TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Diana Müürsepp 232635IVGM

The Impact of GDPR on User-Centred Design in Estonian Public Sector E-Services: An Organisational Case Study

Master's Thesis

Supervisor: Eric Blake Jackson
PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Diana Müürsepp 232635IVGM

IKÜM-i mõju kasutajakesksele disainile Eesti avaliku sektori e-teenustes: organisatsioonipõhine juhtumiuuring

Magistritöö

Juhendaja: Eric Blake Jackson
PhD

Tallinn 2025

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: Diana Müürsepp

12.05.2025

Abstract

This thesis explores how the General Data Protection Regulation (GDPR) is interpreted and applied in the context of user-centred digital service development within one Estonian public sector organisation responsible for multiple e-services. Through a qualitative case study, drawing on semi-structured interviews with analysts, product owners and legal advisors from different teams, the research investigates how GDPR influences design decisions, what kinds of tensions arise between legal and user-centred design (UCD) priorities and how these tensions are managed in everyday development work.

Based on the findings, the author proposes several practical recommendations to improve cross-role collaboration, clarify internal responsibilities and support proportionate and constructive approaches to data protection. The study contributes to the innovative field of digital governance by offering a grounded account of how regulation shapes public service design in practice and identifies where improvements are needed to better align compliance with user needs.

Keywords: GDPR, Data Protection, User-Centred Design, Public Digital Services

This thesis is written in English and is 64 pages long, including 7 chapters, 2 figures and 3 tables.

Annotatsioon

IKÜM-i mõju kasutajakesksele disainile Eesti avaliku sektori e-teenustes: organisatsioonipõhine juhtumiuuring

Käesolev magistritöö uurib, kuidas isikuandmete kaitse üldmäärust (IKÜM) tõlgendatakse ja rakendatakse kasutajakesksete e-teenuste arendamise kontekstis ühes Eesti avaliku sektori asutuses, mis muuhulgas arendab mitmeid e-teenuseid. Kvalitatiivse juhtumiuuringu meetodi abil, viies läbi poolstruktureeritud intervjuusid süsteemi- ja ärianalüütikute, tootejuhtide ja juristidega eri arendustiimidest, analüüsib autor, kuidas IKÜM mõjutab e-teenuse disainivalikuid, millised pinged tekivad õigusalaste ja kasutajakesksete eesmärkide vahel ning kuidas neid ebakõlasid igapäevases arendustöös hallatakse.

Antud töö annab ülevaate andmekaitsealase regulatsiooni mõjust avalike e-teenuste disainipraktikale ning toob esile, milliseid võimalusi nähakse kasutajakesksuse ja õigusnõuete parema kooskõla saavutamiseks. Analüüsi tulemuste põhjal teeb autor praktilised ettepanekud rollidevahelise koostöö parandamiseks, sisemiste vastutusvaldkondade selgitamiseks ning proportsionaalse ja konstruktiivse andmekaitse toetamiseks teenusedisaini kontekstis.

Märksõnad: IKÜM, Andmekaitse, Kasutajakeskne disain, Avalikud digiteenused

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 64 leheküljel, 7 peatükki, 2 joonist, 3 tabelit.

List of abbreviations and terms

AKI	Data Protection Authority (Estonian)
DPA	Data Protection Authority
DPI	Data Protection Inspectorate
DPO	Data Protection Officer
EEA	European Economic Area
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
HCD	Human-Centred Design
HCI	Human-Computer Interaction
ISO	International Organization for Standardization
IS	Information Systems
IT	Information Technology
MKM	Ministry of Economic Affairs (Estonian)
OECD	Organisation for Economic Co-operation and Development
RIA	Information System Authority (Estonian)
RQ	Research Question
SQ	Sub-question
TA	Thematic Analysis
TFEU	Treaty of the Functioning of The European Union
UCD	User-Centred Design
UX	User Experience

Table of contents

List of figures

List of tables

1 Introduction

Digital transformation has fundamentally reshaped how public sector delivers services and interacts with citizens. As governance is becoming more automated across the European Union (EU), member states are increasingly expected to provide seamless, secure and user-friendly e-services that improve public sector effectiveness, transparency and citizen trust (OECD, 2024). Estonia, often regarded as a country at the forefront of digital governance domain, exemplifies this shift. With a highly digitized state infrastructure – including universal digital identity, interoperable data-exchange platforms and a wide range of online public services – the government's digital presence has become a strategic and vital aspect of the nation's daily operations (Margetts & Naumann, 2015; Vassil, 2016).

However, public digital service delivery in the EU is not merely a technical or design challenge – it is also a deeply legal one. Estonia, like all member states, must develop its e-services in compliance with supranational EU legal requirements, respecting obligations regarding privacy and security (European Commission, 2016; TFEU, art. 288). Among the most influential of these is the General Data Protection Regulation (GDPR), which establishes binding requirements for how personal data must be collected, processed, stored, accessed and deleted. The GDPR not only governs back-end data practices but also has implications for how information is presented to users, how consent is obtained and how privacy is integrated into design and operation of digital services (Regulation (EU) 2016/679, 2016).

Digitalisation in the public sector has thus created a complex environment where technological innovation, legal accountability and citizen experience must be balanced, when creation of public e-service takes place. While policy reports and academic studies have increasingly recognised the importance of user-centred design (UCD) in public service development and delivery (OECD, 2020; European Commission, 2022; Kotamraju & Van Der Geest, 2012; Welby & Tan, 2022), there seems to be limited understanding, how this design logic is reconciled with the procedural and legal challenges faced by public organisations responsible for developing these services (França & Mont'Alvão, 2024).

This thesis explores this phenomenon through institutional logics theory, which provides a lens to examine how systems, practices and values shape organisational decisions (Thornton et al., 2012). The study adopts two main logics:

- Legal compliance (GDPR-driven) – a logic that involves organisational responsibility to define, structure and execute mechanisms that fulfil legal obligations (Lanamäki et al., 2025);
- User-centred design – a logic that prioritises user needs through iterative, user-involved design processes (Chammas et al., 2015).

While these two logics are foundational when considered independently, they may create conflicts and uncertainty when coexisting within one organisation. To analyse these dynamics, the study applies the multiple institutional logics framework, which explains how the centrality and compatibility of coexisting logics shape organisation's outcomes (Besharov & Smith, 2014). By focusing on how these logics intersect in Estonia's advanced public digital service design within specific organisational setting, this research seeks to contribute both to scholarly debates on operalisation of legal obligations and to practical obstacles encountered by public service professionals working at the intersection of law and e-service design.

In accordance with good academic practice, the author acknowledges limited use of ChatGPT 4o assistance during the thesis writing process, used as a supportive tool to refine research focus, improve translations and grammar. No AI-based content has been included without extensive revision to ensure academic integrity (OpenAI, 2025).

1.1 Objectives of the Study

This research seeks to explore how legal obligations drawn from General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679, 2016) are understood, interpreted and operationalised by public sector professionals during the early stages of digital service design. Accordingly, the research examines how GDPR regulatory demands are transformed into concrete service design decisions within the Estonian national context.

The study pursues the four main objectives:

1. To explore how public sector professionals interpret and integrate GDPR requirements into design of public e-services;
2. To analyse how organisational processes influence the operationalisation of these requirements in practice;
3. To identify the challenges, tensions and mitigation strategies that arise when balancing GDPR obligations with user-centred design principles;
4. To develop practical recommendations to support the creation of GDPR-compliant and user-centred public digital services.

Through a qualitative case study approach, research is set to contribute both to theoretical debates on legal compliance in digital governance domain and to practical efforts aimed at improving the design and delivery of digital public services in compliance with EU data protection requirements.

1.2 Research Gap

Although GDPR has been widely studied from legal and policy perspectives, there is quite limited research on how its requirements are interpreted and operationalised in the design of public e-services – particularly at the level of citizen-facing environments. Existing studies tend to emphasize privacy awareness, user trust and regulatory compliance, but rarely explore how abstract legal principles like privacy, despite their importance, are translated into user-oriented design decisions within public services (França & Mont'Alvão, 2024).

To the best of current knowledge, there is no publicly available case study researches within the Estonian context, that examine how GDPR is interpreted and applied in day-to-day processes of public digital service design – particularly in its early stages, such as collecting information, prototyping, writing analysis, etc., where analysts, product owners, data protection specialists and other stakeholders must collaboratively transform legal norms into functional and user-friendly e-service. While this thesis is anchored by specific Estonian public sector organisation and four distinct e-services developed and provided by it, participants may reflect on a range of services they have worked on – the goal is not to analyse a single case of GDPR integration in isolation, but to use it as a reference point for understanding the general process and challenges, which arise due coexistence of different logics.

1.3 Research Questions

This research explores how the GDPR influences the design of Estonian public digital services. It examines how this EU regulation affects the ability to follow user-centred design principles. The objective is to understand how public organisations balance legal compliance with usability goals, what kinds of problems arise and what recommendations could be made to improve general practice in this area.

To achieve this objective, the following research questions (RQ) and sub-question (SQ) guide the study:

- **RQ1:** How are GDPR requirements interpreted into the design of Estonian public e-services?
    - **SQ1:** How do institutional and organisational processes influence the way GDPR is integrated into digital service development?

RQ1 investigates how GDPR's legal provisions are manifested into practice by the public sector actors working at the very core of service design. The focus is on how the regulation is perceived and applied within concrete organisational and design contexts, helping to reveal how legal meaning is negotiated internally, before interpreted in everyday e-service logics. SQ1 examines the institutional and organisational conditions under which these design decisions occur. It focuses on how organisational structures, workflows and interdepartmental relationships influence the interpretation and prioritisation of GDPR requirements during digital service development, revealing the main elements impacting the design outcome.

- **SQ2:** What kinds of tensions arise between GDPR compliance and user-centred design in Estonian public e-services?
    - **RQ2:** How are tensions between GDPR compliance and user-centred design managed in Estonian public e-services?

RQ2 investigates the kinds of conflicts that arise between data protection requirements and user-centred design goals in the development of public e-services. This includes tensions between legal obligations and usability principles, such as information visibility, simplicity, and accessibility. SQ2 complements this by exploring how public sector professionals respond to or manage these tensions in practice – whether through workarounds, compromises, or other strategies used to navigate conflicting expectations. Together, these questions aim to uncover both the nature of the challenges and the approaches currently used in everyday service design work.

- **RQ3:** What factors could support a more balanced integration of GDPR compliance within user-centred design of public e-services?

RQ3 takes a future-oriented goal to identify ideas proposed by the professionals that face such challenges that friction of those two logics creates – to manage the demands of GDPR compliance in alignment with user-centred design principles.

By addressing these three research questions and two sub-questions, the study aims to gain deeper understanding of how GDPR is interpreted and implemented in the design process of Estonian public digital services and how it affects user-centred design. Based on the outcome, the study also seeks to provide actionable recommendations for relevant public sector stakeholders. To ensure the trustworthiness and validity of the findings data triangulation is applied (Bans-Akutey, 2021), combining the analysis of legal and policy documents with semi-structured interviews conducted with public sector organisation actors involved in the development and design of user-centred digital services.

1.4 Justification of the Study

The GDPR (Regulation (EU) 2016/679, 2016) has been in force for several years meaning that today, it can be considered as well-established and widely understood EU regulatory framework. However, while its legal requirements seem clear, there is not enough research on how these obligations, interact with the practical goals of user-centred public service design. Little is known about how the public sector professionals interpret and implement GDPR requirements during the creation of e-services, which challenges arise and how they are managed – if possible, to manage.

This case study focuses on the Estonian context, offering an opportunity to examine how legal compliance challenges shape design choices in one of the most digitally advanced countries in Europe – a compelling and timely area for further academic investigation.

1.5 Motivation of the Study

This study is motivated by both academic and professional interests in how legal requirements and design principles intersect in the design of public digital services. The author's practical experience in the e-service development sphere has revealed how EU regulations change, limit, delay or sometimes even reverse design decisions that directly affect usability and accessibility of the services. These observations have raised pressing questions about how public sector employees – the ones at the core of the e-service development process – apply data protection requirements in ways that correspond to user needs and how they address obstacles that arise during this process. Moreover, the author feels a professional responsibility to bring recurring problems into public view – issues that continue but remain under-researched, and to propose applicable suggestions that contribute to improving of the situation in this domain.

1.6 Thesis Outline

This research has seven main chapters. Chapter 1 includes the introduction, objectives, questions, justification and motivation of the study. Chapter 2 introduces the theoretical framework, drawing on institutional logic theory with particular attention to legal compliance and user-centred design. It also includes a subsection on the Multiple Institutional Logics Framework, which is used to analyse how these logics coexist and interact in practice. Chapter 3 introduces state of the art – a literature review combined with context on GDPR, EU and Estonian strategic policy frameworks, public e-service design and operationalisation of GDPR into design topics. Chapter 4 is about the research design and methodology, including data collection, analysis and ethical considerations section. Chapter 5 presents the empirical findings from the interviews. Chapter 6 discusses the results considering the theoretical framework, provides practical recommendations, acknowledges study's limitations and outlines suggestions for future research directions. Chapter 7 is the conclusion of this thesis.

2 Theoretical Framework

This chapter presents the theoretical foundation for analysing how GDPR is operationalized into design of digital public services. Because this research sits at the intersection multiple domains, it requires an interdisciplinary approach that can account for both formal rules and institutional-organisational interpretation. To address this need, the study adopts institutional logics theory, which provides a lens to understand how organisations respond to multiple – and sometimes competing – value system demands in complex institutional environments (Mountford & Cai, 2022; Saqib & Allen, 2024). More specifically, the study draws on multiple institutional logics' framework developed by Besharov & Smith (2014) – a tool for examining how different logics coexist and shape organisational outcomes.

2.1 Institutional Logics Theory

Institutional logics theory originates from sociological institutionalism, serving as an approach that connects and extends diverse social science perspectives to examine how cultural systems shape behaviour at the individual, organisational and societal-cultural levels (Thornton et al., 2015). The approach builds on a foundational work of Friedland and Alford (1991), who introduced that modern society is structured by multiple institutional orders, such as capitalism, state, democracy, family and religion. Each of these, along with newer institutional orders emerging today, has its own logic that can at times be contradictory with one another. According to Thornton, Ocasio and Lounsbury (2012), when a particular order becomes excessively dominant or detached in relation to others, it may signal systemic instability. However, the system may self-correct through the rebalancing of interdependencies between orders, acting as a feedback mechanism that supports institutional continuity (Thornton et al., 2012).

This research draws on these theoretical insights in the context of public sector digital service design, where institutional dynamics emerge not at the level of entire societal orders, but through specific organisational-level logics (Saqib & Allen, 2024). The study applies two such lenses:

- Legal compliance (GDPR-driven) – a logic that reflects an organisation's responsibility to guarantee upholding to legal and regulatory demands by defining, structuring and implementing mechanisms that fulfil formal obligations (Root, 2019; Lanamäki et al., 2025);
- User-Centred Design (UCD) – a logic of iterative, user-involved development that centers on understanding and responding to users' needs, goals and contexts to improve usability and experience (Chammas et al., 2015).

Institutional logics are understood as historically shaped, socially constructed systems of cultural meaning and material practices that guide how individuals and organisations interpret their environment, coordinate their activities and provide meaning to their behaviour over time. In this study, institutional logics theory is not used to categorise actions, but rather to interpret the underlying rationalities that inform how design decisions are justified, negotiated and sometimes questioned within public sector and data protection contexts (Thornton et al., 2012).

2.1.1 Legal Compliance as Logic

Public organisations are required to operate within the strict legal and regulatory boundaries that govern their respective domains – these obligations extend not only to day-to-day operations, but also to the design and use of the information systems (IS) that support them. In sectors where the legal framework plays a central role in defining institutional functions (e.g. public administration), compliance with regulations becomes more than a requirement; it becomes a fundamental principle for service delivery and system development (Turki & Bjekovic-Obradovic, 2010).

Legal compliance refers to implementation of processes and procedures designed to ensure alignment with government regulations and legal requirements (Claydon, 2013). Lanamäki et al. (2024) describe legal compliance as ''seldom straightforward, requiring interpretation before conceiving and designing mechanisms for compliance'' (p.1). In the context of this study, legal compliance is mainly influenced by the General Data Protection Regulation (GDPR), which outlines the requirements on the personal data must be handled (Regulation (EU) 2016/679, 2016).

Within the framework of institutional logics theory, legal compliance can be understood as an organisational-level logic insofar as it encompasses the regulative, normative and cultural-cognitive components that link it to broader concept of institutional order (Thornton et al., 2012; Saqib & Allen, 2024). As Berthod (2017) points out, organisations do not act in isolation or based solely on efficiency; instead, they respond to a complex web of external influences, such as legal obligations, cultural norms and stakeholder expectations. From this view, legal compliance to GDPR is not only a matter of operational necessity, but also a means of meeting institutional expectations.

In practice, this logic becomes visible in how organisations formalize processes such as data collection, consent handling and documentation, often prioritising legal defensibility over usability or flexibility (Veale & Binns, 2017; Utz et al., 2019; Regulation (EU) 2016/679, 2016).

2.1.2 User-Centred Design as Logic

User-Centred Design (UCD) refers to a systematic method for developing user-facing systems by involving actual or potential users and addressing their needs throughout the entire design process (Kotamraju & Van Der Geest, 2012). The term was originally introduced by Donald A. Norman (1986) and is now considered as one of the leading methodologies within Human-Computer interaction (HCI) field that focuses on dependability, usability and performance of forthcoming digital systems (Mithun & Yafooz, 2018).

A closely related term, Human-Centred Design (HCD), is defined by International Organisation of Standardization (ISO 9241-210:2019) as an ‘‘*approach to systems design and development that aims to make interactive systems more usable’’*, prioritising the application of not only usability, but also ergonomic principle**.** While these terms – UCD and HCD – are synonymous in practice, the ISO standard broadens the scope by highlighting the inclusion of all stakeholders affected – not just the end users (ISO 9241-210:2019). Within this broader domain, the concept of User Experience (UX) plays central role, referring to the full range of perceptions as well as emotions that occur prior to and furing system use, as well as feelings that follow the interaction (Chammas et al., 2015).

In this study, the UCD is treated as a logic that potentially conflicts with the obligation of legal compliance in e-service design. In practice, the UCD logic manifests in decisions concerning interface clarity, accessibility, ease and comfort of user interaction and the degree of user control – areas that may be affected by interpretations of the GDPR (Regulation (EU) 2016/679, 2016; Veale & Binns, 2017; Utz et al., 2019; ISO 9241-210:2019). This logic-framing enables a deep analysis of how user-centred practices are either integrated into or sidelined by GDPR requirements, reflecting a degree of tension between competing institutional logics (Besharov & Smith, 2014).

2.2 Multiple Institutional Logics Framework

This study applies the framework of Multiple Institutional Logics by Besharov and Smith (2014) as a tool for examining how heterogeneous institutional logics coexist within organisations and shape their decisions and outcomes.

Besharov and Smith (2014) observe that the presence of multiple institutional logics can lead to very different outcomes. In some cases, it creates friction and disagreement, while in others, these logics are more seamlessly blended. As a result, logic multiplicity can either undermine organisational performance – potentially leading to stagnation and destabilisation – or enhance resilience and innovation when successfully integrated. The lack of clarity about the conditions under which these divergent outcomes occur was a key reason behind the authors' proposal of this framework (Besharov & Smith, 2014).

Besharov and Smith (2014) identify two critical dimensions for analysing this (Figure 1):

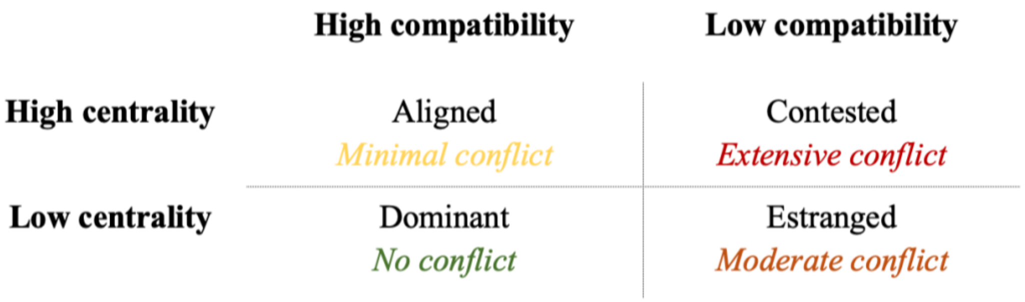
- Compatibility – defined as *"the extent to which the instantiations of multiple logics wihtin an organization imply consistent organizational actions";*
- Centrality – defined as *"the extent to which these logics manifest in core features that are central to organizational functioning''* (Besharov & Smith, 2014, p. 365).

Based on the degree of compatibility and centrality, organisations can be categorised into four ideal types (Figure 1.):

- Contested – combines highly central but conflicting logics, leading to ongoing inner turmoil, unclear priorities and possible instability within the organisation;
- Aligned – reflects high centrality and high compatibility, where different logics shape distinctly the core practices but support unified goals, resulting in minimal conflict;

- Estranged – characterised by low coherence and low centrality, where one dominant logic drives core activities, while conflicting peripheral logics create moderate internal tension; although conflict does not dominate, these organisations are still vulnerable;
- Dominant – includes high compatibility and low centrality, where one core logic shapes organisational functioning, while other compatible logics remain in the background; as logics align, internal conflict is absent and the organisation remains stable (Besharov & Smith, 2014).

These two dimension degrees and four organisational types are summarised in Figure 1.



	High compatibility	**Low compatibility**
High centrality	Aligned *Minimal conflict*	Contested *Extensive conflict*
Low centrality	Dominant *No conflict*	Estranged *Moderate conflict*

Figure 1. Types of Logic Multiplicity Within Organisations.

Source: Besharov & Smith (2014, p. 371)

This theoretical lens supports the study’s analysis by shifting attention to how logics are enacted in practice, offering a tool to examine how the compatibility and centrality of GDPR-driven legal compliance and user-centred design influence the development of digital public services (Besharov & Smith, 2014).

3 State of the Art

This chapter reviews academic and institutional literature relevant to the development of digital public services in the EU, with a special focus on Estonia. The review builds a conceptual as well as a contextual foundation for the study by examining how legal obligations arising from GDPR interact with e-service design approaches in public sector. Sources include academic research, EU legal documents and digital policy strategies, Estonian national digital agendas and public e-service design frameworks to define the operational and legal context in which digital services are developed.

3.1 The GDPR: Foundations and General Limitations

The GDPR (Regulation (EU) 2016/679, 2016) was adopted on 27th of April 2016 by the European Parliament and the Council of the European Union and enforced on 25th of May 2018, establishing a unified legal framework for personal data protection across the EU. It ensures EU citizens' rights over their personal data by establishing guidelines and obligations for its proper handling (Franke et al. 2024). The regulation was later incorporated into the European Economic Area (EEA), thereby extending its scope and ensuring unified standards across the EU and the members of the European Free Trade Association (EFTA) (EEA Joint Committee, 2018; Lourenço, 2019).

The regulation is directly applicable to all Member States and does not require national transposition – it has immediate effect and uniform application across EU (European Union, 2016). The compliance to regulation is primarily overseen by national Data Protection Authorities (DPA-s), which are coordinated by the European Data Protection Board (EDPB) (Hoffman & Mustert, 2023). In addition, other EU bodies such as the European Union Agency for Cybersecurity (ENISA) support the regulatory environment regarding GDPR. In national context – in Estonia, for example – the Data Protection Inspectorate (AKI) provides national-level guidance and legal obligations are further specified by the Personal Data Protection Act (*Isikuandmete kaitse seadus*, IKS) (Riigi Teataja, 2019).

The GDPR replaced the 1995 Data Protection Directive (95/46/EC), responding to technological change, fragmented national implementations as well as increasing demands for clearer and more aligned digital rights across the EU (de Hert & Papakonstantinou, 2016). New regulation was expected to improve legal certainty and bring greater uniformity, as well as enforcement, addressing inconsistencies that were evident under the previous framework (Albrecht, 2016) – and it did, not only on at the EU level, but also globally (Mahieu et al., 2021; Zaeem & Barber, 2020, Sirur, et al. 2018). Furthermore, the regulation reinforced the recognition of data protection as a fundamental right stated in Article 8 of the EUCFR (Charter of Fundamental Rights of the European Union, 2012), granting it more constitutional weight within the EU legal framework (European Union, 2012; Regulation (EU) 2016/679, 2016).

Despite such progress, many scholars argue that GDPR has significant limitations. For instance, Wolters (2018) concludes that while the GDPR regulates data subject rights, it ultimately offers only limited practical empowerment. In addition, Utz et al. (2019) critize regulation for its imprecise provisions. Similarly, de Hert and Lazcoz (2022) highlight the GDPR's emphasis on organisational accountability, which does not specify how exactly it should be demonstrated. Furthermore, Hoofnagle (2019) points to its length and complexity as general limitation. Alongside such scholarly criticism, organisations report that they struggle to comply with the GDPR because it requires a fundamental and enterprise-wide rethinking of how personal data is processed and stored – changes that go far beyond minor legal adjustments and touch upon more complex aspects of organisational systems (Labadie & Legner, 2023).

In sum, the explored literature suggests that while the GDPR unifies as well as strengthens data protection in the EU, and can be further specified through national laws and guided by DPA-s, its ambiguous provisions, complexity and limited enforceability continue to invite scholarly critique and calls for refinement.

3.2 Strategic Policy Frameworks: EU and Estonian Agendas

While binding regulations such as the GDPR define formal obligations, the development of digital public services across the EU is also shaped by broader strategies. This subsection reviews selected current agendas relevant to the intersection of legal compliance in the data protection domain and UCD in public sector service delivery.

At the EU level, two broader frameworks are established: the 2030 Digital Compass and the Digital Decade Policy Programme 2030. According to the Digital Compass, all citizens should have access to efficient, easy-to-use and personalised public services, supported by privacy and security standards by the year 2030 (European Commission, 2021). Complementing this, the Digital Decade Policy Programme 2030 sets targets for Member States – among its general objectives, as outlined in Article 3.1(a), the promotion of ''a human-centred, inclusive, secure and open digital environment where digital technologies and services respect and enhance Union principles and values'' (European Parliament & Council, 2022). The European Interoperability Framework (EIF) also provides principles for interoperable as well as user-centric digital public service creation, while the European strategy for data promotes secure and innovation-friendly data sharing across sectors (European Commission, 2017; European Commission, 2020).

At the national level, Estonia's contributes to the EU's path by establishing Digital Decade Strategic Roadmap (Estonia, 2023 version). The roadmap is based on three national strategies, among which the Estonian Digital Agenda 2030 serves as the core framework for the country's continuing digital transformation (Majandus- ja Kommunikatsiooniminis-teerium, 2023). The agenda sets priorities for developing digital public services that are user-centred, secure and interoperable. In parallel, it refers to needs-based service design and highlights the importance of involving users in the design process. It also highlights the need for transparency, secure data handling and compliance with legal rules on data processing (Majandus ja Kommunikatsiooniministeerium, 2021). Estonia's E-State Charter also outlines the rights of individuals when interacting with digital public services (Riigikontroll & Õiguskantsler, 2018).

Together, this literature supports broader goals of data protection and user-centred design in public sector digital service development.

3.3 E-Service Design in the Public Sector: Tools, Principles and Challenges

Public sector digital transformation has shifted from the internal digitisation of administrative processes to the external delivery of public e-services, and today, governments are navigating a complex transition between traditional analog service delivery and multi-channel digital models, where online and offline services often coexist (Mergel, 2019). This highlights the importance of the design when it comes to ensuring that public e-services are not only functional but also accessible and citizen-friendly.

To support governments in designing and delivering high-quality digital services, the EU and member state public governance bodies have developed practical tools offering actionable guidlines. For example, the OECD Going Digital Toolkit presents a set of user-focused and principle-based recommendations aimed at helping public service teams implement inclusive and effective digital government strategies (Welby & Tan, 2022). In Estonia, for instance, the Ministri of Economic Affairs and Communications (MKM) established the following 10 Commandments of Digital Services (*Digiteenuste 10 käsku*):

1. Identifying the real user needs and problems;
2. Including people with different background and skills (in the team);
3. Exploring different possible solutions to be able to choose the best one;
4. Designing with the future in mind;
5. Making essential and simple services;
6. Developing together with users and collaborating across sectors;
7. Ensuring interoperability, reusability and opening your solution to others;
8. Working in agile steps;
9. Ensuring security and transparency of the service developed;
10. Taking full responsibility for your service (Majandus ja Kommunikatsiooni-ministeerium, *n.d.*).

These principles are operationalised through E-service Design Toolbox (*Avalike digiteenuste tööriistakast*), which includes process models, content templates, accessibility-usability guidance, as well as practical tools, recommended practices for designing user-centric public digital services (Majandus- ja Kommunikatsiooni-ministeerium, n.d.). In addition, Estonia has developed a range of supporting resources such as handbook on public e-service design (Ziraff, 2014), the usability metrics system (Trinidad, 2014), a handbook on protsess analysis (Ernst & Young Baltic AS, 2012) and many more (Majandus- ka Kommunikatsiooniministeerium, 2024, November 26).

However, despite the growing emphasis on digital transformation and the availability of the various supportive tools, significant challenges remain in international practice.

Recent research reflects that many public digital services still fail to meet actual due to lack of user involvement in the design proccess (Chan et al., 2024; Hashim, et al., 2022; Sharma et al., 2018; Patergiannaki & Pollalis, 2023; Patergiannaki & Pollalis, 2024). This often occurs when public administrations replicate existing offline processes, reinforcing outdated bureaucratic models in digital form instead of redesigning services to reflect how users interact with digital systems (Roberts, 2011), or when laws and regulations guiding the design decisions are too complicated (Danielsen, 2021).

Altogether, the literature suggests that public e-service design today is supported by timely tools and principles, but must still account for legal and organisational constraints that continue to shape its implementation in practice.

3.4 Operationalising GDPR into Design: Articles, Guidlines and UCD Tensions

For public sector institutions, GDPR creates a binding legal environment that must be operationalised through both technical infrastructure and service design. While the regulation sets out a coherent framework of rights and obligations, public service teams must interpret and apply its requirements within real-world design processes. At the core of the regulation are several key data protection principles – highly relevant to the design of public e-services – as they shape how personal data is handled throughout the whole service delivery process. These include lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality (Art. 5.1(a–f), Regulation (EU) 2016/679, 2016).

While these principles provide legal guidance for data protection within service design-related questions, certain GDPR articles address this domain more directly. For example, Articles 12, 13 and 14 mandate transparent information practices, requiring users to be informed clearly and understandably about data processing activities. As closely related, Article 7 governs the conditions for valid consent, which must be freely given, specific, informed and unambiguous (Regulation (EU) 2016/679, 2016). Together, this often translates into added interface layers – but as the regulation lacks concrete rules on how exactly the consent should be obtained, this may lead to inconsistent implementation which, in turn, can contribute to user fatigue due to an overload of confusing, manipulative or poorly designed privacy prompts (Utz et al., 2019).

In addition, Article 15 grants users the right to access and review their personal data. While this provision is intended to enhance user control (Regulation (EU) 2016/679, 2016), its effectiveness depends heavily on how it is implemented in system design. As Wolters (2018) argues, despite the formal governance of data subject rights, individuals often remain in a disadvantaged and reactive position, lacking the tools or visibility to meaningfully oversee the full scope of personal data processing.

Finally, Article 25 introduces the principle of data protection by design and by default, which mandates that privacy considerations be built into systems-services from the very start. This includes guaranteeing that only the data necessary for a given purpose is collected or visible to the user, influencing how interfaces are structured, what information is shown and many more (Regulation (EU) 2016/679, 2016). Yet, Veale and Binns (2017) argue that Article 25 is often implemented too narrowly – as a technical compliance requirement rather than a holistic design paradigm – thereby missing the broader spirit of the regulation.

Relevant to this context, the European Data Protection Board (EDPB) has issued guidance to help interpret Article 25 in practice, offering recommendations for implementing data protection by design and by default in service development (EDPB, 2020). At the national level, the Estonian Information System Authority (RIA) provides publicly available materials that, while primarily technical, influence design-related decisions (RIA, n.d.). Additionally, the Estonian Data Protection Inspectorate (AKI) has issued general guidelines for data processors (Andmekaitse Inspektsioon, 2019).

As such, the literature regarding operationalisation of the GDPR in public e-service design reveals a recurring tension between legal intent and real-world implementation – where abstract regulatory principles often translate into inconsistent, fragmented or usability-challenging design outcomes. While various practical tools and guidelines have since been introduced to support compliance, it remains unclear to what extent they have actually helped resolve these issues, as much of the critique emerged prior to their widespread adoption.

4 Research Design and Methodology

This study adopts a qualitative case study approach to examine how a national public organisation in Estonia interprets and applies the GDPR in the design process of user-centred digital services. The case organisation manages several state e-services, making it a relevant context for analysing how data protection obligations are addressed in practice. The research focuses on the challenges of aligning legal compliance with usability goals, particularly in situations where abstract regulatory requirements must be implemented under real-world organisational and technological constraints. A case study approach is well suited to investigating such complexity, allowing for an in-depth exploration of professional practices and institutional dynamics (Yin, 2018).

The research combines document analysis and semi-structured interviews. Triangulation of these data sources enhances the depth and credibility of findings by supporting cross-validation and enabling a more thorough grasp of the case (Bans-Akutey, 2021).

4.1 Data Collection

To capture both the phenomenon itself and its broader organisational context, this case study approach incorporates data from multiple sources, as recommended by Yin (2018). Accordingly, both primary and secondary data were collected.

4.1.1 Primary Data Collection

The primary data was collected through semi-structured interviews conducted with professionals from the case organisation. Eight participants were interviewed: six from four different e-service development teams, including analysts and product owners, and two legal experts involved in advising on data protection compliance. Participants were recruited through purposive sampling to ensure the inclusion of individuals with direct, practical experience in both service design and regulatory interpretation (Palinkas et al., 2015). These roles were deliberately selected because of their central position in the design process. Analysts and product owners are responsible for gathering service requirements, creating initial service concepts and conducting functional analysis – activities where legal obligations such as GDPR must already be accounted for. Legal experts, in turn, advise on data protection matters throughout the design cycle, ensuring that legal risks are identified and managed.

Two different sets of questions were created: for legal advisors (Appendix 2) as well as for analysts and product owners (Appendix 3). Both versions were open-ended and flexible to encourage participants describing their personal experiences and reflect on how they have handled GDPR-related decisions – follow-up questions were also asked, if further clarification was needed. All interviews were conducted via Microsoft Teams and in Estonian language, recorded with consent and transcribed using Estonian Speech Recognition and Transcription Editing Service tool (Olev & Alumäe, 2022). Each session lasted between 24 and 59 minutes. Table 1 gives an overview of the participants, and for anonymity, each interviewee is represented by a code.

Table 1. Overview of Interview Participants.

Code	Job title	Interview Format and Duration	Date
A1	System Analyst	Microsoft Teams Recording (24 minutes)	28.04.2025
A2	Business Analyst	Microsoft Teams Recording (32 minutes)	30.04.2025
P1	Product Owner	Microsoft Teams Recording (59 minutes)	30.04.2025
L1	Legal Advisor	Microsoft Teams Recording (25 minutes)	02.05.2025
P2	Product Owner	Microsoft Teams Recording (32 minutes)	02.05.2025
A3	Business Analyst	Microsoft Teams Recording (36 minutes)	02.05.2025
L2	Legal Advisor	Microsoft Teams Recording (26 minutes)	05.05.2025
P3	Product Owner	Microsoft Teams Recording (34 minutes)	05.05.2025

4.1.2 Secondary Data Collection

In addition to interviews, secondary data was used to contextualise the research and support the interpretation of primary findings. The reviewed sources included legal documents, EU and national digital policy strategies, official guidance from public authorities and academic literature related to data protection and UCD in public services. Reviewing these materials helped clarify the broader legal and strategic context in which user-centred public services are developed and where GDPR compliance must be integrated.

In addition to providing background, these documents were used to cross-check findings from the interviews and to support the credibility of the analysis. This contributed to a more grounded understanding of how institutional expectations, legal obligations and design practices intersect in the public sector.

4.2 Data Analysis

The primary data was analysed by using thematic analysis (TA) method, which is flexible and the most suitable option for identifying patterns across qualitative data (Clarke & Braun, 2017). All coding was conducted manually to allow close engagement with the material and ensure that emerging themes remained grounded in the data.

The analysis proceeded in several stages. First, interviews were transcribed, translated and then read to familiarise the researcher with the content. Second, initial thematic codes were generated by marking repetitive thoughts mentioned by interviewees. Third, the codes were gathered into broader themes based on similar patterns. Fourth, themes were reviewed and refined to ensure they corresponded to the research questions and reflected the diversity of perspectives across roles. Finally, the coded material was organised into analytical themes, which form the basis for the presentation of findings in the next chapter.

In parallel, relevant secondary documents were re-reviewed to identify key references to GDPR and design practices. These materials supported the interpretation of interview data and strengthened the credibility of the overall analysis through triangulation.

4.3 Ethical Considerations and Data Validity

This research follows all relevant ethical guidelines to protect interviewees and ensure validity of the study. Participants were informed about the aim, as well as the nature of their involvement, and given the right to withdraw at any stage without explanation or consequence – right before the interview.

To protect interviewees anonymity, the name of the organisation and its specific e-services are not disclosed in this thesis. This decision was made due to the relatively small size and specialised nature of the teams involved, where individuals could potentially be identified through their role or association with specific services. For example, some teams consist of only one or two analysts, product owners or legal advisors, making identification possible through publicly available information. To minimise such risk, all references to the organisation and its services have been classified.

No personal identifiers were collected and participants are referred to using role-based codes – for example, A1 for analyst (both system's and business), P1 for product owner and L1 for legal advisor. Interview recordings as well as the transcripts were stored securely and handled exclusively by the researcher. All data used in the analysis and reporting was anonymised.

A clear and transparent thematic analysis process was followed to identify key patterns in the interviews. Findings were also cross-checked with secondary sources to support consistency, which also allowed for a more balanced interpretation. The risk of data bias was considered and mitigated by asking open-ended questions, which allowed free opinion-sharing.

5 Results

This chapter presents the empirical findings of the study, based on semi-structured interviews with analysts, product owners and legal advisors involved in the development of public e-services in Estonia. While the research was guided by three core questions, the thematic analysis resulted in four distinct themes that reflect how GDPR is interpreted, experienced and operationalised in the context of user-centred service design (Figure 2). These themes were identified deductively from the research design, while more specific sub-themes emerged inductively through detailed coding and analysis of the interview data. The aim of this chapter is to understand how GDPR is interpreted, experienced and operationalized by different professional roles in the context of user-centred public digital service design.

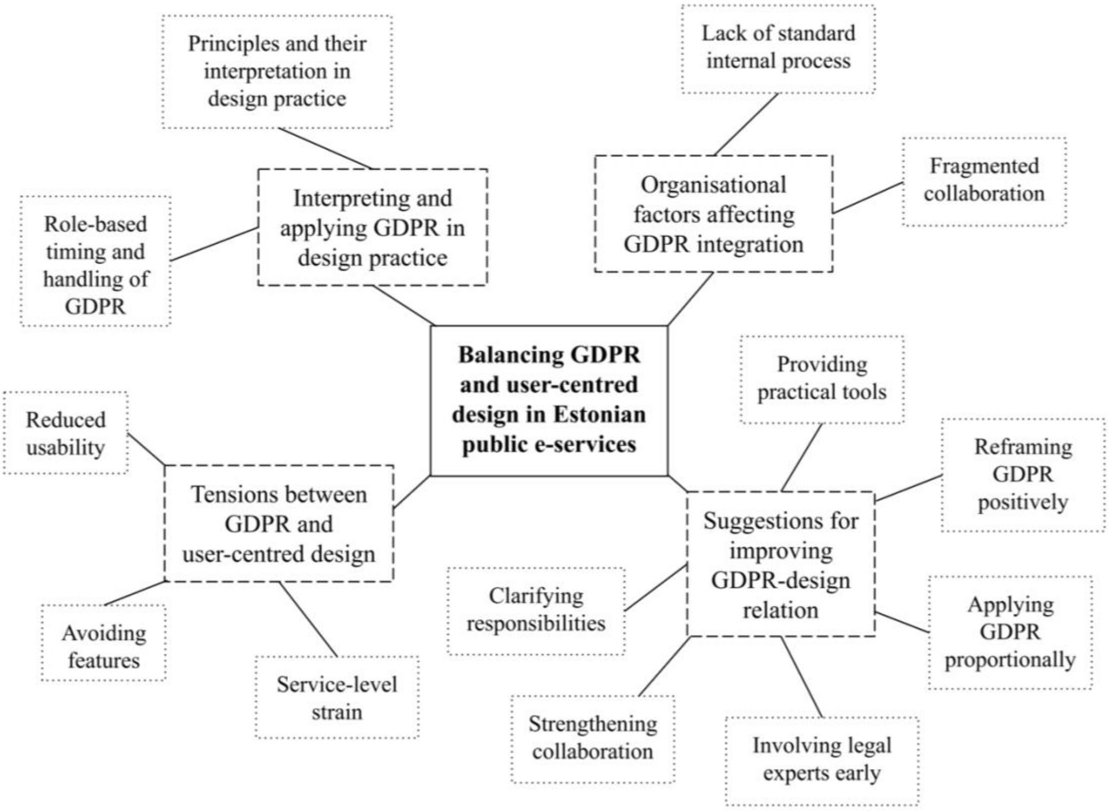

Balancing GDPR and user-centred design in Estonian public e-services
Interpreting and applying GDPR in design practice
Principles and their interpretation in design practice
Role-based timing and handling of GDPR
Organisational factors affecting GDPR integration
Lack of standard internal process
Fragmented collaboration
Tensions between GDPR and user-centred design
Reduced usability
Avoiding features
Service-level strain
Suggestions for improving GDPR-design relation
Providing practical tools
Reframing GDPR positively
Applying GDPR proportionally
Involving legal experts early
Strengthening collaboration
Clarifying responsibilities

Figure 2. Thematic Map: Balancing GDPR and User-Centred Design in Estonian Public E-Services.

5.1 Interpreting and Applying GDPR in Design Practice

This section explores how public sector professionals interpret and apply the General Data Protection Regulation (GDPR) during the development of user-centred e-services. The findings show that although the regulation is formally binding, its practical influence depends largely on individual understanding, informal routines and the stage of the design process in which it is addressed. Differences between professional roles also affect how specific GDPR principles are noticed, prioritised and translated into concrete design actions.

5.1.1 Role-Based Timing and Handling of GDPR

Professionals from all interviews agreed that GDPR considerations are neither systematically brought into play nor introduced in a uniform way throughout the service design process. Instead, GDPR tends to appear at different points in the timeline, depending also on the role – sometimes during early planning or analysis, but more often as a reaction to specific questions, user feedback or launch preparations.

Analysts reflected that GDPR tends to emerge in the business analysis phase, particularly when data requirements are first mapped out, when they consider what kind of personal data is being gathered, assess whether the data is duplicated elsewhere and occasionally consult with legal or data protection staff. However, this early attention does not generally involve a complete legal analysis, but more informal readings in the light of their own experience or assumed rules. Analysts seem to work under shared assumption of what is acceptable, applying GDPR principles pragmatically, often without formal legal input. Common triggers included user interviews, form design considerations and informal concerns raised during research.

The product owners described that the GDPR enters the process during planning or specification, especially when determining if certain data can be made public-hidden or reused across systems. However, it is often a matter of user testing and other external feedback that indicates potential problems regarding the GDPR. Several product owners indicated that complaints or concerns from users and external authorities prompted GDPR discussions late in the process, occasionally requiring reactive changes that disrupted previously agreed-upon design features.

Legal advisors are rarely involved in the early stages of service development – they typically become engaged only when a specific legal question arises or when a project is nearing deployment. As one of them expressed: "*I assume and hope that by that point the commissioning party from the ministry provides clear, lawful requirements. We are not consulted in that process*". But several participants noted that this late-stage involvement often results in rushed evaluations, reactive fixes or even the reversal of earlier design decisions. These role-based differences in timing, triggers and handling of GDPR are summarised in Table 2 below.

Table 2. Role-Based Differences in Timing, Triggers and Handling of GDPR.

Aspect	**Analysts**	**Product Owners**	**Legal Advisors**
Timing *During…*	Early *- data mapping* *- research*	Early to mid *- planning* *- testing*	Late *- near deployment* *- when issues arise*
Triggers	- interviews - form design - informal user concerns	- data visibility - complaints - legal uncertainty	- legal queries - escalations - final compliance
Handling	- habit-based - informal - minimal legal input	- trial-an-error - experience - delayed legal consultation	- formal - reactive review of legal basis and documentation

All in all, this suggests that GDPR may not be sufficiently taken into account at the appropriate stages of the design process. Instead, it tends to be considered unevenly and often too late to shape key decisions without disruption. This reactive approach reflects the absence of a clear structure for integrating legal considerations into user-centred service design from the outset.

5.1.2 Principles and Their Interpretation in Design Practice

When asked which principles of the GDPR are most related to their everyday work, most interviewees pointed to the same few core examples: minimisation, purpose limitation, and lawfulness and transparency. Interpretation also varied between roles. Although other principles like storage limitation and accuracy were occasionally mentioned they seemed less central to steering design decisions.

Data minimisation was the principle most referred to by all the roles. Both analysts as well as product owners highlighted the importance of need to avoid collecting unnecessary information, particularly when designing forms, input fields and other user interface elements. Minimisation was also mentioned in relation to system access, where permissions were configured to restrict visibility of sensitive data to only those users with a clearly defined need. Legal advisors confirmed that this concept is frequently at the basis of data sharing agreements and systems architecture reviews, particularly regarding sensitive data types.

Purpose limitation was mentioned regarding user research and testing. Analysts described how they make sure participants understand why their data were being collected in interviews, survey or usability testing, including explanations about retention periods and data access. While there was common awareness of the need to define purposes, there was also major uncertainty about the level of detail or formality such explanations should be, as no formal structure or process appeared to confirm such steps.

Lawfulness and transparency, which were less frequently mentioned in technical terms, emerged in how participants described interpreting legal bases for data collection. Some informants noted that detailed justifications had to be provided for why certain data were needed and on what legal basis access to that data was required. Consent was frequently used as safe option, even in cases where other legal bases – such as legal obligation or public interest – may have been more appropriate. One of the interviewees stressed that consent is often applied unnecessarily or incorrectly: *"Things could be done better. For example, the cookie consent box always comes up first, which in my opinion doesn't even need to be there – especially in public services. For certain services, I think it's not necessary at all to ask for voluntary cookie consent. A legitimate interest analysis would be more appropriate in relation to what we actually need. [...] What matters is looking at it from the data subject's perspective – what is most critical for them."*

Notably, the interpretation of GDPR principles and their operationalisation do not always seem to align. For example, while data minimisation was seen as undeniably important, some interviewees equated it with limiting the amount of information shown to users, even when that data had already been lawfully collected – this was a common misinterpretation. In addition, applying the purpose limitation principle sometimes led to fragmented service experiences, as certain data could not be reused across systems or contexts. In these cases, cautious or overly narrow interpretations of GDPR principles ended up creating friction in service use and design.

In sum, professionals demonstrated good awareness of the main GDPR principles and provided some relevant examples on how these principles have influenced the design of services. Rather than being guided by shared organisational processes, many decisions were shaped by personal judgement, experience and the level of available legal input.

5.2 Organisational Factors Affecting GDPR Implementation

This section explores how GDPR is handled within the organisational setting, where structured, repeatable processes for integrating data protection into service development are missing. While the professionals interviewed demonstrated awareness of the regulation, they consistently described an environment where responsibility for compliance was unclear and practical action steps were developed informally. This lack of standardisation meant that decisions related to GDPR were often based on habit, precedent or individual judgement – rather than shared procedures. As a result, teams approached data protection inconsistently, especially in early phases of design..

5.2.1 Lack of Standard Internal Process

Interviewees across different roles described working without a unified structure – there are no designated checkpoints no consistent documentation practices and no in-house coordinated methods applied during the design process. While some teams had developed their own ad hoc routines or templates, these varied widely and were not aligned across the organisation.

This was especially visible in areas such as user research, where participants were unsure what kind of explanations or retention notes were required and how this information should be recorded. As one illustrated: "*Before our interview, I even went to check if it existed, but I couldn't find anything. I'm familiar with the GDPR and have looked into it, but with all the noise and tasks, it's not like a homepage I visit every day or have time to keep up with*. […] *I often just use examples from earlier projects. There's no central place where it's said 'this is how we should handle GDPR'.*'' The same participant also noted that one is never entirely sure whether things are done 100% correctly – but so far, they have passed.

Few interviewees mentioned that some development requirement formats are being updated but these had not yet been implemented – and it is unclear whether systematic integration of GDPR principles would be included. In the meantime, decisions continue to rely on individual-team initiative and assumptions, which can create uncertainty – especially for less experienced staff. One interviewee noted that teams may have developed their own approaches: "*We don't have a standardised template for GDPR things. Some teams have made their own, but it's really based on who you ask or what kind of service it is.*"

To conclude, while compliance is technically met, it is not systematically integrated into core processes – the current system leaves professionals to interpret and operationalise GDPR independently, leading sometimes to inconsistent outcomes.

5.2.2 Fragmented Collaboration

Addressing GDPR topics during service development and UCD practices was perceived as informal and mainly dependent on personal initiative. There was no established routine for cross-role communication about data protection and also the involvement of legal or data protection staff varied widely from case-to-case.

Analysts contacted legal advisors or Data Protection Inspectorate (DPI) only when a some kind of specific problem arose. As one of them said:"*In two years, I've talked to the data protection specialist only once. Everything I've done has been based on my own initiative. [...] I don't have any specific guidance or active communication with the data protection specialist.*" Similarly, product owners described their experiences as mostly relying on instinct or peer advice when navigating GDPR-related decisions. "*There's no clear line about when something should go to legal. It's very much case-by-case. Sometimes it's me guessing if it's serious enough or not,*" one product owner explained. The GDPR-related questions were also addressed back to the commissioning ministry or Data Protection Inspectorate, which in some cases helped, but could also delay feedback or add uncertainty – depending on the team, the task and the experience of the expert involved.

Legal advisors acknowledged that they were rarely included during the design and development process, often found themselves reviewing results only if they endeded up not compatible to GDPR. "*Our involvement usually happens at the final stages. In short, people only ask when a problem or confusion appears. We don't participate by default* *from the beginning,*" one advisor stated. They also mentioned a lack of regarding role boundaries – GDPR-related responsibilities sometimes overlapped, leading to duplicated work or gaps in responsibility, where no one clearly acknowledged/owned the data privacy-related decisions.

Overall, the lack of established and clearly defined approach to collaboration suggests GDPR was rarely addressed and interpreted through specifically coordinated effort. Each role acted largely within its own knowledge or assumption, with limited visibility into how others were approaching the same issues. While participants across roles expressed a desire for clearer expectations and earlier cooperation, no systematic approach to collaboration was in place. As a result, the handling of GDPR remained inconsistent, with legal and usability concerns often addressed separately rather than together.

5.3 Tensions Between GDPR and UCD

This section examines how professionals experience and respond to practical tensions arising between GDPR requirements and UCD. While privacy and usability are not exactly the most opposite domains, participants described a range of situations in which legal constraints, uncertainty or other barriers made delivering user-centric public e-services challenging. These tensions were extended to everyday design decisions, planning workflows and perceived boundaries of professional responsibility. In some cases, teams found pragmatic ways to move forward; in others, tensions resulted in rework or reduced service quality.

5.3.1 Reduced Usability

Participants across roles described how GDPR-related decisions often made public e-services less convenient or useful. A common example was the removal of previously visible data fields – such as personal identification numbers or address details – which had to be hidden following legal review. While these decisions were justified from a privacy viewpoint they often disrupted everyday use. As one product owner noted, "*You want people to be able to see everything, but at the same time, some information probably shouldn't be that easy to access. It's frustrating, because there's no easy way to resolve it.*" In some services, users who had previously accessed data directly now had to log in, submit requests or use separate systems to complete basic tasks.

Automated bot protection was another example that negatively affected usability. One product owner described: "*Well, that robot trap in particular definitely limits and bothers users. [...] They [the Ministry] had to experience first-hand how inconvenient it is – constantly having to solve tasks just to see the data. It really bothers users and we receive a fair number of complaints and contacts about it. It restricts users. And honestly, right now we don't have a good solution.*" The same participant indicated that in the new system under development, another protection system will be used, which doesn't directly give tasks to the user but instead monitors the behavior in the background. So it may improve the situation, but "*since it hasn't been fully tested with users yet, we don't know how disruptive it might be; there is a risk that under certain conditions, someone could be blocked.*"

Some teams responded to legal concerns by restructuring service flows or removing functionality altogether. Services were sometimes fragmented – redirecting users elsewhere instead of integrating features into a single interface. Analysts mentioned that visibility or functionality was sometimes reduced not due to a direct legal requirement, but because "*sometimes we just take something out because we're not sure – it's not that the law says no, but it's safer not to include it.*" Internally, stricter access controls also caused delays, as one analyst explained: "*If someone wants to test or fix something, they often have to go through extra approvals. It delays things*."

In sum, while no participant questioned the importance of strong data protection, many described how the way GDPR was implemented often compromised usability. So rather than enabling balanced, integrated solutions, teams frequently relied on quick fixes – like hiding data or adding extra steps – to stay compliant, even when these made the services more difficult to use.

5.3.2 Avoiding Features

Beyond visible usability losses, many participants described how GDPR-related uncertainty led to the quiet avoidance of certain design features. Teams sometimes chose to delay, limit or entirely exclude functions that seemed not to comply with GDPR – even when these features would have improved UX, service efficiency or fulfilled the purpose of the service more effectively.

This trend to avoid not yet realised challges appeared in several interviews. For example, one interviewee described how a team had in mind implementing some kind of auto-complete functionality, where names of individuals or companies would appear as the user types in real time. But, it was decided not to include it, as the uncertainty arose whether showing the names of natural persons would be allowed under GDPR, especially due to the frequency of name duplication in Estonian national context. To avoid the risk of unnecessary personal data exposure and potential violation of GDPR, the team dropped the idea altogether.

Product owners gave similar examples related to the visibility of historical data. While current legal obligations require some service-specific data to be publicly accessible, there seems to be no institutional clarity on how long such data – for instance, past member roles – should remain visible. In response to increasing pressure from users who did not want to be searchable online, some teams limited or removed this data, even though it could support transparency and accountability. One product owner explained: "*So today I'm listed as a [X] member, but tomorrow I'm removed, and suddenly none of my past involvement should be visible anymore. That's a typical complaint. [...] But if that [X] member can disappear from the data list the moment they've pulled off some fraud, it becomes really hard to trace who was actually responsible*". As a workaround, the team made changes to block search engine indexing: "*We've made technical changes to prevent indexing by Google, to stop those historical details from being accessible that way*".

Another example was given within how the user consent was handled. Interviewees explained that this approach is often used as a precaution, as adding a consent checkbox was seen safer than trying to argue for more complex legal basis – even when it was unclear whether the consent was truly necessary or meaningful. This could led to e-service interfaces that were technically fine-looking, but included complicated legal consent-disclaimers – a less as meaningful tool in terms of user data-related rights and more as a defensive tool to mitigate service development team uncertainty.

These examples show how that teams often defaulted to the safest option – sometimes leaving out features, limiting visibility or deferring to consent mechanisms rather than risking non-compliance. Such examples were not always based on GDPR prohibitions only, but triggered by combined legal risk, some reputational concerns or uncertainty about regulators respond.

While these decisions may reduce legal risk, they also prevent teams from fully exploring user-centred improvements – especially in cases where practical safeguards could have made the feature compliant. In this way, GDPR uncertainty becomes a limiting factor not only on what services can do, but also on how teams imagine and prioritise features in the first place. This kind of feature-avoidance may result in design stagnation, which from one side protects institutions, but from other, hinders innovation and reduces service value for users.

5.3.3 Service-Level Strain

Several interviewees mentioned that rules for data visibility had been changed several times. While such decisions are introduced by oversight bodies or the commissioning ministry, in long-term perspective, they seem to lack stability as well as predictability. One product owner observed: "*The problem I see is that different agencies don't cooperate. The DPA pushes for concealment based on complaints, while on the other hand, there needs to be a broader perspective at the national level: What are the goals? Who needs what and why?*". This highlighted the deepened uncertainty (as well as missing collaboration). The same participant added that this frequent toggling of data visibility is far from trivial in technical means: "*Sure, it's easy to write on paper: 'These data are public, those are not.' But from a system point of view, it's not that simple. Today we remove some data, tomorrow we hide others, the next day we make something public again. That's a huge amount of work*".

Legal advisors confirmed – these changes often emerged reactively, possibly without full understanding of the design or resource implications. From other viewpoint, they also analysed that this could be part of a broader challenge. One of them reflected that when GDPR first came into light, many services indeed leaned toward greater transparency. However, this was not due to a lack of legal guidance, but rather a shortage of professionals with the capability to interpret and apply it appropriately. As one legal advisor put it: *"There was never a lack of regulation – the rules were in place. But there just weren't enough competent people who could understand and apply them. […] I think the same problem continues today – the people doing this work are around my age or younger, and they don't always have the full picture* yet". This suggests that in addition to just legal uncertainty, there might be also the gap in legal-technical expertise. That’s why now, years later, teams are being asked to reverse course.

In addition, some product owners suggested that wider social pressures can also contribute to this cautious shift in data visibility, pointing to rising user sensitivity as a result of the war in Ukraine: “*One factor, of course, is the war in Ukraine – people are more afraid for their personal data exposure,”* said one interviewee. This concern, while not directly linked to GDPR, was cited as a reason why certain services had quietly become more limited over time. Such reactions – although precautionary – added extra layer to the professionals' workload.

Moreover, participants described some operational consequences. One product owner shared that even routine debugging in live systems had become difficult due to GDPR-linked monitoring tools like the Data Tracker: “*People in our team are hesitant to even open the [X] data in the live system because every lookup creates an entry in the Data Tracker and later someone might come and ask, ‘Why did you look at this?’ […] So now people are afraid. Even I always hesitate – do I really need to open this right now? Because a hundred people might later see that I looked at it, and I’ll have to justify it. So I might not double-check some bugs in production. It creates friction. A lot of noise over a single click*”. This shows how internal accountability systems, although intended for transparency, can generate hesitation and even reduce the team's ability to maintain quality efficiently.

To manage risks teams also relied on temporary fixes – such as disabling features, hiding sections of the interface or blocking search engine indexing, as mentioned before. While these helped avoid immediate compliance issues, they also added long-term system complexity – analysts noted that such workarounds often stayed in place longer than planned simply because the underlying legal questions were never really resolved.

Unlike the more visible impacts on usability or feature functionality, this form of strain builds slowly, but affects the overall resilience of public services. Without stable and predictable legal interpretations, systems can indirectly become vulnerable to disruption. As over time, this undermines design continuity, weakens team’s confidence and increases the long-term cost of building and maintaining coherent, legally sound services.

5.4 Ideas for Improving GDPR–Design Integration

Participants offered a number of direct suggestions to improve how GDPR is handled in public e-service development. These are summarised in Table 3 and explained in more detail in the following subsections.

Table 3. Suggestions for Improving GDPR–Design Integration.

Suggestion	Key words
Clarify responsibilities	Role clarity, decision ownership
Strengthen collaboration	Cross-role communication, continuous interaction
Involve legal experts early	Early-stage legal input, proactive risk prevention
Provide practical tools	Internal templates, guidelines, reusable examples / design components, documented previous solutions
Applying GDPR proportionally	Context-based decisions, avoiding over-compliance
Reframing GDPR constructively	Positive mindset, shared values, trust-building

5.4.1 Clarifying Responsibilities

Many participants said that GDPR-related decisions were often delayed because it was unclear who within a team or organisation was responsible for interpreting legal requirements or deciding how those requirements should influence design. This led to delays, hesitation or conservative choices made "just in case." Product owners, in particular, expressed the need for clearer boundaries between legal interpretation and design decisions, so that accountability would be better distributed and decisions made with more confidence. Clarifying responsibilities was seen as a basic, but essential step toward reducing ambiguity and improving design outcomes.

5.4.2 Strengthening Collaboration

Participants emphasised that improving collaboration between legal experts, analysts and product owners would significantly enchance how GDPR is integrated into service design. In several cases, poor communication or role separation led to misunderstandings, duplicated efforts or very last-minute changes. It was described that legal advice sometimes arrived too late to influence design constructively, while legal advisors noted that they were not always consulted early enough to provide meaningful input. Participants suggested that closer, more continuous and structured collaboration is –

through joint planning sessions, some defined processes or discussion panels – would help ensure that legal considerations and design priorities are balanced from the start, rather than corrected at the end.

5.4.3 Involving Legal Experts Early

As repeatedly mentioned already, many participants said that legal experts were often brought into the process too late – usually when development was nearly finished. This often led to reactive last-minute changes, such as quick hiding features or rewriting content, which could have been possibly avoided with earlier professional legal input.

Half of the interviewees suggested involving legal expertise at the planning and design stages would help identify risks in advance and reduce unnecessary rework. Early legal input was seen not just to ensure compliance, but also to design better services from the start – avoiding rushed fixes and making room for more thoughtful, integrated solutions.

5.4.4 Providing Practical Tools

Almost all participants highlighted the need to create GDPR compliance supporting tools for everyday design work. Rather than relying on abstract legal text or one-off consultations with legal advisors, teams wanted access to GDPR-infused templates, visual and textual internal guidelines/documents that could help them make more compliant design decisions. Examples included reusable consent templates, privacy notice formats and Figma components, that are approved and used across whole organisation and services. For example, these tools were seen specially useful in situations, where teams had limited time to seek legal clarification. Legal advisors also supported this idea.

5.4.5 Applying GDPR Proportionately

Some participants highlighted the necessity of integrating GDPR in a manner that accurately reflects the specific context and objectives of each e-service. While legal obligations were addressed with extensive attention, some interviewees stressed that risk-avoidant interpretations had led to overly strict measures, such as unnecessary login requirements or excessive consent prompts straining usability rather than providing the user any clear privacy-related benefits. An idea of a more balanced application of GDPR was proposed as a means to reconcile legal compliance with user needs, especially in situations where public interest or legal mandates already allowed data processing. This idea requires better collaboration and extensive discussions between different stakeholders, and a willingness to assess each case and service on its merits.

5.4.6 Reframing GDPR Constructively

Interviewees legal side suggested that the overall attitude toward GDPR within design and development teams could definitely benefit from reframing. Rather than viewing the regulation purely as a constraint, they encouraged treating it as an opportunity to build trust, improve transparency and support better service design. One also mentioned that GDPR principles often align with user-centred goals – such as clarity, control and accountability – and that embracing these shared values could lead to more aligning results.

6 Discussion

This chapter interprets the findings of the study in relation to the research aim, the existing literature and the theoretical framework. The research explored how GDPR is understood, experienced and applied in the design of user-centred public e-services in Estonia, drawing on the perspectives of legal advisors, product owners and analysts. The analysis revealed variation in how professionals interpret GDPR, organisational factors influencing its application, recurring tensions between legal and design goals, the practical strategies used to manage these challenges as well as professional suggestions for improving GDPR – design integration.

Notably, the results analysis uncovered not only technical or procedural tensions, but also rooted in deeper mismatches between roles, expectations and organisational culture. The difficulties stem less from the regulation itself and more from how it is interpreted, communicated and managed within service development teams. In practice, GDPR is not experienced as a clear or easy-applicable framework in day-to-day design work. But such interpretation also varies significantly by role – legal advisors engage easily with abstract legal reasoning and general principles, while product owners and analysts seek more specific and rather actionable direction for the concrete design choices. This disconnect often leads to widely expressed uncertainty and unnecessarily cautious decisions – not because they are required by law, but that is how professionals feel safer operating in described conditions. These decisions reflect tendency of defensive thinking, which meaning the teams are not certain of how to proceed or the legal input arrives too late – that is when they decide to fall back quicker but usability-limiting defaults.

E-services were described as first thing being launched, only later modified and rolled back because of the GDPR interpretation, which often resulted in major rework, resource loss and even lower confidence in planning future service or updates. Such reactive mode can sometimes be the main contributor to slower development, increased cross-organisational frustration and making design innovation less user-centred and progressive.

Participants did not state GDPR and UCD as being incompatible domains, but explained the tensions arising from because of lack of shared organisational processes, or professional knowledge that would allow legal and design concerns to be more considered together. Legal advice was usually asked only after the design decisions had already been made and GDPR-related conflicts already surfaced, which made compliance into a more of a reactive restriction rather than a guide. Product owners sometimes felt themselves managing legal risk alone, without sufficient and structured involvement of stakeholders who could engage in meaningful discussions about integration or exploration of other alternatives. This lack of integration also reduced the opportunity to balance obligations with broader service goals, by contrasting data protection domain with principles like transparency, for example.

In addition, organisational setting deepened these aforementioned dynamics. Interviewees reflected need for a better role clarity as well as documented practices and institutional memory. In the absence of shared resources or unified cross-team learning, they relied on precedents, guesswork or personal-professional assumptions and experiences. While this allowed work to continue, it also introduced inconsistencies and contributed to a culture where legal defensibility was prioritised over usability. This explains why, even with good intentions, design decisions often leaned toward limitation and caution rather than innovation or further clarity.

Viewed through the lens of institutional logics, these findings reflect what can be described as an estranged logic arrangement, as legal and design rationalities coexist but remain structurally separated. Legal reasoning becomes dominant in situations of uncertainty, while UCD – though supported in principle – is less embedded in everyday decisions. Without formal structures to negotiate between these logics, professionals must resolve tensions individually, often by deferring to perceived legal safety rather than collaboratively exploring balanced solutions.

These internal challenges are widespread – public institutions frequently face obstacles in implementing GDPR, particularly when legal and design functions operate in isolation. What this study contributes is a very detailed, grounded account of how those tensions materialise in daily work, how they affect service outcomes and why current organisational arrangements make them difficult to resolve. The findings indicate regulatory uncertainty, but not as simply a compliance issue more of systemic design governance challenge.

All participants consistently expressed strong support for GDPR's core principles, especially transparency, accountability and data minimisation. They did not reject regulation, nor the first-level importance of individual data protection rights, but they clearly expressed the need for better systems to applythe regulation in ways that also respects UX – real constraint was not legal complexity, but the lack of mechanisms in place to interpret and operationalise GDPR in a way that supports both legal defensibility and design coherence.

This study highlights the need for more deliberate structures that support collaboration, early legal involvement and shared decision-making. Proportionate application of GDPR should be normalised – not as an exception but as a supported default. This change would require better-established internal responsibilities, practical design tool and stronger organisational will and resource inclusion to ensure learning carries across projects.

More broadly, the findings add to ongoing debates about how public institutions can balance legal obligations with innovation. As digital services become core to state–citizen interaction, the challenge is not just interpreting the law accurately, but doing so in ways that enable constructive and forward-looking service development. A proactive, integrated approach to GDPR – one that treats compliance as a design opportunity, not an obstacle, could help public institutions deliver more consistent, transparent and user-focused services.

6.1 Practical Recommendations

This study has shown that many of the challenges in applying GDPR to user-centred public service design are not caused by the regulation itself, but by the way it is interpreted, communicated and managed within case organisation. Based on the findings and synthesis of participant suggestions, the following recommendations are proposed to improve current approaches to GDPR implementation in UCD work:

1. **Strengthen consistency and predictability of legal interpretation**

Organisations should establish shared internal interpretations for common GDPR issues – such as the use of consent, data visibility thresholds and regarding legal bases for processing. These positions should be formalised, validated and accessible to all development teams and roles.

In addition, reducing reliance on individual case-by-case interpretations would prevent contradictory decisions, minimise redesign work and increase overall legal confidence across teams – the author recommends forming a special workgroup (including commissioning Ministry, DPI and other relevant stakeholders from organisation) to raise the broader discussion and try finding the most optimal solution.

2. **Integrate legal support earlier and more systematically**

   Although legal advisors are officially assigned to projects, they are often involved too late to influence planning and design constructively. Legal expertise should be embedded at the start of each development cycle, including during early-stage requirement analysis, solution scoping, and testing phases. Standard procedures should mandate timely consultation so that legal and design concerns can be considered in parallel, rather than in isolation.

3. **Improve internal access to past decisions and privacy-related examples**

   A central documentation system should be updated to include knowledge about how GDPR-related issues have been addressed in organisational past. Maintaining and consulting such a knowledge base would reduce ambiguity, enable reuse of good practices, and improve continuity – especially in complex or multi-team environments. In addition, supportive and reusable guidelines/components should be created and made accessible to all the service development teams.

4. **Clarify decision-making responsibilities within multidisciplinary teams**

   Roles related to GDPR interpretation and design implications must be clearly defined within each project – teams should know, who exactly is responsible for data protection decisions, when legal input is required and how those responsibilities are distributed and managed. This would foster accountability and prevent indecision.

5. **Promote a proportionate and constructive approach to compliance**

   Instead choosing by default the strictest way of interpretation, teams should be encouraged to assess GDPR requirements considering service purpose, data sensitivity and user needs. Internal discussions between legal and design stakeholders should support risk-based, balanced solutions. In addition, this would also require workgroup or panel discussion between relevant institutional stakeholders, as mentioned in the first recommendation.

Together, these recommendations highlight the need for more consistent, collaborative and confident approaches to GDPR implementation within organisation – ones that support compliance without compromising the goals of user-centred public service design.

6.2 Limitations

As with any qualitative research, this study has a few limitations. The research focused on one public organisation in Estonia that develops digital services, offering thorough insights into how GDPR is interpreted and put into practice during design. Although this approach offered a detailed view into internal public organisations' processes, the findings may not be fully transferable to other similar agencies or general institutional contexts within the public sector.

The study focused on professionals who are directly involved in design and development of public sector e-services – including legal advisors, product owners and analysts. It did not include representatives of the Estonian DPA or the data controller (the commissioning Ministry). While this choice allowed the research to focus on those closest to practical operationalisation in design domain, it may have left out perspectives on how strategic legal decisions are shaped at the policy level.

Finally, the study reflects a specific point in time within a rapidly developing regulatory and design environment. Organisational practices, interpretations of GDPR and modes of collaboration may evolve, which could affect how some findings apply in the future.

6.3 Future Research Directions

This study highlights the need for further and deeper research on how GDPR influences the UCD of public digital services in practice. It is now clear, that there are timely and unresolved issues that require attention, but addressing and actually resolving the issues will demand more data, interviews and possibly even a separate research team to fully capture the very needed scope.

Follow-up research should involve more sectors and roles to reflect a broader range of different experiences. Involving not only design and legal professionals, but also policy-makers, implementers and end users, would provide a complete picture of how these tensions play out nation-wide.

Since the challenges identified are real and recurring, future investigation should aim not only to describe them further, but also to support the development of workable solutions that are currently lacking in practice.

7 Conclusion

This thesis examined how the General Data Protection Regulation (GDPR) is interpreted and applied during the design of user-centred public e-services in Estonia. Based on interviews with legal advisors, product owners and analysts, the study showed that GDPR is not experienced as a consistent or operational framework, but as dynamic shaped by role-specific interpretations, timing and communication practices.

All three research questions and two sub-questions were addressed through thematic analysis. The study found that interpretations of GDPR vary significantly across roles and stages of service development and while participants generally supported the regulation's aim, they also described recurring tensions between compliance requirements and usability goals. These tensions often surfaced from legal uncertainty, lack of structured organisational guidelines-processes or limited collaboration across legal and design roles. As a result, teams frequently adopted overly cautious approaches that protected legal defensibility but, on the other hand, constrained service usability.

The analysis showed that these challenges are caused not mainly by the regulation itself, but by how GDPR is applied and managed in design and development practice. The two institutional logics involved – legal compliance and user-centred design – often operated in parallel. With limited coordination or shared understanding, when risk or uncertainty increased, legal considerations tended to dominate, reflecting an estranged logic configuration, where compliance remains central but user experience is only partially integrated.

After the analysis, the author proposed several practical recommendations, directly informed by insights and proposals shared by the interviewed professionals and respond to systemic gaps identified in the study – such as fragmented collaboration, inconsistent interpretation of legal rules and late-stage legal involvement. These aim to reduce uncertainty, improve decision-making and support more user-conscious design outcomes in parallel with also GDPR compliancy, including strengthening the consistency of legal interpretation, involving legal expertise earlier in the process, improving access to institutional memory, clarifying team responsibilities and promoting a more proportionate compliance mindset.

Although limited to specific context, this study contributes to the practical knowledge of how legal and design priorities are negotiated in public sector service development. It highlights the need for structural as well as cultural changes that support integrated decision-making in environments shaped by such complex regulation. Future research could explore how end-users experience these trade-offs or how similar tensions are addressed in other public sector domains.

References

Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review, 2*(3), 287–289. https://doi.org/10.21552/EDPL/2016/3/4

Andmekaitse Inspektsioon. (2019). *Isikuandmete töötleja üldjuhend*. https://www.aki.ee/isikuandmed/juhendid-ja-materjalid/isikuandmete-tootleja-uldjuhend

Bans-Akutey, A., & Tiimub, B. M. (2021). *Triangulation in research.* Academia Letters, 2, 1-6. https://doi.org/10.20935/AL3392

Besharov, M. L., & Smith, W. K. (2014). Multiple institutional logics in organizations: Explaining their varied nature and implications. *Academy of Management Review, 39*(3), 364–381. https://doi.org/10.5465/amr.2011.0431

Cai, Y., & Mountford, N. (2022). Institutional logics in higher education: What we learn from the existing research and suggestions for future research. https://www.researchcghe.org/publications/research-findings/institutional-logics-in-higher-education-what-we-learn-from-the-existing-research-and-suggestions-for-future-research/

Chammas, A., Duarte, C., & Figueiredo, J. (2015). User-Centred Design approach for interactive systems. *Procedia Manufacturing, 3*, 5397–5404. https://doi.org/10.1016/j.promfg.2015.07.656

Chan, F. K., Thong, J. Y., Brown, S. A., & Venkatesh, V. (2025). Design characteristics and service experience with e-government services: A public value perspective. *International Journal of Information Management*, *80*, 102834. https://doi.org/10.1016/j.ijinfomgt.2024.102834

Clarke, V., & Braun, V. (2017). Thematic analysis. *The journal of positive psychology*, *12*(3), 297-298. https://doi.org/10.1080/17439760.2016.1262613

Claydon, J. (2013). Compliance/Legal Compliance. In: Idowu, S.O., Capaldi, N., Zu, L., Gupta, A.D. (eds) Encyclopedia of Corporate Social Responsibility. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-28036-8_353

Čtvrtník, M. (2023). Data Minimisation – Storage Limitation –Archiving. In *Archives and Records: Privacy, Personality Rights, and Access* (pp. 197-240). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-18667-7_8

Danielsen, F. (2021, June). Benefits and challenges of digitalization: An expert study on Norwegian public organizations. In *Proceedings of the 22nd Annual International*

Conference on Digital Government Research (pp. 317-326). https://doi.org/10.1145/3463677.3463703

de Hert, P., & Lazcoz, G. (2022). When GDPR-principles blind each other: Accountability, not transparency, at the heart of algorithmic governance. *European Data Protection Law Review, 8*(1), 31–40. https://doi.org/10.21552/edpl/2022/1/7

de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

EDPS. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* European Data Protection Supervisor. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

EEA Joint Committee. (2018). *Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 to the EEA Agreement*. https://eur-lex.europa.eu/eli/dec/2018/1022/oj

ENISA. (n.d.). *Data* Protection. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/about-enisa/data-protection/data-protection

Ernst & Young Baltic AS (2012). *Avaliku sektori äriprotsessid. Protsessianalüüsi käsiraamat.* https://dspace.ut.ee/items/57f19ade-9ff0-43eb-a21d-2c10a40247d9

European Commission. (2017). *European interoperability framework – Implementation strategy*. Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0134

European Commission. (2020). *A European strategy for data*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066

European Commission. (2021). *2030 Digital Compass: The European way for the Digital Decade*. COM (2021) 118 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0118

European Parliament & Council. (2022). *Decision (EU) 2022/2481 on the Digital Decade Policy Programme 2030*. https://eur-lex.europa.eu/eli/dec/2022/2481/oj

European Parliament and Council of the European Union. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Official Journal of the European Communities, L 281, 31–50. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

European Union. (2012). *Charter of Fundamental Rights of the European Union*. Official Journal of the European Union, C 326, 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2012/326/02

European Union. (2016). *Consolidated version of the Treaty on the Functioning of the European Union* (TFEU). Official Journal of the European Union, C 202/47. http://data.europa.eu/eli/treaty/tfeu_2016/oj

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

França, F., & Mont'Alvão, C. (2024). Privacy at the e-government within user-centered design and human-centered design context: a literature review. *DAT Journal*, *9*(2), 88–102. https://doi.org/10.29147/datjournal.v9i2.806

Franke, L., Liang, H., Farzanehpour, S., Brantly, A., Davis, J. C., & Brown, C. (2024, October). An exploratory mixed-methods study on general data protection regulation (gdpr) compliance in open-source software. In *Proceedings of the 18th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement* (pp. 325-336). https://doi.org/10.1145/3674805.3686692

Friedland, R., & Alford, R. R. (1991). Bringing society back in: Symbols, practices and institutional contradictions. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 232–263). University of Chicago Press. https://www.researchgate.net/publication/238198697_Bringing_Society_Back_In_Symbols_Practices_and_Institutional_Contradictions

Hashim, N. L., Yusof, N., Hussain, A., & Ibrahim, M. (2022). User Experience Dimensions for E-procurement: A Systematic Review. *Journal of Information and Communication Technology*, *21*(4), 465–494. https://doi.org/10.32890/jict2022.21.4.1

Hofmann, H. C., & Mustert, L. (2023). Data protection. In *Research Handbook on the Enforcement of EU Law* (pp. 461-475). Edward Elgar Publishing.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means*. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Isikuandmete kaitse seadus. (2019). RT I, 31.12.2024, 44. https://www.riigiteataja.ee/akt/131122024044?leiaKehtiv

Kotamraju, N. P., & Van Der Geest, T. M. (2012). The tension between user-centred design and e-government services. *Behaviour & Information Technology*, *31*(3), 261-273. https://doi.org/10.1080/0144929X.2011.563797

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16-44. https://doi.org/10.1177/02683962221141456

Lanamäki, A., Viljanen, M., Väyrynen, K., & Bennett Moses, L. (2025). Legal compliance and the open texture of law. *Journal of the Association for Information Systems, 26*(1), 1–8. https://doi.org/10.17705/1jais.00922

Lourenço, L. (2019). European Economic Area (EEA) and European Free Trade Association (EFTA). In *Research Handbook on the European Union and International Organizations* (pp. 529-545). Edward Elgar Publishing. https://doi.org/10.4337/9781786438935

Mahieu, R., Asghari, H., Parsons, C., van Hoboken, J., Crete-Nishihata, M., Hilts, A., & Anstis, S. (2021). Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens? *Journal of Information Policy*, 11, 301–349. https://doi.org/10.5325/jinfopoli.11.2021.0301

Majandus- ja kommunikatsiooniministeerium. (2024, November 26). *Digiteenuste arendamine*. https://mkm.ee/digiriik-ja-uhenduvus/digiteenused/digiteenuste-arendamine

Majandus- ja kommunikatsiooniministeerium. (2023) *European Digital Decade Strategic Roadmap: Estonia 2023 version. https://mkm.ee/sites/default/files/documents/2024-09/Estonian%20National%20Digital%20Decade%20Strategic%20Roadmap%202023.pdf*

Majandus- ja kommunikatsiooniministeerium. (n.d.) *Avalike digiteenuste tööriistakast.* https://digiriik.eesti.ee

Margetts, H., & Naumann, A. (2017). Government as a platform: What can Estonia show the world. *Research paper, University of Oxford*. https://www.ospi.es/export/sites/ospi/documents/documentos/Government-as-a-platform_Estonia.pdf

Mergel, I. (2019). Digital service teams in government. *Government Information Quarterly*, *36*(4), 101389. https://doi.org/10.1016/j.giq.2019.07.001

Mithun, A. M., & Yafooz, W. M. (2018, July). Extended user centered design (UCD) process in the aspect of human computer interaction. In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*(pp. 1-6). IEEE. DOI: 10.1109/ICSCEE.2018.8538388

Norman, D. A. (1986). Cognitive engineering. *User centered system design*, *31*(61), 2. https://www.researchgate.net/profile/Donald-Norman-

3/publication/235616560_Cognitive_Engineering/links/0c960536c18209b825000000/Cognitive-Engineering.pdf

OECD. (2020). *The path to becoming a data-driven public sector*. OECD Publishing. https://doi.org/10.1787/059814a7-en

OECD. (2024). *Global trends in government innovation 2024: Fostering human-centred public services*. OECD Publishing. https://doi.org/10.1787/c1bc19c3-en

Olev, A., & Alumae, T. (2022). Estonian speech recognition and transcription editing service. *Baltic Journal of Modern Computing*, *10*(3), 409-421. https://doi.org/10.22364/bjmc.2022.10.3.14

OpenAI. (2025). ChatGPT (GPR-4o) [Large language model]. https://chat.openai.com

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health and mental health services research*, *42*, 533-544. DOI:10.1007/s10488-013-0528-y

Patergiannaki, Z., & Pollalis, Y. A. (2023). Bridging the gap: assessing disparities in e-Government service offerings and citizen demand. *Transforming Government: People, Process and Policy*, *17*(4), 532-551. https://doi.org/10.1108/tg-04-2023-0050

Patergiannaki, Z., & Pollalis, Y. A. (2024). E-government quality from the citizen's perspective: the role of perceived factors, demographic variables and the digital divide. *International Journal of Public Sector Management*, *37*(2), 232-254.DOI:10.1108/IJPSM-07-2023-0229

RIA. (2025, February 20). *RIA juhendid*. Riigi Infosüsteemi Amet. https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/juhendid

Riigikontroll ja Õiguskantsler. (2018). *E-harta ehk Igaühe õigused e-riigis*. https://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Muudpublikatsioonid/Eharta/tabid/305/language/et-EE/Default.aspx

Roberts, N. C. (2011). Beyond smokestacks and silos: Open-source, web-enabled coordination in organizations and networks. *Public Administration Review*, *71*(5), 677-693. https://doi.org/10.1111/j.1540-6210.2011.02406.x

Root, V. (2019). The compliance process. *Indiana Law Journal, 94*(1), 203–251. https://www.repository.law.indiana.edu/ilj/vol94/iss1/5/

Saqib, S. I., & Allen, M. M. C. (2024). Institutional logics in play at work: How applying an institutional logics approach to employees' intentions to quit contextualizes HRM. *The International Journal of Human Resource Management, 35*(17), 2839–2862. https://doi.org/10.1080/09585192.2024.2382478

Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd international workshop on multimedia privacy and security* (pp. 88-95). https://doi.org/10.1145/3267357.3267368

Thornton, P. H., Ocasio, W., & Lounsbury, M. (2012). *The institutional logics perspective: A new approach to culture, structure, and process*. Oxford University Press.

Thornton, P. H., Ocasio, W., & Lounsbury, M. (2015). The institutional logics perspective. In R. A. Scott & S. M. Kosslyn (Eds.), *Emerging trends in the social and behavioral sciences* (pp. 1–22). John Wiley & Sons. https://doi.org/10.1002/9781118900772.etrds0187

Trinidad. (2014). *Kasutatavuse mõõdikute süsteem avaliku sektori tarkvarasüsteemidele.* https://digiriik.eesti.ee/juhend/kasutatavuse-moodikute-susteem-avaliku-sektori-tarkvarasusteemidele

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973–990). ACM. https://doi.org/10.1145/3319535.3354212

Vassil, K. (2016). *Estonian e-government ecosystem: Foundation, applications, outcomes*. Background paper for the World Development Report 2016: Digital Dividends. World Bank. https://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf

Veale, M., & Binns, R. (2017). When data protection by design and data subject rights clash. *International Data Privacy Law, 8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Welby, B., & Tan, E. H. Y. (2022). *Designing and delivering public services in the digital age* (No. 22). OECD Publishing. https://doi.org/10.1787/e056ef99-en.

Wolters, P. T. J. (2018). The control by and rights of the data subject under the GDPR. https://repository.ubn.ru.nl/handle/2066/194516

Yin, R. K. (2018). *Case Study Research and Applications - Design and Methods* . Los Angeles: SAGE Publications, Inc.

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS), 12*(1), Article 2, 1–20. https://doi.org/10.1145/3389685

Ziraff. (2014). Kasutajasõbralike e-teenuste disainimine Maanteeameti näitel. https://digiriik.eesti.ee/juhend/kasutajasobralike-e-teenuste-disainimine-maanteeameti-naitel

Appendix 1 – Interview Questions for Analysts & Product Owners

Interview questions (SET 1)

Background

1. What is your job title and what are your main responsibilities?
2. How long have you been involved in public e-service development?

Experience with the GDPR

3. In your daily work with public e-services, how have you encountered the GDPR?
4. At which stages of the designing process the GDPR usually comes up?
5. In your opinion, which GDPR principles or requirements have most influenced the design of e-services and its user-centred outcomes?

Organisational Processes

6. What guidelines, standards or frameworks exist in your organisation to ensure that GDPR requirements are considered during the design process?
7. How does collaboration take place between relevant stakeholders when balancing GDPR requirements with UCD goals?
8. How does your role support your organisation's ability to interpret and apply GDPR principles in the UCD of public e-services?

Conflicts and Tensions

9. How does your role support your organisation's ability to interpret and apply GDPR principles in the UCD of public e-services?

10. When such tensions or obstacles occur, how are they usually resolved in your organisation – is there any defined process or is everything handled case-by-case?

Suggestions

11. What do you think could help improve the balance between GDPR compliance and UCD in public digital service development?
12. If you could change any practice or process related to integrating GDPR into public e-services, specifically from a UCD perspective, what would it be?

Last thoughts

13. Do you have anything else to add regarding this topic?

Appendix 2 – Interview Questions for Legal Advisors

Interview questions (SET 2)

Background

1. What is your job title and what are your main responsibilities?
2. How long have you been involved in data protection matters?
3. How long have you been involved in public e-service development?

Experience with the GDPR

4. In what situations have you advised service development teams on GDPR-regarding questions?
5. In your opinion, which GDPR principles or requirements are the most difficult to implement at the design level?

Organisational Processes

6. What guidelines, standards or frameworks exist in your organisation to ensure that GDPR requirements are considered during the design process?
7. Does your organisation have specific internal mechanisms for handling situations where balance must be found between user-centricity and data protection?
8. How does collaboration take place between relevant stakeholders when such questions arise?

Conflicts and Tensions

9. What kind of situations have you observed where GDPR requirements have limited or even hindered UCD?
10. When such tensions or obstacles occur, how are they usually resolved in your organisation?

Suggestions

11. What do you think could help improve the balance between GDPR compliance and UCD in public e-service development?
12. If you could change any practice or process related to integrating GDPR into public e-services, specifically from a UCD perspective, what would it be?

Last Thoughts

13. Do you have anything else to add regarding this topic?

Appendix 3 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Diana Müürsepp

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "The Impact of GDPR on User-Centred Design in Estonian Public Sector E-Services: An Organisational Case Study", supervised by Eric Blake Jackson.
   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.

12.05.2025

[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.