TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Tamara Aslanova 194254IVGM

The Role and Importance of Consent Management in Public Organizations in the Digital Age: Case on Estonia

Master's thesis

Supervisor: Dirk Draheim
PhD
Professor

Co-supervisors: Kevin Tammearu

Sidra Azmat Butt

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Tamara Aslanova 194254IVGM

Nõusolekuhalduse Roll ja Tähtsus Avalikes Organisatsioonides Digitaalajastul: Juhtum Eesti Kohta

Magistritöö

Juhendaja: Dirk Draheim
PhD
Professor

Kaasjuhendaja: Kevin Tammearu

Sidra Azmat Butt

Tallinn 2021

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: Tamara Aslanova

09.05.2021

Abstract

The advancement of the e-governance ecosystem, including the data sharing solutions, open new opportunities for personal data reuse. Nevertheless, it also raises citizens' concerns about losing control over the use and processing of personal data. To empower citizens simultaneously with utilizing data reuse possibilities, a consent management tool is considered one of the effective means, which the government of Estonia is currently developing.

The core objective of this thesis is to examine the importance to adhere the informed consent principles and the role of consent management in the public sector in the digital era based on the case of Estonia. In this regard, the notion of "consent" and its principles are examined based on the descriptions in the GDPR and the literature, which are further explored during the semi-structured interviews with experts. The research also aims to provide a comprehensive analysis of the key challenges associated with the implementation of consent management solutions based on the interview outcomes. Overall, the thesis addresses the literature gap by investigating consent and its management in the light of the GDPR and in the public sector.

Keywords: informed consent, consent management, CMP, personal data, data sharing, data protection, GDPR, Estonia.

This thesis is written in English and is 55 pages long, including 8 chapters, and 4 figures.

.

List of abbreviations and terms

API	*Application programming interface*
CMP	*Consent management platform*
ECM	*Electronic Consent Management*
EDPD	*European Data Protection Board*
EIF	*European Interoperability Framework*
EHR	*Electronic health record*
ENISA	*European Union Agency for Cybersecurity*
E-governance	*Electronic governance*
E-government	*Electronic government*
E-service	*Electronic service*
EU	*European Union*
GDPR	*General Data Protection Regulation*
IT	*Information Technology*
OECD	*Organisation for Economic Co-operation and Development*
RIA	*Riigi Infosüsteemi Amet*
RQ	*Research question*
SQ	*Sub-question*

Table of Contents

List of figures

1 Introduction

The rapid advancement of information communication technologies (ICTs) allows processing a large volume of personal data to accomplish public tasks and deliver relevant public electronic services (e-services). The notion of *processing* covers collection, management, storage, retrieval, (re)use, and sharing or transfer of personal information (European Commission, What constitutes data processing?, n.d.). Since personal information usually contains highly sensitive data such as an identification card number, home address, and a medical condition, individuals (hereinafter *data subjects*) are concerned about access to their data or data processing without their awareness and permissions. According to the Special Eurobarometer 487a survey on the Geral Data Protection (GDPR) awareness (European Commission, Special Eurobarometer 487a - The General Data Protection Regulation, 2019), 30% of the 18975 respondents think that they have absolutely no control over the personal data they provide online, and only 14% think they have full control. In Estonia, the majority of the respondents feel partial control, which is also above the European Union (EU) average, and 21% of them feel no control at all over the data provided online. The survey also demonstrates that 78% of the respondents, who feel partial or no control over the personal data, are fairly or very concerned about the situation. Estonia is among the exceptional countries, where only 39% of the particular respondents are totally worried about not holding control over the personal data provided online.

In respect to being informed about the privacy statements and conditions for collecting and using personal data, among the respondents who provide personal information online but feel no control over the data, 58% have never been informed. In Estonia, 30% of the respondents using the internet, regardless of feeling control over personal data or not, are rarely or never aware of the gathering and processing of their data. As the report states, there is a decrease in being notified about the conditions of data collection and use in this country, which is at the same level in Estonia and the EU.

In this regard, public organizations face the challenge of empowering citizens to have control over their information while collecting, transferring, exchanging and reusing their data to provide e-services (Buyle, et al., 2020). Informed consent and consent management are commonly used mechanisms to control the collection, and personal data use in the online environment. Consent is a voluntary agreement or explicit approval of a person, who owns the data, to process his data for the intended purposes of an entity. Additionally, consent is perceived as a means for individuals to make informed decisions (Hoeyer & Hogle, 2014). Informed decisions include rectifying, withdrawing, or objecting to the access to or processing personal data in accordance with individual right to be informed (European Parliament and Council of European Union, Regulation (EU) 2016/679, 2016). Respectively, consent management is comprehended as a procedure and rules based on which a person voluntarily and knowledgeably agrees or denies another party's access to personal health data.

The existing literature explains consent and its management mainly in the healthcare domain, which is highly data-dependent and where data protection measures are "top priorities" (Priisalu & Ottis, 2017, p. 450). Thus, consent management is mostly linked with the patients' medical data and patient-physician relationship in scholarly articles. Besides, since information systems literature do not extensively include consent management issues (Bonnici & Coles-Kemp, Principled Electronic Consent Management. A Preliminary Research Framework, 2010), research on the necessity of consent management during the data exchange and reuse is very limited despite the fact that interoperability and data exchange platforms are applied in public organizations more extensively in the digital age. Overall, the available studies do not adequately examine (1) the role of and the need for consent management in governmental organizations that collect and process a large amount of non-medical personal data for the service delivery daily, and (2) the necessity of consent management to address the issue of having control over the access and processing of personal data, especially when they are exchanged via interoperability platforms.

The recent E-Government Survey (United Nations [UN], 2020) states that public concerns over the collection and use of personal information by public authorities, as well as the lack of an *"opt-out"* option for data extraction, are in increasing trend. Draheim (2020) argues that based on minimality and consent principles, unless it is the master data

(which is critical for the service provision), citizens can grant or withdraw their consent for the storage and processing of personal data via opt-in and opt-out options. The author also adds that the involvement of non-governmental organizations in data processing as a part of the electronic governance (e-governance) ecosystem even further necessitates consent management, which increases the significance of this research.

1.1 Research Objectives and Research Questions

The abovementioned survey and the increasing necessity for consent management require extensive research on the under-explored topic. This study intends to provide a deep comprehension of public organizations' need for consent management in the digital era. The objectives of the thesis are (1) to identify the role, importance, and potential drivers to implement consent management in the public sector in the digital age, (2) to describe barriers that the governments might encounter before or during the implementation of consent management solutions, (3) to contribute to the knowledge on consent management in the context of personal data reuse stored in the public databases.

In this respect, the main research questions (RQ) and sub-questions (SQ) to be addressed in this thesis are indicated below:

RQ1. How can consent management help public sector organizations to adhere to data consent principles in the digital age?

SQ1(1). What are the main informed consent principles?

This SQ aims to identify informed consent principles applicable to the context of this research and are applied to sharing and processing personal data digitally. The question is explored by reviewing existing literature, focusing on the history and the evolution of basic informed consent theory and principles.

SQ1(2). How is consent reflected in the GDPR?

This SQ aims to define the term "consent" in the legal context and understand the importance of consent management from the legal perspective. For this purpose, the review of relevant articles stated in the GDPR is conducted.

RQ2. How important is the implementation of consent management in the public sector?

SQ2(1). What are the key drivers of consent management for governmental organizations?

This SQ is intended to identify the factors that would necessitate the implementation of consent management for public institutions in the digital age through the literature review and expert interviews.

SQ2(2). How urgent is the need to implement consent management in the public sector?

This SQ is intended to explore the urgency of consent and its management for governmental organizations and data subjects in the technology era through expert interviews.

RQ3. How can consent management be practiced in governmental organizations?

SQ3(1). Which technical solutions exist for consent management that are applicable in the public sector?

This SQ is intended to identify the existing technological solutions suitable for the public sector to apply consent management. To find out the answer, the literature has been reviewed, and the available and currently developing consent management solutions in Estonia were identified through interviews.

SQ3(2). What are the observed challenges to implement a consent management system?

This research question is intended to determine the legal, technological, and organizational challenges that hinder practising consent management in public organizations. SQ3(2) have been explored mainly through expert interviews.

1.2 Outline of the Study

This sub-section provides a clear outline of the paper that gives a broad overview of the content.

In the introduction section, background information about the problem, the aim and objectives of this research and the relevant research questions to explore the topic have been described. The following sections address the main research questions and sub-questions. In this regard, the second section provides background information on informed consent and its principles that are applicable to the context of this study and its reflection on the GDPR. The third section discusses related literature on consent management, focusing on its importance and the real-life application. The fourth section explains the applied research design and methodology to collect and analyze the primary data and used validity test methods. The fifth section describes the existing consent management mechanisms and the ongoing pilot project on "Consent service" in Estonia. The sixth section and sub-sections provide the overview of the data gathered through the semi-structured interviews with the experts from the Estonian public and private sector organizations. The seventh section discusses the findings alongside the literature that allows identifying the answers to the research questions, including the sub-questions. Finally, the last section summarizes the research by matching the discussed results with research questions. Besides, it also provides a brief recommendation for further investigation.

1.3 Motivation for the Research

The primary source of the author's motivation for this research is her keen interest in exploring possible ways of using data sharing solutions countrywide and across borders in the light of the Estonian case. In this regard, the topic of consent management is highly relevant since it is a mechanism that allows data sharing for a wide range of purposes. It includes making citizens' lives better, contributing to the development of private companies, and enabling cross-border data flows to accelerate innovation globally by utilizing personal data. Furthermore, considering the core interest, the author aimed to target an under-researched topic, which would have a higher degree of importance for the science. Informed consent and consent management are among the areas that are mostly discussed in the medical context and separate from the personal data sharing among various organizations. Thus, a thorough investigation of this topic, specifically in the information technology (IT) context, is another motivation for this research. Finally, this study includes perspectives about an ongoing pilot project called "Consent service", which is going to be implemented for the first time in Estonia. Therefore, it can be

considered the first research paper that provides insights and analyses on the new Estonian service, which can also be an initial source for further studies on this matter.

2 Background

The first sub-section of this section focuses on the definition of informed consent that is related to the context of this research. It also includes the descriptions of components that make the consent "informed". The second part of the chapter is about the key principles and values of informed consent that consent-seekers need to adhere to. The third part displays how informed consent is reflected in the articles and recitals of the GDPR to provide a legal context related to the notion. Finally, the last section shortly defines the "consent management" term.

2.1 Basic Definition of Informed Consent

Consent has various forms depending on the context, but in this research, *informed consent* will be discussed. Informed consent is about what data, by whom and for what reason is collected and processed to the data subject in simple language (European Parliament and Council of European Union, Regulation (EU) 2016/679, 2016). It consists of several elements, which include *information disclosure, comprehension, voluntariness* (The Belmont Report: Ethical Principles and Guidelines for the Protection of Human, 1979), *competence, and consent* (Faden & Beauchamp, 1986; Friedman, Felten, & Millett, 2000; Heinze, Birkle, Köster, & Bergh, 2011). Friedman, Felten, and Millett (2000) divide the term into two parts: "*informed"*, which means information is disclosed and fully comprehended, and *"consent"*, which is about voluntariness, competence, and agreement. According to the authors, *disclosure* includes the provision of accurate information on potential benefits and risks of an action as well as what data will be gathered and why, who will have an access to the data, time interval of data storage, and the protection of an identity whom the data belongs; *comprehension* refers to the complete and correct understanding of the disclosed information; *voluntariness* is being able to agree or disagree with the execution of an action without encountering external control or coercion, including decision-making under pressure or threat, lacking the choice options, manipulation of the individuals' perception on the information and choices; *competence* is about "possessing mental, emotional and physical capabilities", that are

beyond the technical competence, to make independent decisions and provide informed consent; finally, *agreement* in an online environment refers to accepting or rejecting visible, easily accessible options for collection and processing of personal data, irrespective to the consent being explicit or implicit (unless, the previous criteria are met).

2.2 Principles of Informed Consent

Faden and Beauchamp (1986) argue that the "consent-seeking" concept evolved throughout history and was directed with *beneficence* and *autonomy* models of responsibility of professionals. The beneficence model emerged from the basic medical principle written by Hippocrates – "help, or at least, do no harm" (Faden & Beauchamp, 1986, p. 10) that necessitated the handling personal information of patients in a way that would maximize medical benefits for them and minimize the potential damage and risks. Nevertheless, beneficence solely is not considered a sufficient ground to practice informed consent since "consent" also includes making informed decisions and freedom of choice (Lemmens, 2014), which is about individual autonomy.

In his study, Lemmens (2014) indicates that *autonomy* is one of the frequently referred base value for informed consent. The autonomy model of Faden and Beauchamp (1986) works based on the moral principles of "*self-governance*" and "*respect for autonomy*" – the most common moral principle related to informed consent in the literature. It mainly focuses on privacy, voluntariness and autonomy in decision-making and freedom of choice (Faden & Beauchamp, 1986, p.7-8). The authors consider the model is considered a trigger for "the movement to informed consent" (Faden & Beauchamp, 1986, p. 8) since it includes the practice of (1) *autonomous choice* – having a capacity of being independent and in control via autonomous authorization and (2) *autonomous action* – being able to realize one's autonomous choice (p. 8). However, the most crucial point is "*to be respected as autonomous*" because being autonomous only cannot guarantee to be free to choose without external interferences (Faden & Beauchamp, 1986). To sum up, based on the moral principle of respect for autonomy, informed consent grants an individual to practice his autonomy and keep control over his decisions, holds other parties responsible, and creates an environment where a person can take autonomous action without coercion or interference.

Besides autonomy principle, Faden and Beauchamp (1986) also define *effective consent*, which has three main elements: (1) being policy-oriented "gatekeeper" to oversee the behavior of consent-seekers (the ones that proceed an action), (2) being enforced by laws and institutions to regulate and (3) obliging information *disclosure* as a "necessary condition" for informed consent. Manson and O'Neill (2007) claim that the significance of autonomy cannot be the only principle that necessitates informed consent since it is not applicable in all conditions. Thus, by merging autonomy and effective consent theories, the authors further frame *informed consent* by stating that an individual's autonomous decision-making depends on the "disclosure of adequate, relevant information" (Manson & O'Neill, 2007, p. 27).

Faden & Beauchamp (1986) state that the introduction of *"the legal doctrine of informed consent"* (p. 23) allowed to enforce the abovementioned moral principles as a part of individual rights, specifically, the right to privacy and duty of professionals. The authors also consider the adoption of the legal doctrine a significant attempt for the development of law on informed consent. Later in the beginning 20th century, the requirement of unambiguous, informed consent of people for human experimentation via various regulations was the starting point of the modern consent-related laws and regulations (Cohen, 2010, as cited in Breen, Ouazzane, & Patel, 2020). Followingly, the United Nations Universal Declaration of Human Rights (UDHR) in 1948 and the European Convention on Human Rights (ECHR) in 1950 provided a basic description of consent in relation to the right to privacy and protection of private life (Kosta, 2013, as cited in Breen, Ouazzane, & Patel, 2020). As Breen, Ouazzane, & Patel (2020) mention, all these descriptions contributed to the current understanding of consent for the use of personal data that is defined in the GDPR.

Considering this evolvement, the more relevant approach to consent principles in the digital age has been identified by Draheim (2020). He defines the consent principle as one of the three data protection principles, which are themselves a part of data governance principles. According to the author, consent management is highly related to the *data category* – whether the required data is master data, which is critical for the service provision, or from other categories of data (e.g. aggregated, transactional, or inventory). In this regard, he states that the consent principle applies beyond the master data and necessitates consent being granted or revoked by citizens through "opt-in" and "opt-out" options.

2.3 Consent in the GDPR

The GDPR, a legal source for data and privacy protection in the European Union (EU) and the European Economic Area (EEA) countries, obliges defining a legal basis for data processing. To comprehensively describe "consent" in the light of the GDPR, several associated terms should also be defined. These terms are indicated below:

- *Data subject*. Article 4 (1) of the GDPR defines data subject as "an identified or identifiable natural person" that can be identified with a name, an identification number, location data, an online identifier or other specific characteristics (European Parliament and Council of European Union, Regulation (EU) 2016/679. Article 4. Definitions, 2016). In this regard, *personal data* is data that belongs to the data subject (European Parliament and Council of European Union, Regulation (EU) 2016/679. Article 4. Definitions, 2016).

- *Data controller* (shortly, *controller*). Article 4 (7) explains the term as *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"* (European Parliament and Council of European Union, Regulation (EU) 2016/679. Article 4. Definitions, 2016). It means data controllers are authorities or persons who decide on for what purposes and how personal data are being collected and processed, overall, who carry the legal responsibility to oversee data (Van Ooijen, Ubaldi, & Welby, 2019). The European Parliament and The Council (1995) specifically emphasize the controller's responsibility to safeguard compliance with personal data protection regulation. Based on these definitions, the data controller is the main party that defines accountability over the collected, held, and exchanged data on the ground of the minimality principle (Draheim, 2020). Information Commissioner's Office (ICO) (n.d.) also describes controllers as autonomous decision-makers who provide instructions to *data processors* on data collection and processing.

- *Data processor* (shortly, *processor*). Article 4 (8) of the GDPR defines a *processor* as "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*" (European Parliament and Council of European Union, Regulation (EU) 2016/679. Article 4.

Definitions, 2016). They are also identified as service providers since they handle the data to deliver relevant services (Pöhls, 2008).

The GDPR defines consent as one of the six legal bases for data processing, including collection, use and reuse, storage, and transfer of personal data ("*What are the GDPR consent requirements?"*, n.d.). The legal definition of consent is *"freely given, specific, informed and unambiguous indication of the data subject's wishes*" (European Parliament and Council of European Union, Regulation (EU) 2016/679, 2016). The primary defined purpose of consent in the GDPR is to ensure that data subjects keep control over their data as per individual rights – "*the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and the right not to be subject"* (European Data Protection Supervisor, n.d.). In this regard, the GDPR identifies several conditions for collecting and handling the consent, indicating that the consent must be

- *freely given* (Article 7 (4), Recital 32, 42, and 43), which include a choice to refuse or withdraw consent. It is also indicated that if there is an imbalanced relationship between the controller and data subject (e.g. a public authority and a citizen), consent should not be a valid legal base for data processing;

- *informed* (Article 7 (3), Recital 32 and 42), which means a data subject being aware of the identity of a controller and his purpose of processing the data;

- *unambiguous indication of data subject's agreement* (Recital 32), which can be a written or oral statement provided in a manual or electronic form. In this regard, silence, inactivity, or pre-ticked boxes are not considered as a consent of a data subject;

- *explicit* (Article 9 (2a), Recital 51 and 71)*;*

- *specific for the intended purpose* (Article 7 (2), 9(2a), Recital 32 and 42), which include consent being provided separately for each purpose, when there are multiple of them;

- *demonstrable by the controller* (Article 7 (1) and Recital 42), which include consent being accessible, clear and easily understandable;

- *and revokable or withdrawable* (Article 7 (3) and Recital 42), which must be easy to do at any time (European Parliament and Council of European Union, Regulation (EU) 2016/679, 2016).

2.4 Consent Management

Consent management is any systematic approach to deal with and apply consent principles in an organization. Kakarlapudi and Mahmoud (2021) define the concept as the *"action or process to manage user and customer consent"* for personal data processing through which privacy preferences can be defined by granting or revoking consent. It is comprehended as a set of processes and rules based on which a data subject can grant or deny another party's access to personal data based on consent principles. It should be noted that although the GDPR defines consent and the conditions for consent, it does not identify consent management and its principles in practice in the public sector. The existing literature does not also largely specify the definition of electronic consent management in the digital age.

3 Related Work

This chapter explores the literature on the topic, which includes academic articles, peer-reviewed journals retrieved from reliable databases such as Scopus, Google Scholar, and the university library, and the reports of international organizations, such as the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD), were taken from their official libraries. The search included keywords such as "consent", "informed consent", "consent management", "e-governance", "e-government", "data protection", and "GDPR". The first sections and their subsections define the importance of consent from various aspects. The second section is about the implemented solutions or ongoing projects for practising consent management in real-life cases.

On the basis of the reviewed literature, semi-structured interview questions have been designed for primary data collection.

3.1 Importance of Consent Management

The theoretical frameworks of Faden and Beauchamp (1986) and Manson and O'Neill (2007) on informed consent allow to identify the importance of consent for personal data collection and processing digitally and understand the need for consent management within the public sector context.

3.1.1 Consent Management for Compliance with Privacy Laws and Regulations

Several scholarly articles point out the need to address compliance with data privacy issue in the online space, especially in complex data use and exchange environments (Fatema et al., 2017; Buyle et al., 2020). In this regard, the recent literature shows consent as *"a primary legislative framework"* (Rissanen, 2016, p. 87) and a user-centric approach (Rissanen, 2016; Zazaza, Venter, & Sibiya, 2019) to data processing and privacy protection as well as a means for *"legitimate processing of personal data by a third party"* (Laurent, Leneutre, Chabridon, & Laaouane, 2019, p. 257). Other scholars argue that the privacy laws and regulations, as well as legal and compliance liabilities of service providers as data controllers and processors, necessitate electronic consent management (ECM) (Bonnici & Coles-Kemp, 2010; Bialke, Bahls, Geidal, et al., 2018). This approach of the ECM includes information disclosure mechanisms (privacy policies, Platform for

Privacy Preferences (P3P), etc.), consent signalling mechanisms (opt-in and opt-out options, automatic signalling based on the privacy statement and preferences, etc.), and consent enforcement mechanisms (legislation and international information security standards) (Bonnici & Coles-Kemp, 2010).

The private sector organizations' failure of compliance with personal data privacy and consent regulations results in being penalized, while compliance is often associated with strengthening customer data protection and trust (Fatema, et al., 2017). The literature does not sufficiently cover the effects of non-compliance with consent regulations in public organizations since consent is not a mandatory legal base for data processing in these institutions. Nevertheless, international penalties for non-compliance are available.

3.1.2 Consent Management for Transparency and Trust

Transparency in the public sector is the common issue raising complex questions in relation to the collected, processed, used, reused, stored personal data and citizen rights on these data (Van Ooijen, Ubaldi, & Welby, 2019). Currently, transparency as a challenge of data collection is considered more serious than identifying the source of the data (Van Ooijen, Ubaldi, & Welby, 2019).

Citizen trust in government authorities and their information systems is crucial for the effective implementation of electronic government (e-government) services, which are highly dependent on processing personal data (Priisalu & Ottis, 2017), and increasing the user acceptance and use rate of these services (OECD, 2019). Trust factor plays a significant role, especially in the environments where interdependence and complex infrastructure exist to execute data-related activities (OECD, 2019). The E-Government Survey 2020 displays that the advancement of data technologies, including data exchange platforms and automated decision-making tools, enhances its benefits for governments in terms of effective decision-making, providing, monitoring and evaluating ongoing governmental activities; however, these technologies also increase concerns on public trust (UN, 2020). The Gallup World Poll 2015 from the OECD Trust Database (OECD, 2017) displays that the level of trust towards governments has been decreasing since 2005. Accordingly, the E-Government Survey (UN, 2020) emphasizes the urgency of handling data-related issues properly to eliminate its impact on the trustworthiness of the government. In this regard, Van Ooijen, Ubaldi, and Welby (2019) say that governments

seek ways to foster public trust and search for the means to provide transparency during data sharing and reuse (pp.40-44).

Clarke (2002) states that the display of consent in information systems creates trust towards e-governance which is critical for organizations with digital solutions. Bonnici and Coles-Kemp (2010) also indicate the importance of consent for establishing end-users' trust in e-services alongside facilitating them in selecting privacy preferences. Rissanen (2016) suggests that to gain data subjects' trust and encourage them to share their personal data, a balance between privacy control mechanisms, including consent management, and the benefits of these mechanisms should be maintained. Finally, Genestier et al. (2017) emphasize individuals' control over personal data via consent management solutions as a significant element for building digital trust.

3.1.3 Consent Management for Privacy Protection and Autonomy

Though the notion of "privacy" can be explained differently, in the context of this paper, it refers to the privacy of personal data or information privacy (Clarke, 2006). In the OECD paper on Public Governance No. 33, Van Ooijen, Ubaldi, and Welby (2019) indicate that protecting the privacy of citizens as " legitimacy and public trust" is a challenge in a data-driven public sector. The reason they state is that the volume of collected, processed, and stored data is increasing due to the governments' proactive service delivery initiatives; thus, the public might have a feeling of governments *"being invasive to a person's personal life"* (Van Ooijen, Ubaldi, & Welby, 2019, p. 42), which would decrease citizens' willingness to share their data. In this sense, the authors emphasize escalating debates around the citizens' rights on personal data held by the public authorities and the necessity to enhance these rights, including the degree of control over the collection, processing, use and alteration of their own data. Data sharing across government departments (Buyle, et al., 2020) and the increasing use of data exchange platforms add to this discussion since despite having apparent contributions to the people's well-being and public value, compound data sharing infrastructures also upsurge the fear of privacy risks (Van Ooijen, Ubaldi, & Welby, 2019). In this regard, Van Ooijen, Ubaldi, and Welby (2019) state that governments should take necessary actions, maintain transparency, responsibility, and security over the controlled data and guarantee that the reuse of personal data does not endanger the public trust.

Several scholarly articles suggest that asking for the consent of data subjects can enhance privacy protection and put control over the hands of data subjects in the digital age. The European Parliamentary Assembly (1998) stated in Resolution 1165: *"In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to [right to privacy] definition."*

The right to privacy in relation to autonomy was an inseparable part of the legal doctrine of informed consent (Faden & Beauchamp, 1986). Based on Faden and Beauchamp's theories of consent, scholars claim that autonomy, in relation to consent management in information systems, encompasses information disclosure, a complete understanding of the provided information, voluntariness, and intentionality for consent provision (Bonnici & Coles-Kemp, 2010; Bonnici, 2013). However, in the online consent management environment, it is impossible to ensure the execution of all these principles. For instance, the factor of full comprehension of the privacy statement is an integral part of autonomous decision-making. Nevertheless, it is difficult to enforce or prove it when consent is given in an online space due to the lack of face-to-face interaction (Friedman, Felten, & Millett, 2000). Based on the studies on the first-generation ECM, Bonnici and Coles-Kemp (2010) also reveal that the abovementioned information disclosure and opt-in/opt-out ticking boxes do not guarantee people's understanding or even reading of terms and conditions. Certainly, a complete understanding of the privacy statements and terms and conditions in an online environment also depends on the simplicity of the language as well as the quality of its presentation (Gautrais, 2004). However, in the first place, it should be assured that data subjects indeed attempt to read them.

Another example that hinders the practice of informed consent principles in the public sector is about voluntariness or, as stated in the GDPR, "freely-given" consent. Although this criterion must be met during the consent obtainment for data collection and processing by the private organizations, it is not the case for the government handling personal data due to the unequal relationship between the parties. In other words, there is "an imbalanced relationship" between citizens as data subjects and the public authorities as data controllers (Buyle, et al., 2020, p. 349). Thus, it is obligatory for citizens to disclose personal data for the government to get public services (OECD, 2016) without "freely-given" consent.

3.1.4 Consent Management for Accountability

Legal requirements on privacy protection and relevant sanctions impose accountability on data controllers, who are the key decision-makers on personal data and data processing. Holding data controllers and processors accountable for the data they handle is one of the critical elements of the GDPR (Van Lieshout, 2016), which makes data "the responsibility of government" (Van Ooijen, Ubaldi, & Welby, 2019, p.41). In the survey of 23 ICT-enabled platforms for citizens' voice, Peixoto and Fox (2016) distinguish between upwards accountability to high-level policymakers and program managers and downwards accountability to citizens. In the context of this thesis, we will consider downwards accountability, which requires responsiveness from service providers based on citizen concern and action.

The beneficence principle proposed by Faden and Beauchamp (1986) can be considered a base for accountability in the consent management context. As the authors mention, this principle creates a moral duty on the professionals – to handle personal data in a way not to impose harm and provide maximum benefit as a part of their work. The contemporary research on e-consent mechanisms indicates that during critical situations, e.g. when a patient's life is in danger, the access of a clinician to personal data should override the patient's consent (Coeira & Clarke, 2004) to be able to proceed with medical intervention as per beneficence model. To satisfy this criterion, Coeira and Clarke (2004) define the form of "general denial with specific consent" and the "gatekeeper" function of e-consent that ensure the prevention of harm by keeping the individual's consent in place.

However, in the literature, accountability through consent is not only linked to the prevention of damage. The positivist informed consent theory proposed by Alderson and Goodey (1998) indicates that informed consent keeps physicians accountable to disclose their purpose of action, gives patients a choice of refusal and only then prevents unwanted interventions. Thus, in the first place, accountability is the answerability of an organization or individuals (OECD, 2016), which means taking responsibility for actions (Council of Europe, n.d.) and reporting the reasons behind the taken decisions. In addition, the 2013 OECD Privacy Guidelines indicates the responsible use of data through accountability in relation to the protection of privacy in the digital environment (OECD, 2016). In this regard, it can be applied to controllers and processors since there must be *"specified, explicit, and legitimate purposes"* (European Parliament and Council of

European Union, Regulation (EU) 2016/679, Article 5, 2016) to gather and process the data, where the controller is accountable to display the compliance with this rule.

The OECD introduced “accountability” as a principle for data privacy protection in 1981, which indicated, *"A data controller should be accountable for complying with measures which give effect to the principles stated above"* (Raab, 2012). Based on the latest updates to the OECD Privacy Guidelines, these principles are collection limitation, data quality, purpose specification, use limitation, security safeguards, and openness (OECD, 2013). Among them, collection limitation and use limitation suggest obtaining the consent of the data subject, and the GDPR recommends this consent being in a written format for the accountability of controllers. The notable points both in the OECD principles and the GDPR are that firstly, none of them necessitates consent due to the issues in practical application. Secondly, both only mentions the controller as a responsible party. Priisalu and Ottis (2017) also argue that data security is a "strategic function" and entails proper management due to its sensitivity and importance for ensuring citizen trust over the government. Therefore, the authors state that data security management should be the responsibility of top-level management of the public institution, who are the primary decision-makers as data controllers.

Nonetheless, Draheim (2020) claims that both controllers and processors are subject to be accountable. He states that collecting and processing citizens' personal data is essential to accomplish public tasks, which also create accountability on the governmental authorities to comply with data governance principles such as minimality, transparency, and consent principles. These principles entail that (1) personal data is *"collected, stored, and processed only for defined purposes and for defined time periods"* (Draheim, 2020, p.3), (2) these purpose and time periods, in certain situations, even the information on the access to data must be disclosed to citizens, and (3) citizens can provide or withdraw their consent via opt-in and opt-out options if data is not a master data (critical for the public service delivery). Overall, it means having data governance principles, including consent principles in place, is essential to hold controllers and processors accountable. Finally, regarding consent management for accountability, the E-Government Survey 2020 of the UN (2020) states that consent-seeking is not always possible since data sharing creates complications in ownership and responsibility for the data. In contrast, Draheim (2020) argues that interoperability and data exchange is significant to deal with difficulties in

consent management and accountability issues by reducing redundancy in data collection and storage.

3.1.5 Consent Management for Information Security

Scholars claim that consent ensures the security of data privacy, including the authorized access to data. As mentioned earlier, Alderson and Goodey (1998) indicate that consent is a tool to protect patients by preventing undesirable, potentially harmful intervention of the third parties to personal data. Indeed, organizations manage informed consent by aiming to avert the use of data for any other purpose than the initially intended one (Landau, 2015) and without data subject's awareness and permission.

Van Ooijen, Ubaldi, and Welby (2019) argue that the government's fulfilment of information security principles – confidentiality, integrity, and availability (CIA) – and connecting privacy and information security fields impact the public perception of the proper use of personal data by the government (Van Ooijen, Ubaldi, & Welby, 2019). The OECD (2019) also defines the primary purpose of digital security as the protection of *"confidentiality, availability and integrity of the activities of an organization that rely on digital technologies and data"* (p. 54). The Security Safeguards Principle of the OECD states: *"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data" (*OECD, 2015, p.38) by data controllers. The damage to the confidentiality of the data is considered a data breach, which can cause the invasion of private life and the loss of trust alongside financial and physical harm (OECD, 2016). As already mentioned, data sharing and reuse create complications in data ownership, which in turn increases citizens' concern over data confidentiality (Van Ooijen, Ubaldi, & Welby, 2019). Coeira and Clarke (2004) state that the absence of an e-consent mechanism in the decentralized online environment would create a possibility of unauthorized access to (patient) data and, eventually, result in privacy infringement. Thus, among the design principles of consent management, they include the access permission to personal (medical) information in the system only with the explicit, implicit, or inferred consent of a patient and the denial of access without consent (Coeira & Clarke, 2004). From this aspect, they describe "a gatekeeper" function of consent in the distributed environment by indicating that the e-consent mechanism checks whether the conditions of the provided consent are met before authorizing access to the physicians. Weber-Janke and Obry (2011) state that

data protection and security in interoperable environments should not be ensured only with confidentiality and integrity instruments but also user consent and disclosure directives. Lastly, in their recent article, Janssen et al. (2020) include consent obtainment for defining the parties with permission to access data as a part of the trusted data-sharing framework.

It should be noted that scholars suggest that consent management systems should also include a security layer. The aim is to maintain confidentiality, data integrity, and non-repudiation so that consent-based decisions of both individuals and controllers would not be distorted with unauthorized alteration of data. (Coeira & Clarke, 2004; Zazaza, Venter, & Sibiya, 2019).

3.2 Consent Management in Practice

Bonnici and Close-Kemp (2010) elaborates on the concept of electronic consent management (ECM) and explain it as *"an online consent management approach that may encompass organizational processes and technological consent management mechanisms"* (p. 119). Other scholars consider this mechanism more efficient and reliable than paper-based consent management (Elkhodr et al., 2013, as cited in Zazaza, Venter, & Sibiya, 2019; Rau et al., 2020). As seen from the definition, consent management is not only about the process but also a technological solution that allows its real-life application. In this regard, Breen, Ouazzane, and Pate (2020) indicate that to comply with consent theory and principles, a transparent mechanism needs to be built, which plainly displays the intended purpose of data collection and processing before a data subject grants consent, confirms the validity and voluntariness of informed consent, and permits the revocation of consent.

To practice this approach in real-life cases, Velmovitsky et al. (2020) present a consent management platform (CMP) and define it as *"a web-based platform that groups all the functionalities necessary for the processing of granting, revoking, and managing consent"* (Velmovitsky, et al., 2020, p. 10). As the reviewed studies display, currently available consent management platforms allow the execution of various activities for different purposes based on the use cases. Firstly, they include enabling data subjects to manage privacy preferences in e-health information systems, which put individuals in control of their data during data exchange (Zazaza, Venter, & Sibiya, 2019). Secondly,

the platforms provide a possibility of observing who access the data, how and for which purposes the data is used, and how long the provided consent will remain valid (Iwaya, Li, Fischer-Hübner, Åhlfeldt, & Martucci, 2019; Rau, et al., 2020), which enhance the transparency of the organization (Mureddu, Schmeling, & Kanellou, 2020). In addition, in the healthcare context, these systems retrieve the exiting consent for delivering a treatment (Yu, Wijesekera, & Costa, 2014), and even override patients' permits when their lives are in danger (Weber-Janke & Obry, 2011). Besides granting consent, these mechanisms also include the functionality for the partial or complete withdrawal of consent (Rau, et al., 2020), which can be performed in an automated or manual way, and its archival for evidential purposes (Iwaya, Li, Fischer-Hübner, Åhlfeldt, & Martucci, 2019). In recent literature, consent management is also displayed as a tool for facilitating the lawfulness of cross-border data portability (Larrucea, Moffie, Asaf, & Santamaria, 2020).

In terms of technicalities, some authors suggest developing a user interface for data subjects through which they can see all the granted or revoked consents (Iwaya, Li, Fischer-Hübner, Åhlfeldt, & Martucci, 2019). Others believe that the application of blockchain technology improves transparency, the accuracy of data management and, more significantly, the security of the consent management systems (Rantos, et al., 2019; Kakarlapudi & Mahmoud, 2021). The notable point is that despite the availability of the abovementioned functionalities and proposals for technical implementation, electronic consent management mechanisms are not widely used in practice (MITRE, 2014, as cited in Rau et al., 2020), especially by the governmental authorities.

4 Research Methodology

This section explains the applied research methods and approaches that are the most suitable to elucidate the research questions. This study aims to explore an underresearched area and gain insights on informed consent and the role and importance of consent management in relation to personal data sharing and hindrances for the implementation of the consent management system. In this regard, a qualitative research method with a holistic case study design has been applied, for which interviews have been conducted as a data collection method.

The research design has been chosen as a single-case study due to two main rationales. Firstly, the author considered the fact that informed consent and consent management have not been widely discussed in the e-governance context and concerning data privacy in the digital era. Thus, the single-case study would help expand the existing knowledge on data consent management (Yin, 2018) and provide a contextual understanding of the case (Creswell, Hanson, Clark, & Morales, 2007). Secondly, the implementation of a consent management platform for consent-based data sharing between public and private sectors in Estonia can be considered as an unusual case worldwide. Therefore the outcome of the single-case study will have a large-scale value (Yin, 2018) so that governments of other countries can also benefit from the Estonian case. In addition, it is an exploratory case study since the author did not only describe the concepts with "what" questions but also explained them through "how" questions (Yin, 2018).

4.1 Data Collection

To collect primary data and acquire expert insights on the topic, short in-depth semi-structured interviews were conducted. The interview questions were open-ended and descriptive. It is the most suitable question form for the case study design to gather comprehensive insights (Creswell, Hanson, Clark, & Morales, 2007). Due to the semi-structured nature of the discussions, some questions were intentionally altered based on the interviewees' expertise. However, all experts were asked about the definition of consent management in an electronic environment related to personal data sharing and data protection, the importance of implementing consent management for public

organizations, and the challenges that arise during the project implementation, which are the essences of the study.

The interviewees were selected based on the relevance of their professional background, including the knowledge and experience on consent management and their involvement in the pilot project of the government on the consent management platform. They included the Estonian government officials, legal experts, and experts on consent management, e-governance, and information security. Considering that reaching out the governmental officials can be challenging, the author also applied the snowball sampling procedure and asked several interviewees to recommend other experts that are aware of the project or possess extensive knowledge on the matter.

In total, eleven experts participated in the one-to-one interview that are listed below:

1. Senior Government Official (Ministry of Economic Affairs and Communications for Estonia, (MEAC)).
2. Sten Tikerpe (Chief Legal Officer, Ministry of Economic Affairs and Communications for Estonia, (MEAC)).
3. Sander Randorg (Product Owner of the Consent Management Platform for the Estonian government, Information System Authority (Riigi Infosüsteemi Amet (RIA)).
4. Anneli Laansoo (Head of Digital Capability Development, Ministry of Social Affairs).
5. Arvo Ott (Member of the Board, Director of e-Government Technologies, eGA).
6. Dan Bogdanov (Head of Information Security Research Institute, Cybernetica).
7. Piret Hirv (Head of Health Technology Division, Connected Health Cluster Manager, Tallinn Science Park Tehnopol).
8. Katrin Nyman-Metcalf (Senior Legal Expert, eGovernance Academy (eGA)).
9. Jaan Priisalu (Researcher, former Director-General of the State Information Systems Board).

10. Triin Siil (Privacy Engineering Consultant, Cybernetica).

11. Kaija Valdma (Product Manager of Estfeed platform, Elering).

Due to the COVID-19 pandemic, face-to-face on-site meetings were not possible. Thus, the interviews were conducted via online platforms such as Zoom and Microsoft Teams. Based on interviewees' verbal consent, the conversations were recorded through the "Screen record" functionality of the mentioned platforms for a precise transcribing process. The duration of interviews changed between 30 and 60 minutes depending on the interviewees' availability and the flow of discussion.

4.2 Data Analysis

Thematic analysis (TA) method was applied to analyse the qualitative data. According to Clarke and Braun (2013), TA is "*a method for identifying and analysing patterns in qualitative data"* (Clarke & Braun, 2013, p. 3) that can be used for a variety of research questions, regardless of the data type and the size of datasets. In this study, six phases of TA (Clarke & Braun, 2013) have been followed, as indicated below.

In the first phase, which is familiarization with the data, the interview recordings were carefully listened to and transcribed. Since the language of the interviews was English, the author was able to use the speech recognition technology of the YouTube Automatic Captions feature to transcribe the recordings automatically. After transcription, the texts were reviewed once more to confirm their accuracy. Upon request, the transcriptions of records will be presented.

In the second phase, codes have been generated based on the transcribed interview data in a systematic manner. Codes are defined *as "the most basic segment, or element, of the raw data or information that can be assessed in a meaningful way regarding the phenomenon*" (Boyatzis, 1998, as cited in Clarke & Braun 2013). To generate the codes and themes, the "NVivo" qualitative data analysis software was used. During the coding process, data collected from each interview transcription were sorted out using the tool. The repeated patterns data were grouped under the same meaningful codes. As coding for as many themes as possible is recommended (Clarke & Braun, 2013), more than 30 codes were generated initially.

During the "searching for themes" phase, the codes were collated under larger groups – *themes,* while unsuitable codes were discarded. Followingly, in the fourth phase, themes were reviewed in parallel to the interview excerpts. Consequently, some themes were merged while the others were disintegrated or eliminated when necessary. This process continued until the coherency in patterns was reached, and the initial thematic map corresponded to the dataset and formulated a data-driven story.

In the fifth phase, themes were named according to the data they included, and a detailed narrative on each theme was created, taking into consideration the research questions and, overall, the aim of the study. As a final stage, a meaningful and analytical report was written based on the themes and data extracts, including the arguments from the literature.

4.3 Validity Testing

Several testing methods are available to examine the validity and quality of the research. The author used construct validity, internal validity, and external validity tests (Yin, 2018).

To test the construct validity of the case study research, a "multiple source of evidence" tactic has been used (Yin, 2018). As indicated earlier, interviews were conducted for primary data collection. Documentary information was collected from the internal official reports called "Consent service analysis" ("Nõusolekuteenuse analüüs") and the "Summary of the Consent Service analysis" as the secondary source of evidence. These documents provided the author with an extensive overview of the ongoing implementation of the pilot project on consent service, including the objectives, key beneficiaries, risks and risk mitigation activities associated with the project and allowed to create a logical connection between the documents and expert viewpoints.

A tactic to confirm the internal validity of case study research differs from experimental and quasi-experimental researches (Yin, 2018). Considering this factor, a pattern matching technique was used to strengthen the internal validity of this study. For this purpose, the "NVivo" tool was also used to create relationships between the themes.

External validity is about the generalizability of study results for other situations beyond the research (Yin, 2018). The external validity of single-case studies is usually questioned

due to the lack of evidence. However, in this study, posing "how" questions instead of merely "what" questions confirmed the external validity.

5 Existing Consent Management Solutions in Estonia

Presently, no consent management service exists that allows personal consent-based data sharing from the public sector to the private sector in Estonia. The Consent Service Analysis report (Nõusolekuteenuse analüüs, 2021) shows the access right management in the Health Information System (CIS) and e-Elering consumer portal[1] for consent-based sharing energy consumption data as similar existing services. In terms of CIS, this service is restricted with the opt-out option to share health data, including the electronic health records (EHRs). The consent management system in the e-Elering portal allows the data owners to give consent and synchronizes consent between the data providers and data users who request consent. However, it does not allow the consent provider to keep control over the data after granting access (Nõusolekuteenuse analüüs, 2021). Neither of these services enables the data flow from the public databases to private sector service providers based on data subjects' consent. For this reason, currently, the Estonian Information System Authority (RIA) is developing a system to provide a *consent service* to the public.

5.1 Consent Service

Consent services are defined as *"electronic services enabling data users to initiate/request and individuals (data subjects) to grant consent for releasing personal data relating to a particular data subject from public sector databases, and public sector databases to verify the existence and validity of such consents before the relevant data is released to data users"* (Consent service analysis: Summary, 2021). It is so-called a convenience service that aims to allow the consent-based retrieval of the personal data held in the state databases to develop new innovative services. As seen from the

[1] https://elering.ee/

definition, key beneficiaries of the consent services are people as *data subjects*, the state authorities as database administrators and *data controllers*, and the private sector service providers as *data users*.

The Estonian eHealth Strategic Development Plan for 2020 (Task Force, 2015) necessitated developing a consent platform. According to the development plan, a technical capability such as a platform needed to enable the cross-use of personal health information held in public databases for research and other application purposes. In this regard, the objectives of the ongoing project include (1) fostering the development of innovative services by allowing companies to use the personal data held in public sector databases, (2) supporting data-driven innovation, increasing the data quality and usability, and (3) handing control over the use of personal data to data subjects (Consent service analysis: Summary, 2021).

6 Interview Results

This section provides a comprehensive overview of the data gathered through eleven semi-structured interviews, including the key themes identified through the number of code references via the "NVivo" qualitative data analysis tool.

6.1 Overview of Consent Management

Based on the conducted semi-structured interviews, the thematic map on key themes and that the experts discussed and associations between the concepts are illustrated in Figure 1 auto-created via "NVivo" software and re-drawn through Draw.io tool.

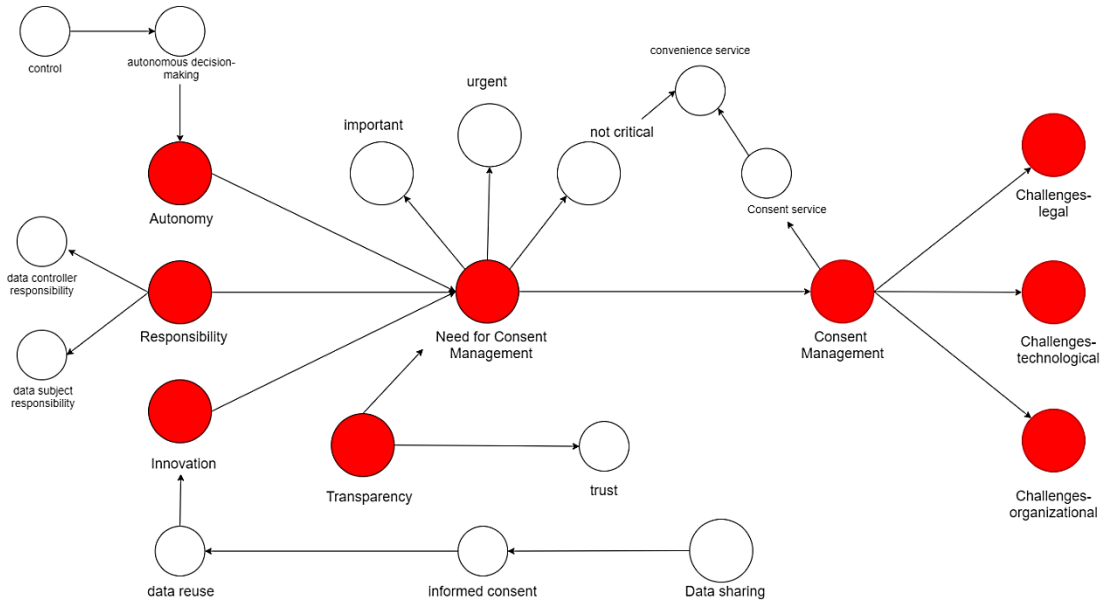


Figure 1. Thematic map

According to the map, the role and importance of consent management and the need to implement the digital consent management mechanism can be defined by its contribution to data subjects' autonomy, the responsibilities over personal data protection, the promotion of innovation, and transparency.

The GDPR does not provide the definition of the "consent management" notion, and the existing literature does not describe it in the public sector context. The interviewees clarified the reason by connecting the currently ongoing discussions on consent and its management to the GDPR implementation, which started only in 2018. Consent

management has been practised before the enforcement of the GDPR since, as interviewees mention, not only the electronic but also paper-based informed consents should be managed and preserved. However, the GDPR brought significant attention to the lawful use of personal data and included consent as one of the legal bases for data processing.

In this term, the author asked the interviewees to define "consent management" and the technology that allows managing consents based on their perceptions in the digital sphere. The analysed data in "NVivo" illustrates that the experts referred to the consent management mainly as a "platform", "system", and few times as a "process".

- Product Manager of Estfeed platform Valdmaa explained it as a technical process or the aggregation of technical, legal and process requirements necessary for the consents to be granted through the technological system. She also included the process of synchronization and sharing consent among the data owner, data operator, and data users that request to access the data.

- Senior Government Official described it as a voluntary system and a layer on top of the data exchange platform that allows data sharing with third parties outside the public sector.

- Product Owner of the CMP Randorg showed consent management as an assurance for data controllers to acquire consents as described in the GDPR to fulfil particular actions. In this regard, he defined consent management as a centralized system or process that provides private sector companies with a way to ask for personal data and gather consents within the legal boundaries to deliver services. Head of Information Security Research Institute Bogdanov also added the storage and demonstration of consent to the key user stories during the consent management process.

- Chief Legal Officer Tikerpe specified consent management as "*a tool that helps controllers, processors and data subjects to conclude the activities that they are already concluding today, in a more comfortable, efficient and transparent manner."*

- In Privacy Engineering Consultant Siil's opinion, it is a practical term. Thus, it needs a practical definition than a legal one rather, even though the notion contains legal content, which is the description of the consent requirements in the GDPR.

6.2 Consent Management and Adherence to Informed Consent Principles

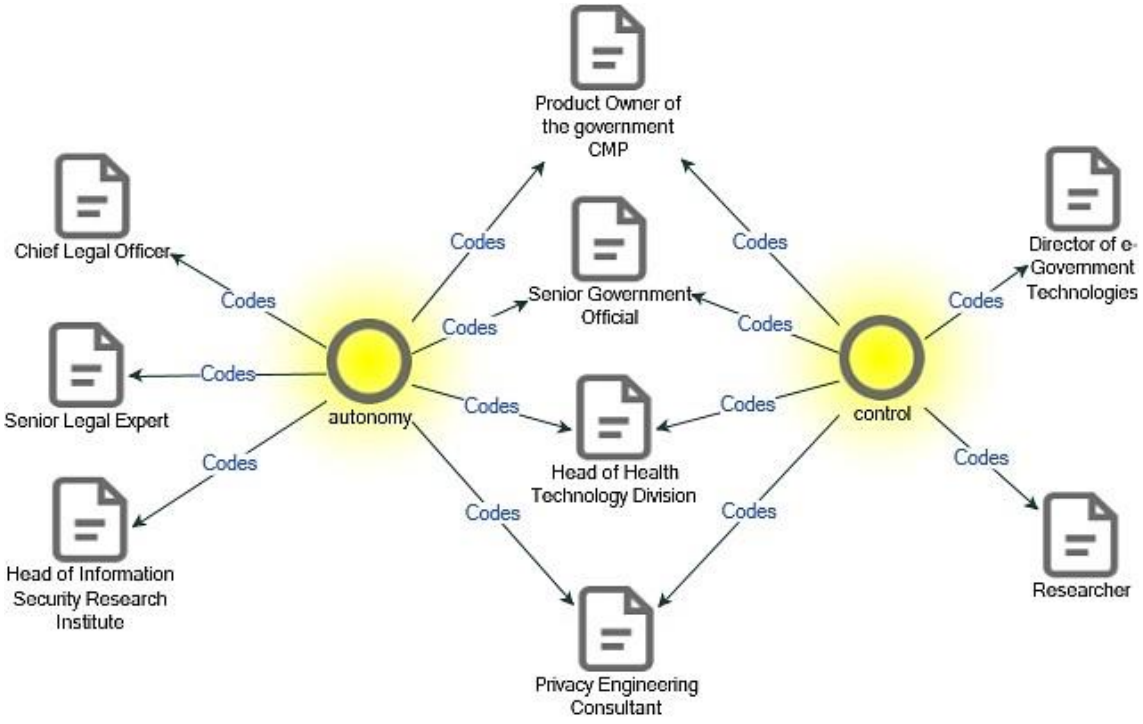


Figure 2. Adherence to main consent principles

The interview results display that nine out of eleven interviewees mentioned data subjects' control on the use of personal data, autonomous decision-making or both factors among the key significances of consent management that would allow public organizations to adhere to consent principles (Figure 2).

The interviewees think that in practice, people have lost control over the use of their data by private sector service providers. In this regard, they indicate the consent management service as an attempt to bring a person in charge of his data and an opportunity for a data subject to constantly control and have the final say on the data queried from the public databases. Privacy Engineering Consultant mentions that the availability of the CMP can provide data subjects with an opportunity to stay in a constant relationship and dialogue with controllers regarding how the data is being used. She adds that citizens have played

a passive role in monitoring their data collected by private service providers until today. It means consent management has been a "one-way road" associated only with ticking boxes without knowing where the data is stored and what other processing activities are conducted. Thus, it is expected that the application of consent management for data sharing between public and private sectors will make consent more dynamic and directional and allow data subjects to practice their rights under the GDPR in the digital world.

The experts discuss data subjects' autonomous decision-making simultaneously with their control over the personal data via consent mechanism. As mentioned in the GDPR and confirmed by the legal experts, consent-based processing is not fully applicable to the public sector because of the imbalanced relationship of data subjects with the government and the impossibility of the consent being "freely given". In other words, the government cannot provide a choice for data subjects to share data since people's refusal to do so would make the government nonfunctional, obstruct the public authorities to fulfil their duties arising from law, and deprive citizens of receiving critical public services. As Senior Government Official mentions, data processing in proportionate to the purpose is "an inherent need" for the government. Thus, having no choice of opt-in and opt-out option makes the informed consent invalid.

Nevertheless, Senior Government Official indicates that the authorities do the mundane bureaucratic services during the public service provision, especially during life-event services, and give citizens the chance to decide when necessary. Besides, according to senior legal expert Nyman-Metcalf, data subjects must exercise their right to respect private and family life in the digital sphere through autonomous choices. In other words, the authorities must collect the minimum amount of personal data relevant to the provided service without requiring information about the private life. Priisalu notes that the definition of "privacy" is context-dependent and not easy to identify. However, as stated before, privacy in the GDPR context is about personal data privacy. Nyman-Metcalf indicates that historically, data protection mechanisms emerged from the need to protect the private life or sphere. Privacy Engineering Consultant further elaborates this argument by stating that the GDPR is designed to protect both individual privacy and a person as a part of society. Thus, even though the government must collect and process personal data, to some extend, citizens still hold autonomy over the protection of data privacy through non-consent mechanisms indicated in the GDPR.

Chief Legal Officer states: *"the main purpose of the introduction of consent-based processing options into law has been to give an individual the opportunity to directly decide, which third parties should be able to access their data."* In this term, experts add that the availability of a consent management system will bring data subjects to the center of the private service provision and give them the liberty to choose which services to receive based on the shared data. Also, Senior Legal Expert considers consent-based data processing very important since it allows data subjects to independently decide on the use of personal information in certain ways outside the public sector without state intervention.

Overall, the experts mention that by empowering data subjects to freely decide on and control personal data use freely, the consent management mechanism also increases people's knowledge on data privacy and protection issues as they start acquiring more information about what happens to their data once shared.

6.3 Role and Importance of Consent Management in the Public Sector

Based on the interview results, it can be concluded that the main role of the consent management system includes the promotion of countrywide innovation, holding the controllers, data users and data subjects responsible for the personal data processing. The experts also indicate the indirect contribution of consent management to transparency and public trust.

Consent Management for Innovation

The interview results revealed the connection between consent-based data sharing and innovation (see Appendix 3). The experts and the Consent Service Analysis report (2021) emphasize that one of the key roles of implementing consent management is to boost innovation and the development of data-enabled services by the private sector actors. Product Owner of the CMP states: *"Private sector companies tend to have great ideas on how to utilize the data that has been gathered in the public databases and how to innovate and provide services that have not provided until now by the government."* From this perspective, most interviewees believe that consent management solutions will allow the private sector service providers to build innovative services based on the personal data collected in various public sector databases upon the data subjects' consents.

Two interviewees indicate the necessity of the consent management system to accelerate innovation in the healthcare sector and build new and more personalized health services, while others mention either of these factors. Head of Digital Capability Development Laansoo mentions that the healthtech industry demands personal data to build new products and services and expand the market. Thus, the aim is to provide a more technically enhanced way to provide easier access to the data and build innovative services efficiently without administrative burden. Ott indicates that this is a "legally correct solution" for people who will voluntarily consent to share their health and other personal data to acquire personalized services with specific benefits. For instance, based on the shared history of health data or prescriptions, private companies or startups can create personalized dietary recommendations. Nevertheless, Laansoo indicates that the growth of the demand for the government consent service cannot be forecasted at the beginning. As the other interviewees agree, it is a "convenience" and value-added service to support the development of the private sector and the provision of personalized services, which are optional to use.

Consent Management for Accountability

The interview outcomes illustrate that the use of a consent management system for data sharing increases data subjects' responsibilities to take care of the personal data since they are the key "decision-makers" in sharing the data (see Appendix 3). However, they also do not exclude the controllers' responsibilities.

From the consent management perspective, Product Owner of the CMP indicates that the controllers' main interest is to oversee and prove that data sharing is done legally with all of the required consents in place. Thus, several interviewees agree that consent and its management can hold controllers accountable and compliant. Nevertheless, most of the experts emphasize that when data subjects give informed consent for the data sharing and processing purposes, they also share the responsibility of taking care of the personal data. They indicate that since individuals make decisions of transferring and processing their data autonomously, they also bear the consequences of data sharing with third parties. From this aspect, the experts consider that consent management is an essential means to increase people's responsibility to take care of personal data and be aware of the risks before granting access to their data.

Consent Management for Transparency

According to the interview results, nine out of eleven experts mention transparency and follow their arguments on citizen trust while discussing the importance of consent management. The experts argue that the consent management system in itself does not directly contribute to transparency (see Appendix 3). Although Tikerpe describes it as a tool that assists controllers and processors by increasing the efficiency and transparency of their activities, he also adds that consent management is not a legal instrument in itself nor the only legal ground for the processing.

The interview results also show that in order for the consent management system to be considered a means for transparency and assist organizations in complying with transparency requirements, besides the options of providing and revoking consent, it should also allow data subjects to track the parties and gain a clear overview of who access and process the personal data, for what purposes and duration. As an example, the experts point out Eesti.ee[1], the state one-stop-shop portal. In this case, firstly, the Estonian residents need to log in to the system through one of the electronic identification (eID) solutions. Followingly, they can monitor which authorities send the queries to access their personal information and for what purposes. This process happens through the data tracker, which logs data exchange activities in the information systems of the data processors and keeps the records of processing as required in Article 30 of the GDPR. The interviewees also indicate that this technology provides average data subjects with a better understanding of how and when different organizations use personal data and the reasons behind their activities. In this sense, Randorg states that the goal to implement data tracker is to make the data traffic transparent by allowing individuals to trace authorized parties that involve in data exchange and, eventually, to maintain the high trust level in Estonia.

Following these arguments, the experts also indicate that creating transparency in the public sector lead to enhancing citizen trust towards the government. Priisalu explains trust as a meta-expectation. In this regard, he explains public trust as meeting the public expectations and displaying how these expectations are reinforced. Ott remarks on the fact that in some countries, people do not trust directly to the government but how the

[1] https://www.eesti.ee/et/

data is handled in the public sector. In this sense, the interviewees again bring up the transparency issue by stating that if data processing in proportion to the purposes is clear and easily observable, data subjects will be more trustful and willing to consent to the data collection and sharing.

Ott considers the data monitoring tool or data tracker *"a good mechanism to build trust."* The reason behind this connection is not only the possibility of tracking the data processing activities but also the availability of the option to ask for a clarification from the processors. The interviewees illuminate that in case of data subjects observe a suspicious activity concerning their data, including unclear reasons or legal grounds for the processing, they can demand a detailed explanation from the respective authorities. They must also be able to demonstrate their purposes in a transparent way.

Additionally, several interviewees mention the importance of the agencies that deal with personal data protection violations and related concerns of data subjects to further enhance transparency in the public sector. Valdmaa states that in the transparent system, besides providing consent, observing to whom the permission is granted, and who access the data, there has to be a means to protect individuals against the misuse of personal data. As an example from Estonia, the experts highlight the supervisory agency – Data Protection Inspectorate[1] under the Ministry of Justice. This agency deals with individuals' complaints if they are not satisfied with the explanation of the public authorities or encounter personal data protection and privacy violations.

Nonetheless, the interviewees state that if the other conditions are met, the development of the consent management tool is a practical step to foster these principles further. In this respect, Ott states that autonomous decision-making on providing permission to use personal data is about trust-building.

Still, several interviewees stated that public trust is vulnerable. The lack of transparency and few incidents regarding the misuse of personal data or the violation of data protection regulations are sufficient to considerably decrease trust. Priisalu also adds that public trust is "a shared value in any society or organization", which reduces friction in processes and thus increases the performance of the whole organisation. It is applicable to governmental

[1] https://www.aki.ee/en

organizations as well since the government consists of various public authorities. Hence, if any authority faces the abovementioned incidents, the loss of trust is also projected to the other public organizations. It primarily affects the use rate of e-services. Senior Legal Expert explains that the lack of trust creates “a vicious cycle” in the sense that people “feel uneasy” and stop using services; consequently, the government loses its incentive to build new digital services due to the low use rate.

6.4 Need for Consent Management

Based on the interview discussions, the experts argue that the need for consent management in public organizations depends on the use cases. Overall, the experts think that the use of consent management tool by the public sector is an essential solution in the digital age to support the private sector service development, provide innovative and personalized services, ensure transparency and accountability of stakeholders. However, they also state that the implementation of the system is somehow urgent and not critical (Figure 3).

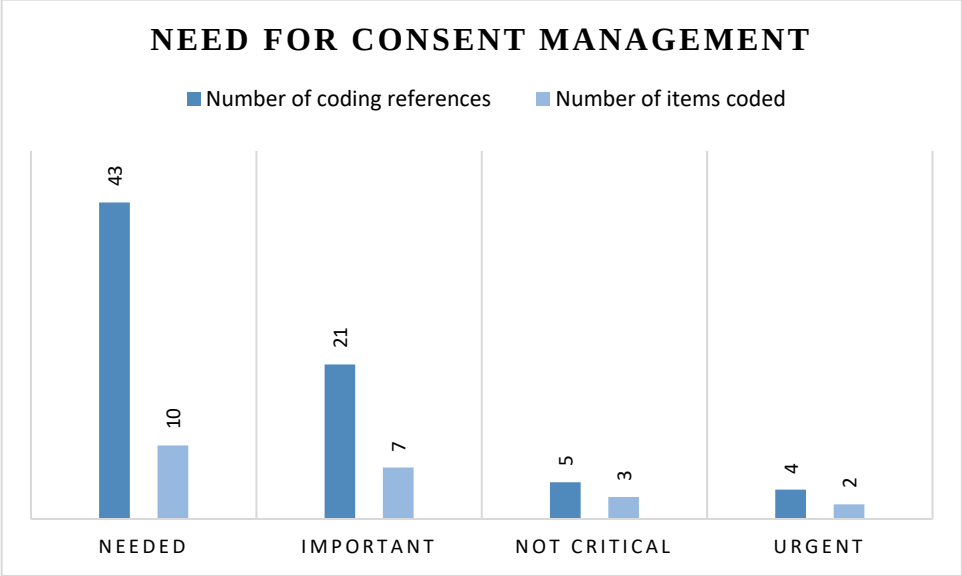


Figure 3. Interview results on the need for consent management

Several interviewees identify the implementation of the consent management system as a “not critical” but an important step to increase data reuse practices. Among them, Senior Government Official argues that the absence of this service does not affect the well-being of the data subjects nor interrupt public authorities’ work, which makes it not critical in

the current situation. Besides, Bogdanov justifies his opinion by emphasizing that a high maturity level in data reuse and interoperability among the public databases is needed for consent management to become critical worldwide.

In terms of urgency to implement a consent management system, interviewees argue that it depends on the volume of the data gathered and stored in the public databases and third parties' interest in reusing this data. For instance, the healthcare sector has a demand for innovative services, as mentioned earlier; thus, healthtech industry actors are highly interested in high-quality data reuse. Nevertheless, exceptional cases that require prompt action increase the urgency of practising consent management in the public sector. Several experts remark on the situation during the COVID-19 crisis that the consent-based reuse of personal data could expedite the development and provision of technological solutions to combat the pandemic.

6.5 Implementation Challenges

Taking into account the interview outcomes, challenges in the implementation of consent management system can be categorized as legal, organizational, and technological challenges. Among them, participants mainly discussed the legal challenges and mentioned organizational ones the least. (Figure 4).

Figure 4. Challenges in the implementation of consent management

Legal Challenges

From the perspective of the legal challenges, the experts mentioned legal framework, division of responsibilities, and citizens' understanding of purpose statements and terms and conditions (T&C) (see Appendix 4). Firstly, the interviewees' responses display that generally, the existing legal framework is not a barrier for the application of consent management solutions due to its technology neutrality. In addition, Siil states that legally consent can be provided in any form, including verbal, written on paper, or electronically, via digital signature or box-ticking; thus, significant legal changes are not needed to implement consent management in the public sector.

Nevertheless, the experts indicate that there will be a necessity for the secondary legal instruments such as rules and guidelines on how the platform will function and manage the provided consent in compliance with data protection regulations. It is a challenge to decide on these rules and the law that defines the CMP since there are many different ways available to regulate the solution. However, eventually, the platform must be designed to align with the existing national and binding international legislation and allow data subjects to keep control over the data. In this regard, Senior Government Official assumes that the regulation of the CMP in Estonia will fall under the Public Information

Act (*"Avaliku* Teabe Seadus"), which also regulates how public databases and the data exchange layer – X-Road must function.

Several interviewees stated that the issue is not about laws and regulations per se but their implementation and monitoring in practice. According to the experts, understanding the GDPR, including data processing requirements and how to execute them, is not yet clear to all data controllers and processors, especially small or not-mature private companies.

Another legal challenge that the experts emphasize is the division of responsibilities in consent-based data sharing and processing. Firstly, currently, the scope of the consent management system includes only the consent management for data transfer from the public database to the private sector service providers. As Bogdanov states, this is not a legal basis for the private companies to process the data; thus, further data processing will be based on the contract or consent between them and the data subject. The role and responsibility of the public authorities, in this case, remains unclear.

Furthermore, as mentioned earlier, the experts consider data subjects as the primary responsible party in the consent management process since ideally, data will be shared and processed based on their voluntary and informed permission. Nonetheless, it is the fact that data subjects do not always make an informed and autonomous decision due to several impediments. For instance, all interviewees claim that unclear and lengthy purpose statement and T&C discourage data subjects from reading them or making them difficult to comprehend. Asking for broad consent and data subjects' unfamiliarity with private sector service providers' activities are other hindrances. In this regard, the key question that experts impose is whether the government should share the responsibility for the processing personal data by private organizations to protect the citizens. If yes, in which stage of the process the government should take action.

More importantly, the interviewees focus on is the responsibility for the purpose and conditions for processing, which will be displayed over the government-provided CMP. According to the experts, the government can take one of two approaches in this case. The first one is the conservative way of controlling, which means the government itself assesses and decides whether the service that private organizations provide is relevant, safe or the company owners are trustworthy so that personal data can be shared. The experts mention that people are usually not careful or knowledgeable enough about a

private service provider. Thus, they can make irrational decisions on sharing their data on many platforms. Therefore, this kind of activities might encourage the government to take a conservative approach. In this regard, the interview participants bring up another issue – the strictness of screening. They state that how to decide which private service provider will be given access and where to draw the line not to restrict the activities and rights of businesses remain open questions.

The other one is a liberal approach that will make the government completely free from the responsibilities over the agreement between data subjects and private service providers on data sharing and processing. In this scenario, the government carries the obligation to build the platform to create such a condition for data subjects to exercise their data protection and consent-related rights and data users to comply with the consent requirements identified in the GDPR. However, the clarity of the purpose and privacy statements, the scope of consent, and the data subject's decision will be out of government control. From this aspect, Bogdanov emphasizes another issue that if companies acquire broad consent with a tricky and complicated purpose statement, data subjects have a right to bring the case to the court. In this regard, whether the government would be a defendant for people because it assisted those companies remains a challenge.

Technological Challenges

The interviewees generally think that technological challenges take a small portion of all obstacles to implement the CMP in countries like Estonia. The reason is the existing underlying infrastructure, including ready information systems, electronic identification and authentication systems, and the data exchange platform enables the unproblematic development and integration of the consent management system. Nevertheless, they also point out several technical complications that might arise during or after the implementation of the CMP (see Appendix 4).

The first one that Bogdanov and Valdmaa mention is the synchronization of consent across information systems. After a data subject provides or revokes his consent for data sharing, the time lag might occur during the synchronization of consent among the data controller and the data user. The duration of the lag can vary between several seconds to minutes, depending on the internet connectivity or other system-related issues. Within this timeframe, a private company, who previously had the right to access the data, might use the data again while the physical person has already withdrawn the consent. From this

point of view, Bogdanov also indicates the revocation as an issue for consent management systems. Particularly revocation becomes complicated if two consents for data sharing and processing are collected from data subjects since the withdrawal of consent for data sharing should technically nullify the consent for processing specific personal data given directly to the data users. In this regard, how the data users will be aware of the revoked consent in time or whether they can still keep the data under other legal bases are the critical issues that seek the solution. The experts also relate the synchronization and revocation challenges to cross-border data sharing via informed consent. In this case, the main questions are how to synchronize consents and ensure their simultaneous revocation from different consent management systems of the parties located in different countries.

Regarding system security, the interviewees primarily do not see it as a challenging part of the CMP implementation since the platform itself relies on the security levels that information systems define based on the three-level IT baseline security system requirements – ISKE [1]. The security level of the information systems is determined based on the types and their sensitiveness of data stored in the information systems. For instance, Laansoo states that the health information system in Estonia has the highest security level due to the sensitivity of health data.

Other mentioned technological challenges include the overloaded system due to the poorly defined system success, the match of technical and legal requirements, and the availability of resources in the small or young private sector service providers to build machine-readable automated Application Programming Interfaces (APIs).

Organizational Challenges

From the organizational perspective, the interviewees indicate the rearrangement of work processes and change management as a non-permanent challenge, especially for large organizations. Besides, they argue that consent management as a process can create complexities. For instance, this process will be readily run on top of the already existing processes of the organizations, which is not always the best fit for each other.

[1] https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html

7 Discussion and Recommendations

In this section, the abovementioned interview results are analysed and synthesized with the literature and official reports on the topic to determine the answers to the research questions.

7.1 Adherence to the Principles of Informed Consent

The experts indicate control over personal data and autonomous decision-making as the key consent principles to adhere to through consent management mechanism. Today, control over personal data is ensured through eight individual rights stated in the GDPR, including the right to be informed about who is processing the personal data and for what purposes, the right to access the data, and the right to restrict processing. However, as the Special Eurobarometer 487a survey (European Commission, Special Eurobarometer 487a - The General Data Protection Regulation, 2019), indicated in Chapter 1, illustrates and interviewees confirm, individuals have lost control over the personal data. The main importance of the control over personal data processing is the autonomy in decision-making on digital privacy and the use of personal data by private service providers. In this sense, losing control over the data also results in the deprivation of individuals from autonomous decision-making.

As stated in the literature, self-governance is one of the moral principles of informed consent that Faden and Beauchamp (1986) indicated, including privacy, voluntariness and autonomy in decision-making and freedom of choice. Presently, in Estonia, *"andmejälgija"* or *data tracker*[1] is used to adhere to this principle, allowing data subjects to hold control over their data during the personal data sharing within the public sector. Nevertheless, data sharing outside the public sector requires complete control of people on their data to decide whether they are willing to use a private service or not. In this regard, the experts point out that the availability of consent management tool will play a significant role since it will enable data subjects to actually control the use of data outside the public sector and see the outcome of their decisions, which Genestier et al. (2017)

[1] https://e-estonia.com/data-tracker-build-citizen-trust/

also mentions. Based on the outcome, they can report the incident to the responsible authorities such as Data Protection Inspectorate.

Thus, it can be concluded that consent should be considered a powerful tool not only for data subjects to give or deny permission for the use of personal data but also, as Faden and Beauchamp (1986) mention, for data subjects to be respected as autonomous. In other words, through this mechanism, organizations will acknowledge the data subjects' rights and independent choices over their data that are free from any interferences. Overall, as indicated in the Consent Service Analysis Summary report (2021), the main goal in implementing consent management in the public sector is citizens' empowerment. Risling et al. (2018) explain this factor in the digital healthcare context by indicating that for patients to feel empowered, they expect to be informed, heard and have ownership over the decisions before receiving the treatment. Similarly, data subjects feel total control over their data if their rights under the GDPR are fulfilled via the help of the consent management tool.

7.2 Consent Management for Innovation

The interview results illustrate that consent-based data sharing and the availability of consent management system supports innovation and private sector development, which is not sufficiently covered in the existing literature. Borgogno and Colangelo (2019) state that the reuse of high-quality government data allows the new service delivery effectively and efficiently. Thus, the private companies can take this advantage by asking data subjects' consent to use the readily available personal data.

As already mentioned, the interviewees also talk about the provision of personalized services based on consent-based data processing as a part of innovation. The survey conducted by Tehnopol in 2018 demonstrates that more than 70% of respondents living in Estonia, who will be the primary beneficiaries of the consent service, are willing to share their health data with third parties with the expectation of receiving better service outcomes (Tehnopol, 2019). It is possible to hand out these data on paper; however, the paper-based personal data exchange from the security perspective is not a reliable process nor the most efficient way for citizens.

Furthermore, Siil indicates that consent-based data sharing contributes to data altruism, which is defined as *"data voluntarily made available by individuals or companies for the common good"* (European Comission, 2020) in Data Governance Act. In other words, it is about the people' consent to share their data with businesses in a safe environment and in compliance with the European Union (EU) policies. The act considers creating *a data altruism consent form* for efficient consent acquisition and data transfer directly by the individuals or data controllers. From this aspect, the availability of a consent management system for standardized and simplified consent-based data sharing will facilitate the process.

Yet, the value of the consent management service from an innovation perspective is also closely connected to the value and quality of the requested data. Draheim (2020) identifies data quality principles as correctness and consistency, as well as integrity, accuracy, completeness, authenticity, and recency of data. Bogdanov states that data quality is mainly about the data owners or subjects providing correct information, and it depends on whether the public service meets the citizens' demands so that they are willing to share accurate information. Generally, data held in public databases is considered high-quality. However, if people do not feel the necessity to use the service, they are demotivated to provide accurate personal data. Thus, in the first place, data quality needs to be ensured for its meaningful reuse based on consent.

7.3 Consent Management for Accountability

The literature emphasizes that consent and its management can be an effective tool to hold data controllers and processors accountable. As stated in the GDPR, data controllers, who are primarily organizations than individuals in practice (European Data Protection Board, 2020), are the responsible parties that decide on data policies, including access grants and the disclosure of information, *how* and *why* data is processed, and consent management, when necessary. The interviewees state that they are mainly from the higher level of the organizational structure, such as ministries. As mentioned in Chapter 2 and explained by the experts, a data processor or in Estonian, *"andmetöötleja"*, is from the lower levels of the organizational structure and follows the controllers' instructions, including dealing with the data and its processing from a technical perspective. Therefore, consent management does not really affect how accountable the processors are.

However, the interviews revealed that data subjects also take the responsibility to take care of personal data once they share it through informed consent. Pattinson, Chen, and Basu (2020) indicate that freely given consent is also an indicator that a person is mindful of the potential risks and will share the responsibility of consequences. Data subjects make voluntary choices to share personal data with any person or organization outside the public sector via social media platforms or other communication channels, in paper or electronic forms, while bearing the consequences. Senior Legal Expert states that data breach incidents mostly happen in the private sector, which is also proven by the statistics. For example, the European Union Agency for Cybersecurity (ENISA) (2020) reports that in 2019, digital services, including e-mail, social media platforms and cloud providers, are among the fields that are exposed to cyber-attacks. However, she also adds that data subjects are also responsible in these cases since they choose to share personal information with the parties that might or might not be trusted service providers.

In terms of data sharing through the government CMP, as interviewees indicate, ultimately, the responsibility of giving the consent lies with the data subject himself due to two main reasons. Firstly, as shown above, it is based on the data subjects' free will to provide consent through the CMP. Thus, based on their free will, they can choose to grant consent to benefit from personalized services or revoke consent if they wish to stop using these services. Secondly, the government carries out the pre-screening of private company service providers that want to use personal data held in public sector databases in advance. It means, in this process, the government takes the responsibility to conduct a background check of private service providers to ensure that they function within the legal boundaries and protect data privacy. Yet, the final decision to share the data is made by the citizens.

7.4 Consent Management for Transparency

The European Interoperability Framework (EIF) (European Comission, 2017) explains transparency as (1) the internal visibility of public authorities and the possibility of observing administrative and decision-making processes, (2) the availability of user interfaces connected to the information systems, and (3) the protection of personal data handled and stored in public sector databases. The literature shows that achieving transparency in data processing is a complex process; yet, it is a significant factor for

enabling people to exercise their rights and enhance public trust over the government. From this point, the scholars also claim that consent management solutions enhance transparency due to the explicit display of evidence regarding the provision or withdrawal of informed consent (Bialke, Bahls, Geidal, & et al., 2018), which ultimately increases data subjects' trust towards the e-services. The guidelines of the European Data Protection Board (EDPD) on consent (2020) defines that informed consent being "specific" is about the requirement for transparency.

On the contrary, the interview results display that there is no direct relationship between consent management and transparency. The Recital 58 of the GDPR explains transparency as the clarity of the information presented to the public as well as the clarity on the identity of a party that collects the personal data and the purposes behind this action. In addition, Articles 13 and 14 in the GDPR require that data processing must be transparent so that data subjects can exercise their right to be informed. These articles do not display consent as a means for transparency specifically but specify criteria to be met in advance to enhance transparency. In this regard, the experts point out the one-stop-shop state portal Eesti.ee and the data tracker as the available solutions.

More awareness about how and why personal information is processed fosters trust. To be more precise, obtaining a clear overview of personal data related activities and having a choice to decide on the use of data reduces citizens' concerns about the large volumes of personal information collected and stored in the public databases, which is further processed and exchanged among various parties. Head of Digital Capability Development thinks that the cornerstone of patients' trust is the opt-out option in the health information system that allows patients to decide not to share personal information with healthcare providers through consent. However, the current consent platform will also provide an "opt-in" choice for the health data to flow from the eHealth system (Task Force, 2015). Unforced data sharing will increase the confidence of data subjects to trust the data controllers and processors. Mainly if the personal data contains highly sensitive health-related information, as Tith et al. (2020) mention, the consent should be managed based on the purpose in order to avoid the data subjects' hesitancy for data sharing. Generally, interviewees argue that when individuals clearly see and comprehend the purpose and benefits of consent-based data sharing, they will be more likely to trust the data controllers and processors and feel comfortable using digital services. It approves Rissanen's (2016)

suggestion of balancing the implementation of consent management mechanism with its benefits for the society to maintain the citizen trust.

As indicated previously, the interviewees highlight that public trust can be broken with the minor mistake of controllers or processors while handling personal data. In this regard, several characteristics of the consent management system can potentially prevent the incidents and maintain data subjects' trust. For instance, government officials draw attention to the automatic background checks of private companies that request personal data for processing before asking consent from data subjects. It includes inspection of the registration and licenses of a company and the lawfulness of the company activities, including the data protection violations. The purpose of the background screening is to confirm the reliability and compliance of the private sector service provider with the legal requirements and the proportionality of the area of activity and motives to the requested personal data. Thus, it is considered a measure to ensure public trust (Consent service analysis: Summary, 2021). The state approval of the private sector service providers will be so-called a control system and increase the reliance of data subjects on the consent service. Therefore, people will be more willing to share their data to acquire personalized services.

The purpose verification of data release will be another significant part of the consent service indicated in the Consent Service Analysis (2021). This functionality will work based on the data minimization and transparency principles, which are also identified as data governance principles (Draheim, 2020). It means the collection and processing of data will be "adequate, relevant, and limited to the purpose" (Information Commissioner's Office (ICO.), 2021), time-bounded and demonstrable so that data subjects will trust the consent-based data sharing.

Finally, user-centricity in consent management can contribute to citizen trust in the system. Junginger (2018) state that user-centricity in governmental service design improve people's trust and confidence in governmental activities. In this regard, Product Owner of the CMP emphasizes that data subjects can provide, observe, and manage all their consents for data sharing from a single point – the state portal. Consequently, the consent management process will be hassle-free, which will lead them to use the system more confidently and regularly.

7.5 Need For Consent Management in Public Sector

As state earlier, it is neither necessary nor practical to ask for citizens' consents for the public service provision. In countries as Estonia, where the government provides proactive life-event services, people expect to receive the services in the most convenient and seamless ways possible. The experts confirm that the government tends to deliver automatic services and build an invisible interaction with citizens. For this reason, continuous data processing and exchange across the public sector organizations are essential. Erlenheim, Draheim, and Taveter (2020) also argue that the proactivity in public service provision targets to decrease inefficient and time-consuming bureaucratic procedures make citizens' lives easy. In this regard, asking, granting, or denying the permission on every step would be an additional burden for data subjects, controllers, and processors and delay, even this fact does not exclude a consent-based provision of proactive services (Erlenheim, Draheim, & Taveter, 2020). Friedman, Felten, and Millett (2000) also argue that informed consent management during online interactions can create a burden or "nuisance" for users if the system asks for explicit consent every time they execute web-based actions.

Furthermore, Senior Legal Expert mentions that the social contract theory plays a significant role in regulating the relationship between data subjects and public authorities. It means citizens and the state agree on an implied contract to comply with certain social rules and principles. In the context of this study, she explains that this theory justifies the presumed consent to the exchange of personal data and tax payment to receive public services. The government needs citizens' data to function and deliver public services in the most convenient and seamless way possible. Data exchange among the public authorities is one of the most effective ways to bring convenience to public service delivery and reduce the administrative burden for both citizens and the government. In this sense, these authorities as controllers must have a legal ground to process the personal data within the public sector and explicitly display their purposes. However, the legal basis is not an informed consent described in the GDPR, excluding the cases that the T&C of service indicate. As an example from Estonia, Chief Legal Officer states that there are databases that carry out specific processing activities under consent, such as delivering official documents to a person via electronic means through Eesti.ee, as stated in the T&C of the state portal. Nevertheless, it is rather an assumed and "philosophical consent" taken from citizens in usual cases, as Senior Legal Expert describes.

In addition, as the experts mention, the interoperability maturity level, which is the "organizational capacity to achieve interoperability" (Misuraca, Alfano, & Viscusi, 2011, p. 98), is significant for the consent management system become critical. Gottschalk (2009) defines computer, process, knowledge, value, and goal interoperability as the interoperability maturity levels in digital governments. Indeed, it is challenging to implement a unified consent management system across the different organizations in different interoperability maturity levels.

Yet, the experts find consent management important due to several reasons. Firstly, it enables the democratic use of personal data based on free will by protecting the data subjects' rights. Ott states that personal data processing is strictly regulated by national and EU legislation in Estonia. In this regard, the implementation of CMP would assist the private sector service providers in handling personal data in compliance with the GDPR. Secondly, consent management creates an opportunity to move to the next level in data sharing and accelerates the processes that require the use of personal data. Several interviewees show health data sharing before performing mandatory military service as an example. They state that if people do not provide their consent to share the health data for the indicated purpose electronically, they must present it on paper. However, as said before, the aim is to advance and ease the data sharing methods both for citizens and data users. Thirdly, advancing technologies and personal data reuse possibilities increase the importance of consent management for the public sector. In this regard, one of the expected use cases is cross-border data sharing, which is recently being discussed in the EU context. The European data strategy targets establishing a single market for data – *"an essential resource for economic growth, competitiveness, innovation, job creation and societal progress".* The aim is to make it reusable across the Member States (European Commission, 2021), enable cross-border data transfers, and harmonize the EU-wide innovative service provision (European Comission, 2020). It is also emphasized in the Data Governance Act that citizens and businesses, the actors that generate the data, should be able to control their data during the data exchange and reuse across the EU. Therefore, the experts consider that consent will be a more powerful means, in the long run, to enable personal cross-border data sharing while keeping data subjects in control. Finally, as Product Owner of the CMP emphasizes, the CMP platform will standardize the way of managing consent across the various involved parties, which he considers *"a natural addition to the e-government ecosystem".* It will allow the consent management

process to run uninterruptedly, regardless of the shared personal data. Eventually, it will become a best practice for dealing with consent and simplifying the service provision based on personal data.

7.6 Implementation Challenges

The interview outcomes show that the public authorities might encounter mainly three types of challenges, among which the legal ones draw more attention than technological and organizational obstacles.

As the experts indicate, technology-neutral law is not a hindrance but rather an enabler of the implementation of the consent management system. Hildebrandt and Tielemans (2013) argue that the law is considered technology-neutral when it meets three objectives: (1) compensation objective, which ensures that the law defines specific technology that can potentially jeopardize the fundamental human rights, (2) innovative objective that is about the non-discrimination against the technological designs, and (3) sustainability objective that put an emphasis on the standing validity of the law for a long time duration. The GDPR meets these objectives since *"it protects personal data regardless of the technology used or how the personal data is stored"* and irrespective of the form of data processing and storage (European Commission, 2018). The Estonian legal environment is also technology-neutral since, if insignificant, no law was adopted on a specific technology (European Commission, 2019). Still, the consent management system will be voluntary to join, which poses a problem of whether it should be regulated through the existing acts.

The complication arises from the implementation of the existing laws and regulations, as the experts emphasized. The reason is that the data protection conditions are becoming more stringent as the number of data breach incidents increase. Even if the requirements are precise, the control over the fulfilment of obligations is not sufficient. In this regard, the clear description, the scope and purpose of data processing are among the main challenges. As mentioned in Chapter 2, the GDPR includes exact requirements for consent, such as unambiguity and specificity for the intended purpose. Nevertheless, in some cases, these requirements can also be covered through "*blanket"* and *"broad"* consents. According to Wendler (2013), blanket consent refers to providing personal information unrestrictedly, and broad or general consent refers to sharing personal

information for a wide range of purposes. For instance, interviewees repeatedly mention Estonian Biobank (EstBB) that collects the research participants' genomes through broad informed consent. It raises the question of whether the government should allow to acquire general consents to the private sector service providers or enforce policies to limit the reach of the purpose.

As the literature displays and the interviewees confirm, it is a common tendency that while giving consent electronically, people do not thoroughly read the privacy policies or T&C behind their permits (Obar & Oeldorf-Hirsch, 2018) due to the absence of face-to-face interaction and the complex language of these statements. The Special Barometer 487a survey (European Commission, 2019) displays that only 13% of the respondents read privacy and purpose policies. The others either skip or partially read them primarily due to the complexity or lengthiness of the statements. Pattinson, Chen, & Basu (2020) argue that this factor does not only prevent data subjects from making decisions independently but also leaves them unaware of the full or partial transfer of responsibilities and legal obligations. In this case, as Bonnici and Coles-Kemp (2010) state and interview results confirm, only giving consent does not guarantee data subjects' understanding nor make the service provider compliant with the data protection regulations. Senior Legal Expert indicates that comprehending for what reason consent is requested and having the choice to accept or deny the request accordingly are the main conditions for the consent to be informed. Thus, the lack of understanding of the scope and purpose of consent restricts data subjects to exercise autonomous decision-making, making the consent invalid as per the GDPR requirements.

Chief Legal Officer claims that technological solutions solely cannot build the "data ownership" mindset among data subjects. Considering this fact, one way to assist people in making autonomous yet correct decisions is public awareness-rising on data privacy and protection, data processing, the risks of personal data sharing with untrusted parties, and the opportunities. Nevertheless, the issue here is that the government cannot entirely ensure that ordinary people read as well as understand the terms of service, associated risks, and potential consequences of personal data sharing, which are the basic informed consent requirements. It is also indicated in the Consent Service Analysis report (Nõusolekuteenuse analüüs, 2021) that currently, no evidence supports the fact that a person develops a habit of being aware of the issues related to the processing of their data in data-based services after continuous usage. In this regard, the Consent analysis report

(2021) specifies that a clear and standardized consent form for data users will address this issue. However, it should be considered whether this "one-size-fits-all" solution will enable every data user to explain their purposes plainly.

The interviewees also discuss the division of responsibilities on the protection of shared personal data and the purpose statements that would be displayed to data subjects. The problem might occur if companies process the personal data for other purposes than intended after the public authorities approve their safety and data subjects provide consent. This incident cannot be easily or promptly detected by the government or data subjects; therefore, people will lose their trust in the consent service and the involved parties when revealed. The absence of a proper tracking record of the data collection and processing in the private companies also make the situation unfavourable for the government to take responsibility.

Technological and organizational challenges have been discussed less compared to the obstacles from the legal aspect. Based on the experts' opinions, it can be concluded that minor technological challenges can be encountered during the implementation of the consent management system if the fundamental infrastructure is in place. It is also applicable from the perspective of system security. Nonetheless, the information security principles – confidentiality, integrity, and availability (CIA) must be ensured to provide the highest security to the new platform. On the contrary to the literature, interviewees do not mention the "gatekeeper" role of informed consent mechanisms in terms of information security. Yet, the Consent Service Analysis report (Nõusolekuteenuse analüüs, 2021) indicates that data subjects have to authenticate themselves to have access to the consent management interface and prove being consentors. In addition, data users also have to authenticate themselves to verify that these companies are nationally registered. Both can be considered a part of information security measures.

Still, the report also displays information security and privacy among the risks associated with the consent service. As Head of Health Technology Division Hirv also approves, once the new service is provided, the possibility of the misuse of personal data will increase. New forces will emerge that will exploit the technology in a way that is not meant to. In this case, in most cyberattacks or other security incidents, the weak link is the person or user, not necessarily the system. In the context of this paper, it is highly related to data subjects' awareness about data privacy and protection regulations,

carefulness about personal data sharing. Thus, as the literature suggests, the consent management mechanisms themselves need to be protected via security layers.

In terms of organizational challenges, the experts emphasize change management and process adjustments. Sulistiyani and Susanto (2018) argue that the reason behind the failures of most e-government projects is unsuccessful change management. It includes changes starting from IT, business processes, and legislation to organizational structures and people. As discussed before, in Estonia, both the legal framework and the existing infrastructure allow the implementation of the consent management system without a need for fundamental changes. However, the process to identify who and when to provide or withdraw consent, by whom the permission is requested and whether the provided consent fulfils the GDPR conditions must be correctly defined and managed for the smooth business process. In this regard, Product Manager of Estfeed platform states that an effective logging solution should be added process-wise so that the logged activities such as provision and withdrawal of consents are not manipulated afterwards. Also, if the solution requires interoperability among various parties, the strategic plan, as well as budget allocation and communication regarding consent management, should be organized in a way that is suitable both for data controllers and data users. Finally, as a part of change management, both parties should be regularly trained to understand the GDPR personal data privacy and consent requirements to reduce human error to a minimum and increase the success rate of the project.

8 Summary and Conclusion

This chapter summarizes the key outcomes of the study and displays their relations with the defined research questions.

The first main research question is, “How can consent management help public sector organizations to adhere to data consent principles in the digital age?” To explore this question, firstly, the sub-question of “What are the main informed consent principles?” was discussed through the literature review. Self-governance, autonomous decision-making over the use of personal data through “opt-in” and “opt-out” choices were identified as the main principles of informed consent. Secondly, the sub-question of “How is consent reflected in the GDPR?” was answered by listing and analyzing articles and recitals about consent in the GDPR.

The second main research question was, “How important and urgent is the need to implement consent management in the public sector?” To answer this question, firstly, the sub-question of “What are the key benefits of consent management for governmental organizations” was discussed with the experts, as indicated in Chapter 7 and its sub-sections 7.1-7.5. Based on the expert opinions, it is concluded that consent management is an essential tool and necessary solution (1) to adhere to the informed consent principles and the data protection regulations while sharing personal data with the private sector companies, (2) to foster innovation in the country by allowing the private sector organizations to reuse high-quality personal data upon data subjects’ consents, and (3) to increase data controllers’ and individuals’ responsibilities over the use of personal data. The results also revealed that the implementation of consent management does not directly contribute to transparency since other criteria, such as the data and consent tracking possibilities and the user interface, should be in place as well. To identify the urgency, the sub-question of “How urgent is the need to implement consent management?” was discussed. The interview outcomes illustrated that it is somehow urgent and not critical to have a consent management system and, overall, a consent service since it is not a critical but a voluntary and convenience public service.

The final research question was “How can consent management be practised in the public sector?” To find out an answer to this question, firstly, the existing technological solutions for consent management in Estonia were identified in Chapter 5. Followingly, the

ongoing governmental project of “Consent service” for the consent-based personal data sharing between public and private sectors was described based on the interviews with the governmental officials as well as the official documents on the service analysis. The second sub-question on implementation challenges was explored through expert interviews. Three main challenges – legal, technological, and organizational challenges were identified. The data analysis illustrated that legal aspects need to be considered in the first place to implement consent management in public organizations. Technology is usually not a challenge in countries with a well-functioning e-governance ecosystem like in Estonia. However, information security must be ensured, and the CMP must meet the security standards. Finally, organizational challenges, including change management and process unfit, were discussed the least. Nevertheless, these challenges should not be undermined since the successful implementation of the CMP requires a harmonized processes and adaptation to the advanced-level reuse of personal data countrywide.

8.1 Recommendations for Further Research

This study revealed the potential benefits and challenging parts of the implementation of the consent service pilot project. Thus, as the first research area after the full-scale implementation of the consent management system, the impact assessment of the consent service on Estonian citizens and the private sector development is strongly recommended. Besides, since the current project targets the personal data transfer between public and private sector organizations in Estonia, the focus of this thesis is on the Estonian case. As a future study, the possibility and potential advantages of cross-border consent-based data sharing can be adequately examined to leverage the benefit of the consent management solution. Finally, the question of how the indicated challenges can be effectively overcome needs to find the answer to minimize the risk management failures during the project implementation.

References

European Parliamentary Assembly. (1998). *Resolution 1165 (1998) Final version.* Retrieved from Parliamentary Assembly: http://assembly.coe.int/nw/xml/XRef/XrefXML2HTML-en.asp?fileid=16641&lang%20=en.

Alderson, P., & Goodey, C. (1998). Theories of Consent. *BMJ Clinical Research, 317*, 1313-1315. doi:10.1136/bmj.317.7168.1313

Bialke, M., Bahls, T., Geidal, L., & et al. (2018). MAGIC: once upon a time in consent management—a FHIR® tale. *Journal of Translational Medicine , 16*. doi:10.1186/s12967-018-1631-3

Bonnici, C. J. (2013). An extended conceptual model of consent for information systems. *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems*, (pp. 149-154). doi:10.1109/CBMS.2013.6627780.

Bonnici, C. J., & Coles-Kemp, L. (2010). Principled Electronic Consent Management. A Preliminary Research Framework. *International Conference on Emerging Security Technologies* (pp. 119-123). IEEE.

Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law and Security Review, 35*(5), 1-17. doi:10.1016/j.clsr.2019.03.008

Breen, S., Ouazzane, K., & Patel, P. (2020). GDPR: Is your consent valid? *Business Information Review, 37*(1), 19-24. doi:doi.org/10.1177/0266382120903254

Buyle, R., Taelman, R., Mostaert, K., Joris, G., Mannens, E., Verborgh, R., & Berners-Lee, T. (2020). Streamlining Governmental Processes by Putting Citizens in Control of Their Personal Data. *6th International Conference, EGOSE 2019*, 346-359. doi:https://doi.org/10.1007/978-3-030-39296-3_26

Clarke, R. (2002). eConsent: A Critical Element of Trust in eBusiness. *Proceedings of BLED 2002 - the 15th BLED eConference.* AIS.

Clarke, R. (2006, August 7). *What's 'Privacy'?* Retrieved from Rogerclarke.com: http://www.rogerclarke.com/DV/Privacy.html

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, *26*(2), 120-123.

Coeira, E., & Clarke, R. (2004). e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment. *Journal of the American Medical Informatics Association, 11*(2), 129-140. doi:10.1197/jamia.M1480

(2021). *Consent service analysis: Summary.*

Council of Europe. (n.d.). *12 Principles of Good Governance*. Retrieved from Council of Europe Portal: https://www.coe.int/en/web/good-governance/12-principles#{%2225565951%22:[3]}

Creswell, J. W., Hanson, W. E., Clark, V. L., & Morales, A. (2007). Qualitative Research Designs: Selection and Implementation. *THE COUNSELING PSYCHOLOGIST, 35*(2), 236-264. doi:10.1177/0011000006287390

Draheim, D. (2020). On Architecture of e-Government Ecosystems: from e-Services to e-Participation. *iiWAS '20: Proceedings of the 22nd International Conference on Information Integration and Web-based Applications & Services* (pp. 3-10). New York: Association for Computing Machinery. doi:10.1145/3428757.3429972

eHealth Task Force. (2015). *Estonian eHealth Strategic Development Plan 2020.* Retrieved from https://www.sm.ee/et/eesti-e-tervise-strateegia

Erlenheim, R., Draheim, D., & Taveter, K. (2020). Identifying design principles for proactive services through systematically understanding the reactivity-proactivity spectrum. *ICEGOV 2020: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 452–458). Association for Computing Machinery. doi:10.1145/3428502.3428572

European Comission. (2017). *European Interoperability Framework: Promoting seamless services and data flows for European public administrations.* doi:10.2799/78681

European Comission. (2020). *Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). COM/2020/767 final.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

European Commission. (2018). *The GDPR: new opportunities, new obligations: What every business needs to know about the EU's General Data Protection Regulation.* Retrieved from https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf

European Commission. (2019). *Digital Government Factsheet 2019: Estonia.* Retrieved from https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf

European Commission. (2019). *Special Eurobarometer 487a - The General Data Protection Regulation.* doi:10.2838/579882

European Commission. (2019). *Special Eurobarometer 487a - The General Data Protection Regulation.* doi:10.2838/579882

European Commission. (2021). *Shaping Europe's digital future: A European Strategy for Data*. Retrieved from Digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission. (n.d.). *What constitutes data processing?* Retrieved from European Comission: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Board. (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR.* Retrieved from https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

European Data Protection Supervisor. (n.d.). *Rights of the Individual*. Retrieved 2021, from edps.europa.eu: https://edps.europa.eu/data-protection/our-work/subjects/rights-individual_en

European Parliament and Council of European Union. (2016). *Regulation (EU) 2016/679.* Retrieved from GDPR.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

European Parliament and Council of European Union. (2016). Regulation (EU) 2016/679. Article 4. Definitions. *Official Journal of the European Union*. Retrieved from https://gdpr.eu/article-4-definitions/

European Union Agency for Cybersecurity . (2020). *ENISA Threat Landscape 2020 - Main incidents in the EU and worldwide.* Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

Faden, R. R., & Beauchamp, T. L. (1986). *A History and Theory of Consent.* New York: OXFORD UNIVERSITY PRESS. doi: ISBN 0-19-503686-7

Fatema, K., Hadziselimovic, E., Pandit, H., Debruyne, C., Lewis, D., & O'Sullivan, D. (2017). Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model. *PrivOn@ISWC*, 1-15.

Friedman, B., Felten, E., & Millett, L. I. (2000). Informed Consent Online: A Conceptual Modeland Design Principles. *CSE Technical Report*. Retrieved from https://dada.cs.washington.edu/research/tr/2000/12/UW-CSE-00-12-02.pdf

Gautrais, V. (2004). The Colour of E-Consent. *University of Ottawa Law & Technology Journal, 1*, 189.

Genestier, P., Zouarhi, S., Limeux, P., Excoffier, D., Prola, A., Sandon, S., & Temerson, J.-M. (2017). Blockchain for Consent Management in the eHealth Environment: A Nugget for Privacy and Security Challenges. *Journal of the International Society for Telemedicine and eHealth, 5*.

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly, 26*(1), 75-81. Retrieved from 10.1016/j.giq.2008.03.003Get rights and content

Heinze, O., Birkle, M., Köster, L., & Bergh, B. (2011). Architecture of a consent management suite and integration into IHE-based regional health information networks;. *BMC Medical Informatics and Decision Making, 11*(58). doi:10.1186/1472-6947-11-58

Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer law & security review, 29*(5), 509-521. doi:10.1016/j.clsr.2013.07.004

Hoeyer, K., & Hogle, L. F. (2014). Informed Consent: The Politics of Intent and Practice in Medical Research Ethics. *Annual Review of Anthropology, 43*, 347-362. doi:10.1146/annurev-anthro-102313-030413

Information Commissioner's Office (ICO.). (2021). *Principle (c): Data minimisation*. Retrieved from ico.org.uk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

Information Commissioner's Office. (n.d.). *Controllers and processors*. Retrieved 2021, from ico.org.uk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/#2

Iwaya, L. H., Li, J., Fischer-Hübner, S., Åhlfeldt, R.-M., & Martucci, L. A. (2019). E-Consent for Data Privacy: Consent Management for Mobile Health Technologies in Public Health Surveys and Disease Surveillance. In L. Ohno-Machado, & B. Séroussi (Eds.), *MEDINFO 2019: Health and Wellbeing e-Networks for All* (Vol. 264, pp. 1223 - 1227). IOS Press. doi:10.3233/SHTI190421

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly, 37*(3). doi:10.1016/j.giq.2020.101493

Junginger, S. (2018). Inquiring, Inventing and Integrating: Applying Human-Centered Design to the Challenges of Future Government. *eJournal of eDemocracy and Open Government (JeDEM), 10*(2), 23-32. doi:https://doi.org/10.29379/jedem.v10i2.520

Kakarlapudi , P. V., & Mahmoud, Q. H. (2021). A Systematic Review of Blockchain for Consent Management. *Healthcare, 9*(2). doi:10.3390/healthcare9020137

Landau, S. (2015). Control use of data to protect privacy. *Science, 347*(6221), 504-506. doi:10.1126/science.aaa4961

Larrucea, X., Moffie, M., Asaf, S., & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Computer Standards & Interfaces, 69*. doi:10.1016/j.csi.2019.103408

Laurent, M., Leneutre, J., Chabridon, S., & Laaouane, I. (2019). Authenticated and Privacy-Preserving Consent Management in the Internet of Things. *Procedia Computer Science, 151*, pp. 256-263. Leuven. doi:https://doi.org/10.1016/j.procs.2019.04.037

Lemmens, T. (2014). Informed consent. *Routledge Handbook of Medical Law and Ethics*, 27-51. doi:10.4324/9780203796184.ch3

Manson, N. C., & O'Neill, O. (2007). *Rethinking Informed Consent in Bioethics.* Cambridge University Press. doi:10.1017/CBO9780511814600

Misuraca, G., Alfano, G., & Viscusi, G. (2011). Interoperability Challenges for ICT-enabled Governance: Towards a pan-European Conceptual Framework. *Journal of Theoretical and Applied Electronic Commerce Research, 6*(1), 95-111. doi: 10.4067/S0718-18762011000100007

Mureddu, F., Schmeling, J., & Kanellou, E. (2020). Research challenges for the use of big data in policy-making. *Transforming Government: People, Process and Policy, 14*(4), 593-604. doi:10.1108/TG-08-2019-0082

(2021). *Nõusolekuteenuse analüüs.*

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128-147. doi:https://doi.org/10.1080/1369118X.2018.1486870

OECD. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from oecd.org: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD. (2016). *MANAGING DIGITAL SECURITY AND PRIVACY RISK: Background report for Ministerial Panel 3.2.* OECD Secretariat. Retrieved from https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En

OECD. (2017). Trust and Public Policy. How Better Governance Can Help Rebuild Public Trust. *OECD Public Governance Reviews*. Retrieved from https://www.oecd-ilibrary.org/governance/trust-and-public-policy_9789264268920-en

OECD. (2019). *Measuring Digital Security Risk Management Practices in Businesses. OECD Digital Economy Papers.* Retrieved from https://www.oecd-ilibrary.org/docserver/7b93c1f1-en.pdf

Pattinson, J.-A., Chen, H., & Basu, S. (2020). Legal issues in automated vehicles: critically considering the potential role of consent and interactive digital interfaces. *Humanities and Social Sciences Communications, 7*(153). Retrieved from https://www.nature.com/articles/s41599-020-00644-2

Peixoto, T., & Fox, J. (2016). When Does ICT-Enabled Citizen Voice Lead to Government Responsiveness? *IDS Bulletin: Opening Governance, 47*(1), 23-40. doi:10.19088/1968-2016.104

Pöhls, H. C. (2008). Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data. In L. Chen, M. D. Ryan, & G. Wang (Eds.), *Information and Communications Security. ICICS 2008. Lecture Notes in Computer Science* (Vol. 5308, pp. 279–293). Berlin, Heidelberg: Springer. doi:10.1007/978-3-540-88625-9_19

Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health and Technology, 7*, 441-451. doi:I 10.1007/s12553-017-0195-1

Raab, C. (2012). The Meaning of 'Accountability' in the Information Privacy Context. In D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, & H. Postigo, *Managing Privacy through Accountability* (1 ed., pp. 15-31). Palgrave Macmillan. doi: 10.1057/9781137032225

Rantos, K., Drosatos, G., Kristas, A., Ilioudis, C., Papanikolaou, A., & Filippidis, A. P. (2019). A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem. *Security and Communication Networks, 2019*. doi:10.1155/2019/1431578

Rau, H., Geidel, L., Bialke, M., Blumentritt, A., Langanke, M., Liedtke, W., . . . Hofmann, W. (2020). The generic Informed Consent Service gICS®: implementation and benefts of a modular consent software tool to master the challenge of electronic consent management in research. *Journal of Translational Medicine, 18*(287), 2020. doi:10.1186/s12967-020-02457-y

Risling, T., Martinez, J., Young, J., & Thorp-Froslie, N. (2018). Defining Empowerment and Supporting Engagement Using Patient Views From the Citizen Health Information Portal: Qualitative Study. *JMIR MEDICAL INFORMATICS, 6*(3). doi:10.2196/medinform.8828

Rissanen, T. (2016). Public Online Services at the Age of MyData: a New Approach to Personal Data Management in Finland. *Proceedings of the open Identity Summit* (pp. 81-92). Lecture Notes in Informatics P-264, Gesellschaft für Informatik.

Sulistiyani, E., & Susanto, T. D. (2018). Change Management Methodology for e-Government Project in Developing Countries: a Conceptual Model. *Third International Conference on Informatics and Computing (ICIC)* (pp. 1-5). IEEE. doi:10.1109/IAC.2018.8780500

Task Force. (2015). *Estonian eHealth Strategic Development Plan 2020.* Retrieved from https://www.sm.ee/et/eesti-e-tervise-strateegia

Tehnopol. (2019). *Data-based personal healthcare – a distant future or today's reality?* Retrieved from Tehnopol.ee: https://www.tehnopol.ee/en/andmepohine-personaalne-tervisehoid-kauge-tulevik-voi-tanane-reaalsus/

The Belmont Report: Ethical Principles and Guidelines for the Protection of Human. (1979).

Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W., Taira, N., Obi, T., & Ohyama, N. (2020). Patient Consent Management by a Purpose-Based Consent Model for Electronic Health Record Based on Blockchain Technology. *Healthcare Informatics Research, 26*(4), 265-273. doi:10.4258/hir.2020.26.4.265

United Nations. (2020). *E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development.* New York. Retrieved from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

United Nations. (n.d.). *What is the Rule of Law*. Retrieved from UN.org: https://www.un.org/ruleoflaw/what-is-the-rule-of-law/

Van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Data Protection on Move. Current Developments in ICT and Privacy/Data Protection* (pp. 194-212). Springer Science + Media. doi:10.1007/978-94-017-7376-8_8

Van Ooijen, C., Ubaldi, B., & Welby, B. (2019). *A data-driven public sector: Enabling the strategic use of data for productive, inclusive, and trustworthy governance.* OECD, Paris. Retrieved from https://www.oecd-ilibrary.org/governance/a-data-driven-public-sector_09ab162c-en

Velmovitsky, E., Miranda, P. A., Vaillancourt, H., Donovska, T., Teague, J., & Morita, P. P. (2020). A Blockchain-Based Consent Platform for Active Assisted Living: Modeling Study and Conceptual Framework. *JOURNAL OF MEDICAL INTERNET RESEARCH, 4;22*(12). doi:10.2196/20832

Weber-Janke, J. H., & Obry, C. (2011). Protecting privacy during peer-to-peer exchange of medical documents. *Information Systems Frontiers , 14*, 87-104. doi:DOI 10.1007/s10796-011-9304-2

Wendler, D. (2013). Broad versus Blanket Consent for Research with Human Biological Samples. *43*(5), 3-4. doi:10.1002/hast.200

What are the GDPR consent requirements? (n.d.). Retrieved from GDPR.eu: https://gdpr.eu/gdpr-consent-requirements/

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6 ed.). SAGE Publications.

Yu, B., Wijesekera, D., & Costa, P. (2014). Consent-Based Workflow Control in EMRs. *Procedia Technology, 16*, 1434 – 1445. doi:10.1016/j.protcy.2014.10.163

Zazaza, L., Venter, H. S., & Sibiya, G. (2019). The Current State of Electronic Consent Systems in e-Health for Privacy Preservation. In L. M. Venter H. (Ed.), *Information Security. ISSA 2018. Communications in Computer and Information Science* (Vol. 973, pp. 76-88). doi:https://doi.org/10.1007/978-3-030-11407-7_6

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Tamara Aslanova

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "The Role and Importance of Consent Management in Public Organizations in the Digital Age: Case on Estonia" , supervised by Dirk Draheim, Kevin Tammearu, and Sidra Azmat Butt.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

09.05.2021

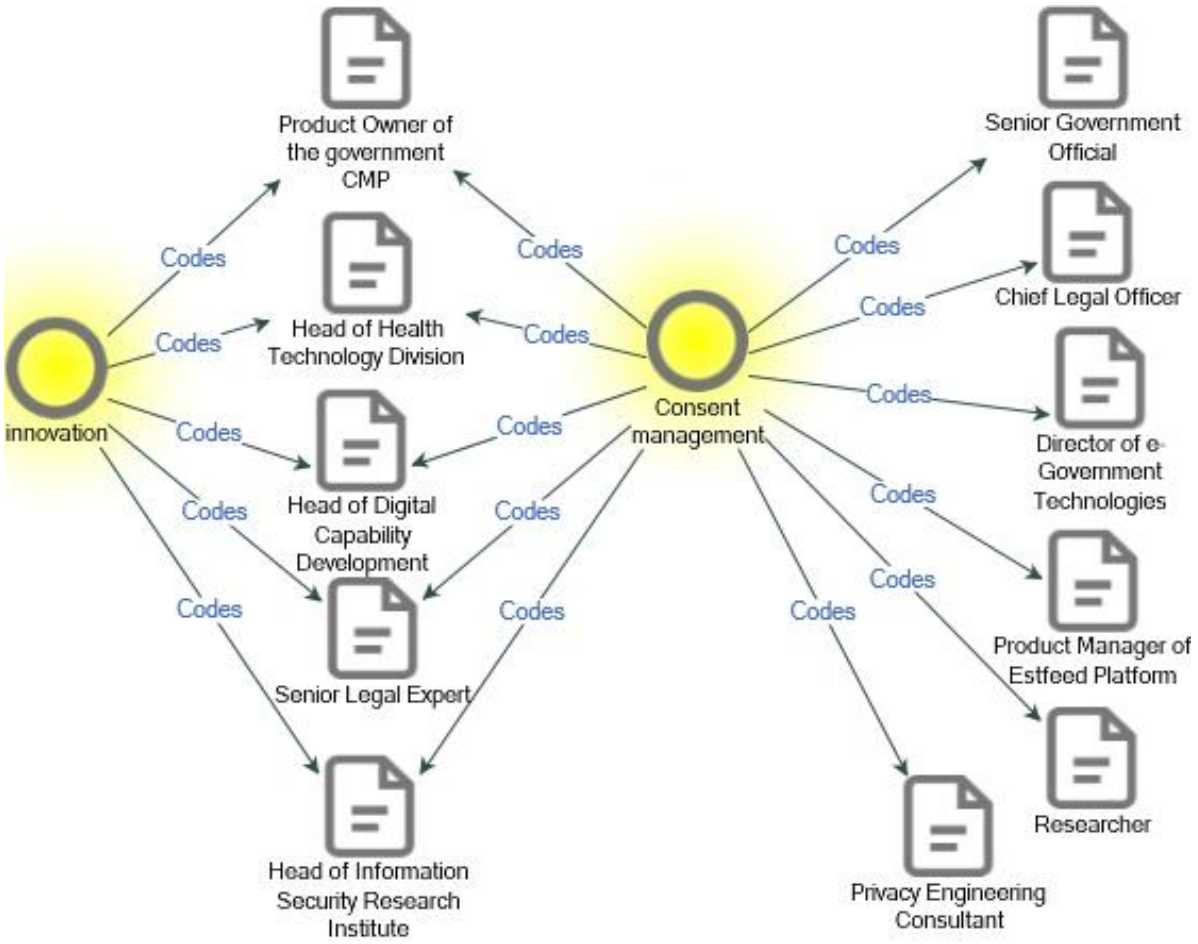
1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

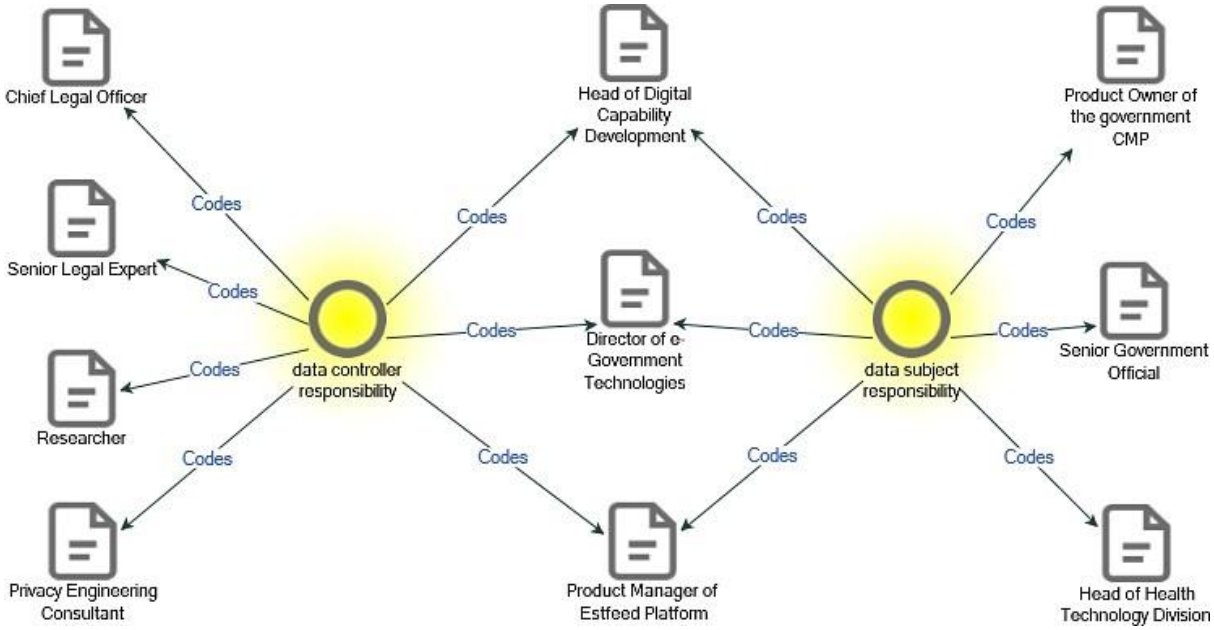
Appendix 2 – Interview questions

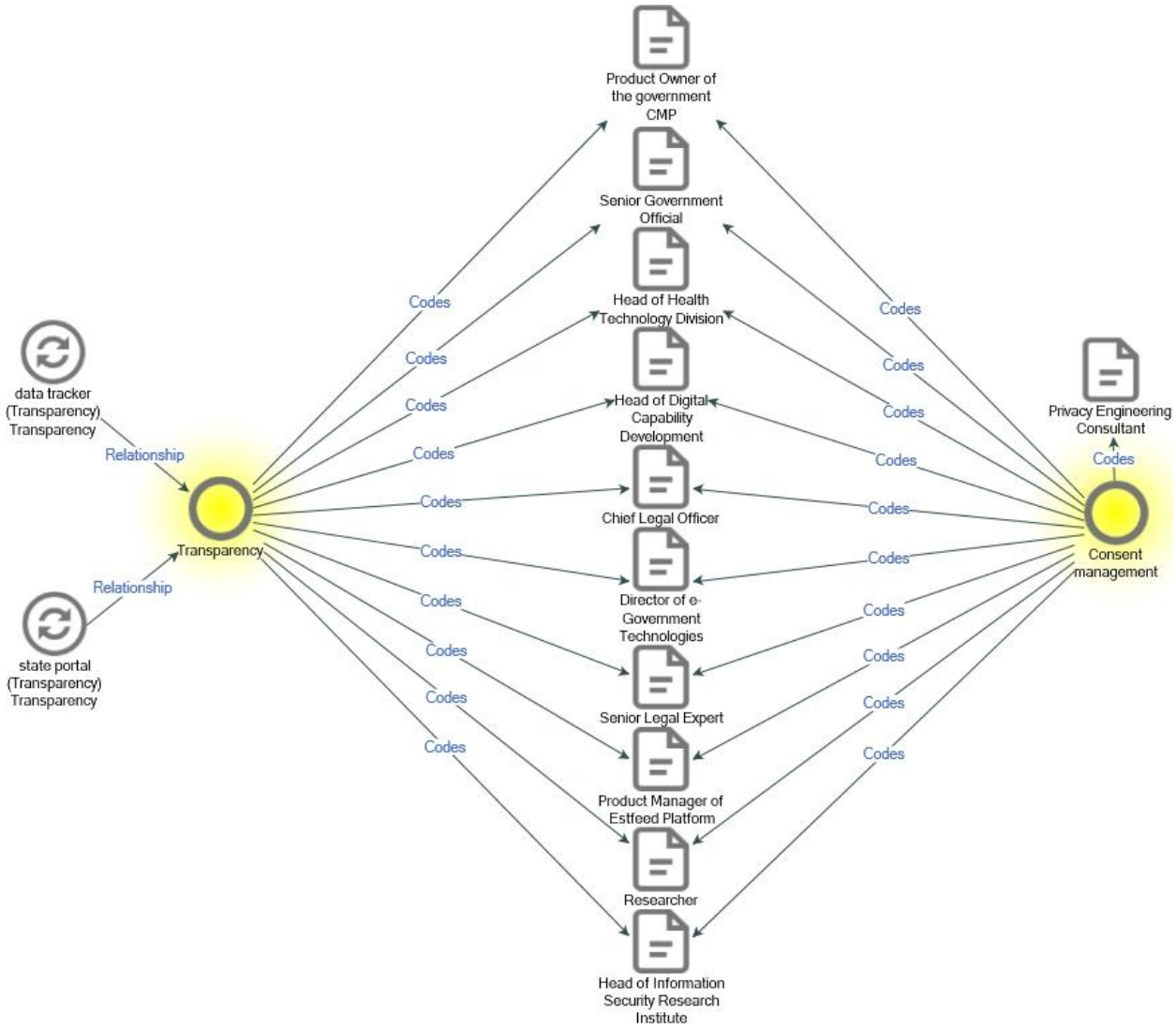
1. As data controllers, what regulations and legal basis does the Estonian government refer to while handling the personal data?
   - Why consent is not the main legal basis?
2. How is consent understood in legal terms?
   - Are there any moral bases that led to include consent-related articles to the law? For instance, human dignity, self-determination, autonomy in decision-making?
3. How would you define consent management in relation to personal data in the context of public sector?
4. Is there a necessity to have more strict or detailed laws or regulations that oblige consent management for data controllers and processors? For instance, should the law say that whenever data is shared with the third party, the data subjects must provide the consent or at least, they should be informed?
5. Are there any consent management solution/platform/system already implemented or are planned to be implemented in Estonia?
   - If yes, describe (why it was agreed to implement this project? Who are the beneficiaries? What are the expected benefits and impact of the project?)
6. Studies suggest several important aspects of informed consent, which can also be potential drivers for the consent management in public sector. The first one is compliance with legal obligations as well as the avoidance of unlawful action. How much do you agree with this claim? Do you think it the role of consent in terms of compliance also adds to accountability of data controllers over the collected and stored personal data?
7. How can consent acquisition contribute to the trust and transparency of the public organizations?
8. Can consent management contribute to the data protection and information security? If yes, how?
9. There is also mentioning of individual autonomy over decision-making and having control over personal data through consent that can enhance the public trust. Do you think it can be a driver for public organizations to manage consent as well?

10. Interoperability and data exchange infrastructures are the inseparable parts of Estonian e-government system. Do Estonian public organizations acquire consent or inform citizens and manage it for service provision or data exchange with other departments?
    - (if yes)
        1. Why and how does this process happen?
        2. Can individuals also see proof that they have explicit consent?
    - (if no)
        1. What is the reason?
        2. Are citizens satisfied with the current situation?
11. Do you think generally, increasing use of interoperability solutions might necessitate or trigger the consent management for public organizations?
12. Overall, based on out discussion, how important and urgent is the need for implementation of consent management?
13. What barriers or challenges might arise for public organizations in terms of the implementation of consent management system?

Appendix 3 – Role and importance of consent management






Product Owner of the government CMP
Senior Government Official
Head of Health Technology Division
Head of Digital Capability Development
Chief Legal Officer
Director of e-Government Technologies
Senior Legal Expert
Product Manager of Estfeed Platform
Researcher
Head of Information Security Research Institute
data tracker (Transparency) Transparency
state portal (Transparency) Transparency
Relationship
Relationship
Transparency
Consent management
Privacy Engineering Consultant
Codes

Appendix 4 – Implementation challenges