duplicate), statutul permisului de conducere (este eliberat sau nu) și în general statutul mai multor documente ce necesită ridicarea de la un oficiu (poate în acest sens și polița de asigurare, ar fi perfect să poate fi accesată, la moment este posibil de verificat doar daca persoana este asigurată. În policlinici uneori se cere să fie prezentată în format fizic, nu doar știind statutul)

В Республике Молдова не может идти речь ни о одной услуге онлайн,пока эти же услуги в реальной жизни не претерпят изменения в сторону корректности,проффесианолизма и антикоррупционной деятельности.

Они уже существуют, но работают плохо. Например оплата счетов, пенсия на карту и запись к врачу.

Мне было всё полезно и очень интересно)

Оплата патента и соц. фонда

Оформление разного рода документов и т.д

Доступ к архиву

Очень много услуг.

Paying bills

i-Voting. e-Tax. e-School. digital prescriptions. doc signing. mobile parking.

Payment of my bills for a room in a building previously owned by the state, but for which the facilities are still paid to the Ministry of Finance in cash only.

e-health

Tax declaration, request of documents, education (enrolment in universities), application for different allowances and benefits in various areas (e.g. healthcare, child allowance)

Figure 15. Some of the answers to the survey question number 12: "What governmental e-Services would be useful for you to have online?".

Appendix 1. Interview Questions

The interviews were semi-structured, the rest of the questions varied, depending on the interviewee’s area of expertise. Audio records or transcripts can be provided by request.

1. In your opinion, are all state institutions at the same level concerning the protection of personal data of citizens, regardless of the data format (electronic or on paper)

2. Do organizations have clear lists of people who have access to personal data of citizens and how is it contained?

3. From a technical point of view, how are people who request certain data for a specific person kept records?

4. In your opinion, is the centralized MConnect data exchange system effective?

5. Is it true that for some time ago (and maybe still) the Center for Personal Data Protection did not accept documents with an electronic signature? For what reason?

6. What are the established protocols for exchanging personal information with other institutions, the most commonly used means of communication to fulfill data requests?

7. What are the criteria for assessing the level of data security by the Inspector for the Protection of Personal Data for both paper and digital data storage? Common safety standards?

8. Can you talk about the most problematic issues regarding the electronic processing of personal data in the public sector, from the experience of the Center for the Protection of Personal Data and your current practice? The types of offenses most commonly encountered in practice.

9. Describe the level of civil cooperation with the personal data protection officer. The frequency of citizens' requests to government agencies regarding the type of data stored about them and the institutions/government employees who have access to them. In what format have citizens answered a request?

10. In your opinion, can a wider introduction of electronic public services provide a higher level of citizens' trust in the state? Will this increase the level of understanding by citizens of the importance of protecting personal data?

11. The most effective method of raising public awareness of the importance of protecting personal data. A common standard for the protection of personal data currently in the public sector.

12. The impact of GDPR on the legislation and practice of Moldova.

Appendix 2. List of the Interviews

1. Interview – Former Ambassador of the Republic of Moldova to the Kingdom of the Netherlands – Audio Recording, 25.03.2020
2. Interview – Civil Servant, Ministry of Economy of the Republic of Moldova – Audio Recording, 26.03.2020
3. Interview – Former Ambassador of the Republic of Moldova to the Republic of Estonia – Audio Recording, 3.04.2020
4. Interview – Former Deputy Chief of General Directorate for Surveillance and Compliance at the National Center for Personal Data Protection of the Republic of Moldova – Audio Recording, 11.04.2020
5. Interview – E-Governance Agency of Moldova Representative – Audio Recording, 13.04.2020

Appendix 3. Survey Questions

1. Your Age
2. Field of Activity
3. Describe your level of trust in Governmental institutions?
4. Are you aware of which form (on paper or electronically) governmental institutions store your data?
5. Which is a more efficient way of storing personal data in your opinion?
6. Which organizations, private or public, do you think are more responsible for personal data protection?
7. Do you trust the state government in the correct utilization of your data?
8. What is your opinion is the biggest issue, when your electronic data is been processed by the government?
9. Have you ever heard of National Centre for Personal Data Protection and its functions? Have you ever used their services?
10. Do you know of your rights to request and to know whom your personal information or data was disclosed to?

11. Do you believe that bringing all the governmental services online will make it more transparent? Will it make you trust the government?
12. What governmental e-Services would be useful for you to have online?