UNIVERSITY OF TARTU
FACULTY OF SOCIAL SCIENCES
Institute of Social Studies
Knowledge and Information Management

Robert Väljur

Impact of GDPR on Personal Data Management - A Case Study

Master's thesis (15 ECTS)

Supervisors: Jake Tom, Maris Männiste

TARTU, 2018

CONTENTS

INTRODUCTION

The year 2018 brings in one of the biggest shake-ups in privacy laws when the new European General Data Protection Regulation (GDPR) applies to all European Union (EU) Member States on 25th May 2018 (Cornock, 2018). The aim of the GDPR is to harmonize data privacy protection laws between member states, although it is likely that member states will have differences in policy interpretation, to the purpose of protecting all EU citizens. GDPR does not only affect companies located in the EU but all organizations that offer services or goods to data subjects in EU.

European Union has declared non-compliant organizations that fail to comply with the GDPR must pay a fine up to 20 million euros or up to 4% of the total worldwide annual turnover preceding financial time, whichever is higher (Council of the European Union, 2016). Additionally, organizations which do not comply with the given regulation are faced with the high risk of reputational damage, which may hurt their business. This makes it essential for organizations to take required steps to comply with the regulation. To do so, all current business processes should be analyzed and reviewed for existing compliance. All non-compliant parts in the business processes should be modified, which can potentially also turn into new business opportunities by re-evaluating current processes and data processing needs.

Eesti Töötukassa is one of many organizations seeking to analyze their GDPR compliance and take necessary steps to ensure proper safeguards are implemented to protect their client's data. The initial focus of the thesis was to analyze two specific Eesti Töötukassa business processes (working ability allowance and working ability assessment) and assess if the data minimization principles defined in the GDPR (Article 5) are applied to them. The scope felt too narrow compared to results that could be derived from captured business process models, as highly detailed process models made it possible to evaluate additional articles of GDPR and thus increase the value of contributions made in this thesis.

The GDPR will affect data processing and data ownership dynamics but there is no proper assessment of the technological impact for an organization. This is because of the complexity of compliance analysis and lack of frameworks for it. This thesis will try to come up with a strategy how to assess the compliance of business process with GDPR policies using real-life compliance analysis case study process. Case study methodology has an advantage of the ability to capture complexities of real-life situations so that phenomenon can be studied in a greater

level of depth. The business process analysis is being conducted by borrowing elements from previous implementations of policies.

This brings us to our main research question: How will the GDPR affect the business processes and info system architecture in Töötukassa? The main research question is broken down into multiple sub-research questions (SRQ):

- SRQ1: How does the GDPR compare to the previous data protection directive (95/46/EC) and what parts of it are relevant to Töötukassa? The GDPR's predecessor already placed some constraints on the organizational handling of personal data. Before conducting the compliance analysis, it would be beneficial to understand what changes does the GDPR introduce.
- SRQ2: What changes would be needed to be implemented to make current processes comply and system architecture comply with GDPR? The purpose would be to recommend possible solutions to non-compliance issues if any exist.

The GDPR impact evaluation of this thesis produces an output which can be used to implement changes required for current processes and system architecture to comply with the new regulation. The results of this thesis can be scaled to other processes, projects and/or systems to be used as a guideline for assessing GDPR compliance or pinpointing the biggest compliance problems.

This thesis is separated into the following chapters: in chapter 2 research methodology used in the thesis are covered, chapter 3 covers overview of changes introduced with the GDPR, chapter 4 consists of case study business processes analysis and each GDPR article applicability to these processes, chapter 5 is compliance evaluation, chapter 6 reviews proposed solutions for non-compliant or partially compliant articles and the impact on system architecture, finally chapter 7 covers the validation part of the thesis.

2. BACKGROUND AND RELATED WORK

To understand analysis process used in the thesis, it is important to have an overview of methodologies in the research, which will show theoretical aspects benefiting the use of these methods. This chapter will give an overview of theoretical framework used to conduct this thesis. The topics covered will be previous practices in policy implementation and business process management notation used to document business processes.

2.1. Policy implementation

Although GDPR is, at the time of writing this thesis, new upcoming Regulation, the concept of policy implementation and assessing compliance with upcoming policies is quite common business practice. Due to that, it is important to learn from previous policy implementation case studies to understand possible different methods available for analyzing the compliance of existing processes towards the upcoming policy.

When it comes to policy implementation or compliance analysis, there are multiple different methodologies how one can assess the status of business processes. Kristie Ball (2010) has studied data protection implementation in an outsourced call center in South Africa by doing an exploratory case study. The data was gathered by observations during six month period, which allowed to have rich high-quality data set about the current processes. She gathered the data about how the customer service is managing the data by shadowing their daily activities, documented them (as interview texts, field notes, secondary documents) and then assessed the compliance of data protection safeguards (Ball, 2010). Although the assessment did pinpoint compliance issues, the resulting meetings with performance reviews did not result in any formal development. As there was no formal documentation or suggestions for improving the existing business processes themselves, the study resulted in acknowledgment that there are compliance issues within the call centers but no real improvement strategy was planned.

There are some studies that already concern the implementation of GDPR. A study made in Serbia (Krivokapić, et al., 2017) was done in two stages: first, by analyzing six public institutions and secondly by sending out targeted requests with more than 200 relevant questions. The first six institutions were important and significant data controllers owning huge databases, while some of them process especially sensitive data such as health information and data about adopted children (Krivokapić, et al., 2017). The initial part of the research was done

analyzing laws, bylaws, regulations and various documents regulating data processing, which also included a review of relevant international legal and policy frameworks. The second part consisted of desk research, which consisted of data from public sources, technical investigations and documents and information received via customized requests for access to information of public importance (Krivokapić, et al., 2017). This research started in 2015 and was quite time-consuming, which resulted in some findings of data quality and data security. The overall level of the data protection compliance was found to be good, but the study wasn't detailed about one particular institution and did not go into details about compliance to each GDPR article, thus serving more purpose as an overall guidance of possible compliance issues.

Some studies have taken another approach to assessing the compliance of business processes towards policies and standards – using the business process management with security risk-oriented (SRP) pattern technique (Alaküla & Matulevičius, 2015). Alaküla & Matulevičius (2015) used SRP to assess the compliance of insurance company business processes to the ISO/IEC 27001:2013 and found that SRP does contribute to the analysis, but there were also some limitations to using SRP. The limitations they found was described as: „For instance, ISO/IEC 27001:2013 (and other standards) does not only concern the computerised information management (i.e., access control, cryptology, or information classification). It also deals with (physical) human resource security, media handling, physical and environmental security, equipment and other.“ (Alaküla & Matulevičius, 2015).

Based on the different approaches taken by the previously presented studies, it seems that the most suitable option for this thesis would be the mixture of these, as the purpose is to understand the impact on one organization business processes, while also considering the scope of the thesis and the amount of workload required for conducting the data gathering and analysis. As such, next sections will consider case study research methodology and business process management techniques, which would be suitable methodologies for this thesis.

2.2. Case Study Research Methodology

The Case Study Research Methodology is strategic empirical research approach which is intended to be used for in-depth understanding of a complex issue in a real-life context. A case study as a research method is an established research design which is used extensively in a various variety of disciplines, for example in social studies (Crowe, et al., 2011). It can be

described as an intensive study on one case, which could be used to understand a larger number of cases (Gerring, 2011), thus perfect for analyzing GDPR impact on a business process which could then be used for assessing the impact on other business processes.

There are different definitions available for the Case Study Methodology, but Benbasat (Benbasat, Goldstein, & Mead, 1987) summarizes them as: "A case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations). The boundaries of the phenomenon are not clear at the outset of the research and no experimental control or manipulation is used".

As with definitions, there are also different views and categorizations of method approaches for case studies. One of the attempts to explain the different approaches was done by Ridder (2017), who classified four different method types: first being no theory first design, which follows Eisenhardt template of having no theory as restriction to capture the richness of the observation and where cases are selected by the theoretical likelihood of offering insights of the phenomenon. Second, gaps and holes, which, contrary to the first approach, is meant for advancing current theoretical frameworks. Third research design approach is social construction of reality, where the direction is shaped by the case, which aim is finding specific actions, in specific places and times, instead of identifying and measuring patterns which can be generalized (Ridder, 2017). Final, fourth, approach is to identify the anomalies in the case, where the focus is usually on interesting and outstanding situations, which existing theories cannot explain (Ridder, 2017).

According to Sarah Crowe (Crowe, et al., 2011), there are four stages when conducting case studies:

1. Defining the case – case methodology is useful when the natural setting is needed.
2. Selecting the case(s) – a choice between one or multiple cases used in the research.
3. Collecting the data – capturing data and complexity surrounding the research.
4. Analyzing, interpreting and reporting case studies

There are multiple advantages for using the case study methodology: data examination within the situation where it is used, ability to use both quantitative and qualitative analysis, qualitative data capturing from real-life scenarios which might not be recorded with a survey or experimental research (Zainal, 2007).

Although there are a lot of benefits for using case studies as research methodology, some disadvantages exist as well – often case studies are accused of insufficient thoroughness, dependency on single case exploration or with a massive amount of documentation (Zainal, 2007). Some of the disadvantages can be prevented and turned into advantages by taking in measures that will minimize the risks. Thoroughness of the case study can be increased by taking in multiple cases to prevent dependency of a single case. Using multiple cases also makes the case study more generalizable, which means the results can be more easily scaled to similar content to the research context.

For the thesis, I will be using no theory first case study approach, which enables to capture the richness of observation and allows the selection of business processes which have theoretically the highest probability of not complying to GDPR. This also enables the possibility to generalize the results, meaning that the methods and activities done in this thesis could be scaled up and applied to other business processes, which is one of the goals set in this thesis.

2.3. Business Process Management

Business Process Management (BPM) is an important systematic approach, which is used to for the identification and structuring of business processes (Paiano, Caione, Guido, Martella, & Pandurino, 2015). A business process is set of activities and events that need to be completed to accomplish organization (governmental, non-profit organization or enterprise) goal (Dumas, et al., 2013). BPM is used for optimizing current and future processes by analyzing the organizational context and activities performed by different actors in one or multiple business processes. BPM can be used for optimizing processes, which include typical problems like reducing the cycle time of the process (by eliminating or re-routing an activity performed in a process), reducing costs (removing or replacing non-value adding activities) or error minimalization (removing or improving activities which produce a high amount of errors).

BPM is usually performed by a business analyst, who will analyze business context and based on gathered information forms or improves existing business process model, which is usually visualized using graphical representation notation, such as Business Process Model and Notation (BPMN). BPMN represents the workflow of given business process using notational and diagramming elements.

BPMN is business process modeling language, which is used to provide businesses process visualization. The purpose of BPMN is to provide means to have common notation

understandable by a business analyst, business technical and business people who manage and implement given business processes (El-Bakry & Mastorakis). As of 2011 January, BPMN 2.0 was released by Object Management Group (OMG), an organization that guides standardization of BPM (OMG, 2011). The 2nd version added messages exchange between actors and interactions between participants of the process (Kožíšek & Vrana, 2017).

BPMN defines and Business Process Diagram, which is based on flowcharting technique and made of a set of graphical elements (White, 2004). BPMN includes five basic elements, which have different variations:

- Flow Objects (objects 1 -5 and 12 in Figure 1)
- Data (object 8 in Figure 1)
- Connecting objects (objects 9-11 in Figure 1)
- Swim-lanes and pools (objects 6 and 7 in Figure 1)
- Artifacts (objects 13-15 in Figure 1)

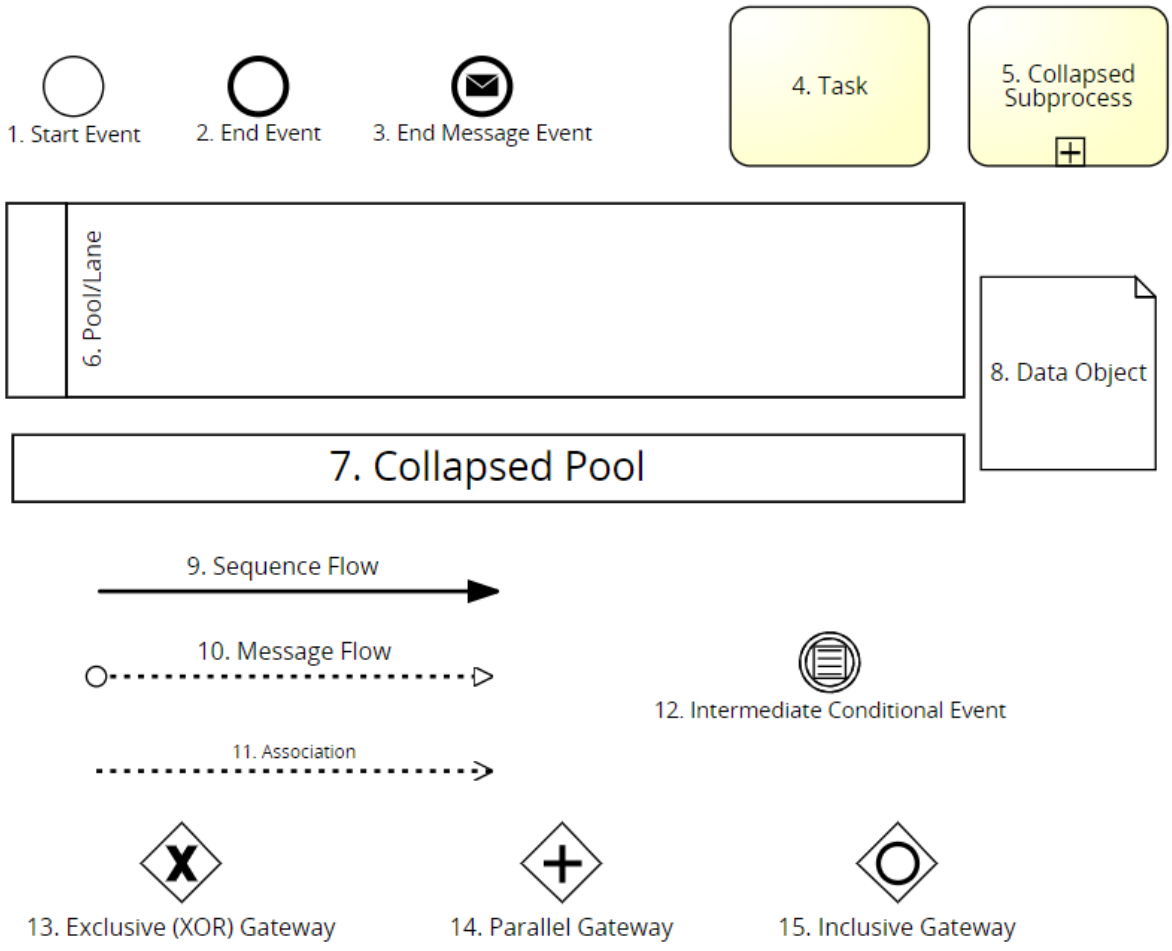

Figure 1. BPMN 2.0 Elements used in this thesis.

The benefit of using BPMN as notation language to visualize business processes is its big community that has accepted the notation as standard. Using standardized notation helps to reduce the fragmentation that can be caused by using notation that is not universally understood or agreed upon, thus increasing the risk that there will not be a common understanding of the process that is documented by the business analyst.

2.4. Summary

In this chapter, I reviewed previous policy implementation techniques and described methodologies used in this thesis. The selected research methodology is no theory first case study approach, to capture the richness of observation and select business processes which have theoretically the highest probability of not complying with GDPR. In addition, existing research regarding data protection policies and business process compliance analysis was presented along with a primer on BPMN concepts used in this thesis.

3. GDPR OVERVIEW AND NEW CHANGES

With the advances in technology our economy, communication, and multimedia usage evolve as well. Every day more activities, objects, and possibilities are moving online – we are moving towards self-driving cars that use network and sensors to measure our position towards other objects, we have lamps that can be controlled by mobile phones, saunas which can be activated and pre-heated while you are shopping 20 kilometers away from home or when we do not feel like going to shop ourselves, we can order everything with just a few clicks or taps from our smart devices. Each of these amazing advances in technologies has become possible by sharing and processing data around us and what is stored in the network.

While there are amazing things to be done with data, there are also corporations that wish to exploit personal data to use it for marketing activities and other business purposes. Personal data can be used to analyze the habits and preferences of data subjects to use them for different advertisement campaigns or influencing their daily choices, for example, data compromise case that happened with Facebook due to Cambridge Analytica (Hern, 2018). Aside from the potential abuse from corporations, there are also criminal minds that may want to use it for their own enjoyment or benefit – stealing money from credit cards, using personal data, like home address and social media boards, to track your moving habits to understand when you are not at home or what would you be most gullible to buy. To minimize the risks of private data misuse and to protect their citizens, European Union has passed in a General Data Protection Regulation (GDPR) which was created with the noble intention to increase control of personal data for citizens and prevent the abuse of personal data by corporations.

The GDPR is a regulation aimed to manage the processing (includes collecting, sharing, aggregating, etc.) of personal data, where's personal data is considered to be any information relating to an identified or identifiable natural person (data subject) (Council of the European Union, 2016). There are special categories for personal data (sensitive data), which is under extra protection because its processing can cause significant risks to data subject personal rights. An interesting thing to note is that, by recital 27, the regulation does not apply to the personal data of deceased.

The principles of data protection and regulating these principles is nothing new, as GDPR is based on Data Protection Directive (Directive 95/46/EC). As such, GDPR modernizes the previous principles by regulating data protection in a context where the amount of available information about data subject has increased significantly, due to multiple ways to collect and

process such data, which means existing old legislation is no longer fit for purpose (Cornock, 2018). Additionally, there are some new concepts that were introduced as well – right to be forgotten, data portability, data breach notification, data protection officer). The GDPR consists of 99 Articles, which can be summarized to three main objectives: to provide rules for the protection of the personal data of natural persons and the processing of their personal data, to protect the fundamental rights and freedoms of natural persons and to ensure that personal data can move freely within the European Union (Cornock, 2018).

The aim of this chapter is to give an overview of biggest changes that GDPR introduces, thus answering sub-research question one (SRQ1), and reviewing some of the key aspects of which should be considered when assessing the applicability of the GDPR articles to the case study use cases and compliance of the applicable articles.

3.1. General provisions and principles

The GDPR introduced multiple new principles, clarified or added definitions and extended multiple existing principles. Some new definitions are pseudonymization, which is a privacy enhancing mechanism, concepts of risk and high risk to individuals, the distinction between personal data and sensitive personal data, and data breach (Linklaters, 2017). Additionally, GDPR increased the territorial scope of data protection with Article 3 to include applicability to organizations that process data of data subjects who are in the Union. This means that companies who are not in Union jurisdiction must also make sure they comply with the GDPR. This means that organizations that provide goods or services to the people in EU (Amazon, Google, Samsung) must make sure that they comply with the GDPR, appoint a representative in the Union and adopt appropriate safeguards.

An important addition to definitions is the distinction between personal data and sensitive personal data, which was added by the GDPR. Personal data is considered to be any information that is relating to identified or identifiable natural person (data subject), this can be simple things like phone number, home address, national identification number or name, but also technical information that can help to identify a person, for example, Internet Protocol (IP) address. The completely new distinction to personal data is special categories of personal data – sensitive data, which has extra protection, because their processing can create significant risks to fundamental rights and freedoms (Council of the European Union, 2016). Examples of sensitive

personal data are genetic information (inherited or acquired genetic characteristics), biometric information (facial image), racial or ethnic origin, data concerning health or sexual orientation.

With GDPR, most of the provisions and principles remain the same, while there are some additions: accountability, processing which does not require identifying and transparency of data processing (Tikkinen-Piri, Rohunen, & Markkula, 2018). Accountability principle is added to make sure that personal data being processed is always up to date, accurate and reasonable steps are taken to make sure the inaccurate data gets corrected (Council of the European Union, 2016). This means that organizations need to be able to demonstrate that collected data is managed correctly. Article 11 introduced the principle where the controller can process data which does not require identification and thus is no longer obliged to maintain or process additional information to identify the data subject for the sole purpose of complying with this Regulation (Council of the European Union, 2016). With the transparency principle, the organizations need to have documentation of their data processing and list of third-party sources in clear language with contact information.

Additionally, some principles were clarified: conditions for consent, data minimization and criteria for lawful processing (Tikkinen-Piri, Rohunen, & Markkula, 2018). Although there was already a requirement to ask for person's consent, which needs to be given freely, when processing his or her data, this requirement was extended with the GDPR. A person is now able to withdraw the consent in which case all corresponding processing needs to be stopped – this also means that organizations need to start supporting the withdrawal of consent. Additionally, organizations that received the request for consent withdrawal must notify other organizations, of whom to the personal data was shared, of the request. The new regulation also regulates the consent of children, ensuring children's rights are being safeguarded and ensuring they understand the information provided to them (under 16 years require parental consent). There may be exceptions in some Member States, as they can lower it to children at the age of 13 years (Council of the European Union, 2016).

Another important principle clarified is data minimization which is described in Article 5 paragraph 1c as: "adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed" (Council of the European Union, 2016). This means that an organization should only process such personal data which is needed to achieve its processing purposes (for example grocery store should not ask an individual to provide his or her occupation since it is not needed for providing a service).

3.2. Rights of data subject

The rights of the data subject are covered in Chapter 3, Articles 12 - 23 of the GDPR. With processing, the controller must take appropriate measures to provide information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, for any information addressed specifically to a child (Council of the European Union, 2016). This means that organizations must ensure that proper communication is in place when dealing with personal data, especially in case of a data breach. Additionally, data subjects can object the processing of their data, subject decisions based on automated processing or profiling and request rectification of incorrect data.

Another right introduced is the right to be forgotten principle - (in some cases partial) erasure of personal data. This means data subjects can, in certain conditions, request for the complete erasure of their data. Data should also be deleted when the retention time is over. However, there are cases where such requests can be denied or the erasure of data shall be partial, for example, in cases where data needs to be stored for proof or future analysis of fraud cases (e.g. in banks).

Article 20 introduces a requirement that data should be portable, which means that the individual has the right to request access to their data in a way that can be read by them. The data subject can also request the data to be ported from one controller to another controller, for example transferring personal data from one service provider (Rimi) to another (Selver).

What these rights mean to organizations is that they must implement new functionalities in their infosystems and activities in their existing business processes – in smaller organizations, the number of requests can be low and fulfilling these requests can be managed manually, but with a larger number of requests, the workload will be manually unmanageable. Organizations need to be aware how and why they store the personal data, to be able to fulfill, or with plausible reason deny, the requests of data subjects.

3.3. Data transferring outside EU

There are specific rules regarding transferring data outside of the European Union, which was introduced in Chapter V of the GDPR (Council of the European Union, 2016). These rules exist to ensure that the individual’s rights are not reduced by the laws in the country receiving the data (Cornock, 2018). This means that data can be shared with third countries or organizations only in cases where appropriate safeguards are adapted and able to demonstrate such protection.

In case of USA, the organizations to whom data is transferred must be certified under Privacy Shield. In the absence of an adequacy, decision transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules, consent etc.

3.4. Data Protection Officer

The GDPR introduced new obligation to organizations to hire a data protection officer (DPO) in case where: "the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10." (Council of the European Union, 2016). This means that DPO will be a mandatory addition to the data-intensive and customer-facing organizations, where personal data is being used for products or services where data can lead to identifying the individual.

The responsibilities of the DPO include informing and advising the controller or the processor, monitoring compliance with the Regulation, cooperation with superior authority, acting as a contact point for issues related to data processing, train employees and assist with data protection impact assessment, as stated in Article 39 of the GDPR. This means that DPO will be responsible for making sure that the organization where he or she works is compliant with the GDPR. For that purpose, DPO must be appointed in writing and appropriate resources must be assigned to him or her.

3.5. Liabilities and penalties

Chapter VIII defines the liability and penalties for breach of the GDPR. For liabilities, the GDPR defines that the data subject has the right to lodge a complaint to supervisory authority if he or she considers that processing of his or her data processing is not compliant (Council of the European Union, 2016). An important aspect to note is that with GDPR not only each controller but also each processor is held liable for the entire damage caused to the data subject (Tikkinen-Piri, et al., 2018).

If the organization fails to comply with the Regulation, supervisory authorities have the right to fine such infringements. There are different amounts of maximum fines defined, dependent on the category of the infringement and each violation is assessed separately. The fines can be up to 20 million euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (for example when a violation of basic principles or the data subject rights takes place.).

It is important to note recital 151 where there is a clause about administrative fines in Estonia and Denmark, stating: "The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanor procedure, if such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities." (Council of the European Union, 2016). As such the courts of Estonia and Denmark should consider the recommendation by the supervisory authority initiating the fine (Council of the European Union, 2016). This means that courts of Estonia and Denmark should impose fines that are effective and proportionate.

3.6. Summary

In this chapter I have reviewed the changes introduced with the GDPR compared to the previous data protection directive (95/46/EC), answering sub-research question one (SRQ1). Although GDPR did add some new principles, extended the existing ones and modernized largely how personal data should be processed, it should still be considered as an opportunity for organizations to improve their data processing procedures, making them more clear to their data subjects and due to that possibly even simplifying the existing business processes. Similarly, BeCrypt Ltd. CEO Bernard Parsons has described their GDPR compliance preparation as an opportunity to reevaluate company's business processes, find new activities and measures to make current processes more effective and simple. It also prompted them to think about what data they are gathering, how they are processing it and how it affects them if the data is lost (Ltd., 2018).

The GDPR introduced additional rights to data subjects, to ensure their fundamental rights are protected when organizations process their data. This also includes data transferring or data

portability, making sure the data subject can access the data being collected about them or that their rights are protected in the countries outside EU. To make sure that data processing is being managed properly, data subjects are informed of data breaches or about their personal data being processed and that organizations have appropriate safeguards in place, large organizations are required to employ DPO, who would guide and analyze on any existing or upcoming business process. Failure to comply with the GDPR means that organizations can get severe fines.

4. GDPR IMPACT ON BUSINESS PROCESSES

This chapter will review what articles of GDPR are relevant to the case study. To assess GDPR impact on business processes and system architecture, there needs to be a real business case to evaluate the compliance on. Per Sarah Crowe (Crowe, et al., 2011), before selecting the cases for the research, it is important to define the case itself. As such, I gave an overview of GDPR and analyzed key changes that it introduced in section 3 of this thesis.

For the selection of cases, Eesti Töötukassa agreed to be the subject organization of my thesis. After getting familiar with Eesti Töötukassa activities and responsibilities by understanding the context of its business processes, I could select the processes which I will use in the case study (see section 4.1). Processes used in this thesis was selected with the help of Töötukassa and Nortal by assessing the technical complexity and the number of activities where personal data is being processed, thus having the highest probability of compliance issues. The idea was to select the processes which assessment would benefit the most for all three parties.

To conduct compliance analysis, it was important to capture data about the processes under study and the complexities behind them. This was done by mapping and modeling the existing state of selected business processes (see section 4.2). Once the data was gathered and captured, it was possible to start with the compliance analysis.

Analysis of the compliance is divided into multiple parts. First, analyzing the applicability of given business processes per each article in GDPR (see section 4.3). Having done the applicability analysis, I could assess the compliance of business processes captured in section 4.2 based on GDPR keyword analysis from section 4.3 and suggesting measures for compliance, if applicable (see section 4.4). Following the analysis in section 4.4, I will evaluate the current system architecture and derive new technical requirements for the system architecture to be compliant with the GDPR (see section 5).

4.1. The context of case study business processes

Eesti Töötukassa (unofficially Estonian Unemployment Insurance Fund) is a quasi-governmental organization, which acts as a legal person in public law, that administers the social insurance provisions related to unemployment and organizes labor market services (About Töötukassa, 2013). Eesti Töötukassa activities are based on the Unemployment Insurance Act which describes the unemployment insurance system and the organization of

Töötukassa, and the Labour Market Services and Benefits Act, which contains the provisions concerning job mediation and related services (About Töötukassa, 2013).

To get most out of the business processes compliance analysis the chosen processes should be complex and have multiple interactions and processing of personal data. For that purpose, there were two processes chosen with the help from Töötukassa, which would potentially have the biggest amount of actions to do with processing personal and delicate data and therefore biggest possibility to have non-compliant activities in the processes – working ability assessment and working ability allowance workflows. Both of these processes collect and process personal data and sensitive personal data (see section 3.1 for definition), such as health information, disability information, working ability assessment, genetic information in info system named TETRIS. Töötukassa does not store all of the processable personal data information in their system database – some of the data is retrieved through X-Road from third-party (and sometimes third-country) infosystems (for example Health Information System, Business Register). The basis of the personal data collection and processing in Töötukassa is Working Ability Allowance Act, Statute of the Unemployment Insurance Database (which states what data is to be collected and from whom), Public Information Act and Archives Act.

Working ability assessment was launched by Töötukassa on 1th of July 2016 and is solely conducted by Töötukassa as of 1th of January, 2017 (Eesti Töötukassa, 2016). The purpose of the working ability assessment is to assess the working capability of people with decreased working ability and their working ability allowance.

The methodology for the assessment of working ability is based on the principle that every individual is unique and the same disability or illness may manifest itself very differently in different people (Eesti Töötukassa, 2016). Assessing working ability consists of checking person's state of health along with restrictions on activities and participation that arises from it. The assessment includes evaluation of physical (walking, climbing stairs, body positions) and mental abilities (responding to different situations, acquiring skills, contacting people) in different areas.

There are five main steps in working ability assessment:

- The submission of working ability assessment application.
- A doctor's visit (unless visited six months prior to application).
- The preparation of an expert opinion (conducted by an expert who is not an employee of Töötukassa).

- Decision making on the scope of working ability assessment (the decision is in force up to five years, in severe states until retirement).
- The payment of a working ability allowance (additionally advice and labor market services, if necessary).

Working ability allowance is a Töötukassa business process, which is performed after (can be started at the same time) working ability assessment has been completed and the person has the right to receive the allowance. The payment of allowances can be stopped temporarily or permanently if a person fails to follow Töötukassa guidelines or procedures, for example appearing on consultations, refusing suitable jobs or failing to comply with activity requirements.

Per Töötukassa (Eesti Töötukassa, 2016), there are multiple different groups of people that are eligible for working ability assessment (age of 16 until retirement age):

- Estonian citizens residing in Estonia.
- Aliens residing in Estonia based on a residence permit or right of residence.
- Persons enjoying international protection staying in Estonia or asylum seekers staying in Estonia who have the right to work in Estonia under the Act on Granting International Protection to Aliens.
- Residents of Estonia who reside in several states, if they are residents for the purposes of the Income Tax Act or if they reside permanently in Estonia for the purposes of the Aliens Act.

4.2. Activities prior to compliance assessment

Before analyzing the compliance of existing business processes, it is important to understand and document the process itself. To document the existing business process, I am using BPMN version 2 (discussed in section 2.2), which allows the capture of current activities, relationships between actors and data objects used in the processes.

Prior to GDPR compliance conducted in this thesis, there was partially some documentation in place capturing the existing business processes, but these were scattered among multiple places within the document management system. Existing business models did not use BPMN 2.0 notation which would provide the most effective overview and the process documentation was not up-to-date. Additionally, the working ability allowance business process did not have a

model covering the whole process but was scattered to multiple separate process models and documents. This meant that to start with the compliance analysis it was necessary to update existing models and fix the notation to be compliant with BPMN 2.0 standard.

To fix the existing models, I used BPM software Signavio. For updating the business processes, I organized meetings with analysts from Nortal that are working on Töötukassa project. Once the existing models I found was converted into BPMN 2.0 notation, I had multiple sessions and e-mail exchanges with Nortal analysts, who reviewed the updated models and gave feedback to improve my models upon. Once the models were confirmed with Nortal analysts, it was then confirmed with Töötukassa, who gave additional feedback, which was used to improve the models.

Since the two cases selected for a case study in this thesis were quite complex, the outcome of data captured was big detailed models which were hard to follow. Due to that, I captured some of the repeating activities into subprocesses and I created an additional version of working ability allowance model, which was simplified and reduced to a data-centric view focused purely on capturing personal data aspects relevant to the GDPR, which was important for GDPR compliance analysis. Since the initial working ability allowance process was not used for the evaluation of compliance, it is added as an appendix (see Appendix 1, Figure 1).

The result of the fixes and updates of two main processes can be seen in Appendix 1, Figure 2 (working ability assessment) and Figure 4 (working ability allowance). Working ability assessment was additionally split into two: the main process itself and the doctor evaluation subprocess (see Appendix 1, Figure 3). Working ability allowance process was also split into multiple processes: main process itself can be seen in Appendix 1, Figure 4, getting or adding client into or from EMPIS system (internal Töötukassa info system) is shown in Appendix 1, Figure 5 and external info systems subprocess can be seen in Appendix 1, Figure 6. The external info systems call is being done when data subject application is submitted into the system to check if the request for allowance and working ability assessment is valid.

The models include data objects, which represent the information being stored, exchanged or processed. Data objects, which have too many fields, to be captured into process models, have IDs assigned to them and these data objects are included in the tables added in the appendix (see Appendix 2). Similarly, each activity in current process models has IDs assigned to them, which helps in identifying and referring the non-compliant activities in compliance analysis presented in chapter 5 and proposed solutions in chapter 6 with the business process models.

4.2.1. Working ability assessment

Working ability assessment process is captured in Appendix 1, Figure 2. Working ability assessment consists of the following activities: requesting the assessment, verifying the application, evaluation by the expert doctor, evaluation by the Töötukassa doctor and final decision.

There are multiple ways of which a person can request for a working ability assessment – through email, application through ITP or SKA portals or from the physical request in the on-site. On-site and through email applicants will have authentication done by the Töötukassa case manager, otherwise the authentication and authorization (in-case of the person requesting assessment on behalf of somebody else) are done by the info system. In order to submit the application person will have to sign the consent form (on-site) or confirm it online through the self-service portal. The application covers a variety of personal data, including genetic data, previous work experience, education and health information (see Appendix 2, tables 18 and 19). After the application is submitted, the requester (and representor) is identified and/or added to the system, the case manager and proceedings handler will check if the application is valid or some data is missing or otherwise incorrect, which will then be corrected by the requester.

Once the application is processed for initial errors and validated, the requester health is being examined (activating the sub-process represented in Appendix 1, Figure 3). For that purpose, a service provider as the expert doctor is chosen from the external Töötukassa partners. The expert doctor will evaluate the application and initial information in e-Health system, after which the doctor decides whether an interview (health examination) or additional data is required. In case of additional data requirement, the applicant is requested to fulfill additional form for extra information. In case of an interview, the applicant has the possibility to request compensation for travel expenses (not covered in this thesis) and the interview is conducted. Once the gathering of extra information is over, the expert doctor provides his or her expertise on the TETRIS system. The health data available in e-Health is not stored in Töötukassa TETRIS info system (unless manually copied by doctors in the comments section). The expertise will be reviewed by the Töötukassa doctor, who assesses whether additional information is required or expertise needs fixing. Once the expertise is confirmed, the decision is being added by the proceedings handler. Once the decision is added and confirmed, notification and decision are being sent to the applicant.

4.2.2. Working ability allowance

Working ability allowance process is captured in Appendix 1, Figure 4, which represents the process from applying for the allowance, verifying the application, assessment of allowance applicability, calculation and the payment of the allowance. Working ability allowance is based on working ability, as such, it is reliant that the assessment has been done before allowance applicability can be assessed.

Similarly to the working ability assessment application, the working ability allowance application can be done through email, online or on-site. Requester data is requested from EMPIS system – if a person does not exist, he or she will be added to the system (see Appendix 1, Figure 5). The application can be submitted once the consent is given, after which the validation and background check is automatically started by the system (see Appendix 1, Figure 6 and section 4.2.3). Simultaneously the application is reviewed and in case of issues, fixes are to be made by the applicant (notification will be sent to the user based on the preferences he or she set on notification delivery methods). Once the application is accepted (or denied, in which case applicant is notified of the decision), allowance eligibility assessment is completed with the calculation of allowance. Proceedings handler will verify the calculation and perform the additional check, if necessary. When the proceeding handler accepts the calculation, the accountant will check the payments and export the payments to the accounting system, after which the payments are made, based on the payment method chosen by the applicant.

The validation of allowance eligibility and calculation of the payment sum is being conducted each month before the payment, due to the fact that previous conditions for which the payments were calculated might not be valid anymore.

4.2.3. External infosystems background check

The external infosystems background check is a sub-process of which the applicant is being assessed on the applicability for the working ability allowance and additional data is requested for the ability allowance calculation. The external infosystems checks are being done using the X-Road endpoints, which are provided by other government organizations. Each request is and the response is logged and saved in the database, with the exact date of which the response was received (required for tracking and calculations).

The external calls are:

1. Activity IA3, responses RR435.v1; RR436.v1 (get detailed data about the person) - Population Register.
2. Activity IA5, EMPIS (checks for unemployment status, Töötukassa internal info system).
3. Activity IA6, Business Register (check if FIE or some company board member).
4. Activity IA7, Employment Register (check employment history).
5. Activity IA8, Tax and Customs Board (check spouse FIE and non-residency status).
6. Activity IA9, Police and Border Guard Board (check treatment or substitution penalties).
7. Activity IA10, Social Insurance Board (check disability, pension, other allowances status).
8. Activity IA11, Defence Resources Agency (check for ongoing military service).
9. Activity IA12, Social Services and Benefits Registry (check persons under care).
10. Activity IA13, Education Information System (check education history).
11. Activity IA14, Persons Detained Registry (check the criminal record).
12. Activity IA15, (check rescue service allowances).

External info system calls are all available through X-Road system, and the request-response templates are publicly available in RIHA (Riigi Infosüsteemi Haldussüsteem) database.

4.3. GDPR keyword analysis

Before starting the analysis of compliance with the case study use cases, it is important to understand the contents of the GDPR and the applicability of articles in Regulation on Töötukassa business processes in this case study. For this purpose, I conducted keyword analysis on each chapter of the GDPR and assess each article applicability on Töötukassa. The purpose of doing keyword analysis is to capture the most relevant ideas with each article to make the article easier to understand for manual relevance assessment on the scenarios reviewed in this thesis. The applicable articles are further analyzed in chapter 5 compliance evaluation.

4.3.1. Chapter I: "General Provisions"

The chapter General Provisions articles cover the scope and objectives of the GDPR, which is summarized in Table 1. Additionally, this section has Article 4, which consists of definitions used and important to understand different aspects of the GDPR. It is notable because this introduced multiple new terms that are used to define different actors and classifications used in the Regulation, such as sensitive personal data, pseudonymization, data protection officer, etc., which were reviewed in previous chapter 3. As it sets the overall scope and definitions used in the GDPR, this chapter is not applicable to Töötukassa processes in applicability assessment.

Article	Summary	Keywords	Applicability (Y/N)
#1	Defines subject-matter and objectives of the GDPR.	Regulation purpose	N/A
#2	Sets the scope where GDPR applies.	Regulation scope	N/A
#3	Defines the territorial scope where GDPR applies. GDPR applies also activities of processors or controllers outside of the Union if data subjects are members of the Union.	Data subjects in the Union, territorial scope, international law	N/A
#4	Definitions.	Definitions	N/A

Table 1. General Provisions.

4.3.2. Chapter II: "Principles"

Principles chapter describes data protection and lawful processing principles that are to be followed by the upcoming Regulation. The purpose of these principles is to make sure that personal data is processed lawfully, fairly and in a transparent manner. The overall changes to principles, introduced with the GDPR, is discussed in section 3.1 of this thesis.

Overall all articles in Chapter II of the GDPR are applicable to Töötukassa, as shown in Table 2. While article 5 describes the processing of personal data and article 6 defines the criteria for lawful processing, the article 7 describes the conditions where processing can be based on consent. It should be noted that processing of personal data based on consent should only be done for the purposes stated in the consent. Further processing is only possible in case of reasonable causes, for example, public health services management or national statistics. Based on recital 33, processing for the scientific research should be based on separate consent and

data subject should be able to give consent only to certain areas of the scientific research or parts of research projects. This means that the data subject should be able to choose the studies he or she would want to be part of, except research done by national authorities with lawful reasons, like for social care system, legal claims or public interest.

In this chapter, Article 8 describes the conditions for child's consent in relation to information society services. Information society service is, by Directive 2015/1535 (European Parliament and of the Council, 2015), any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. A child, based on Estonian Child Protection Act (Riigi Teataja, 2018), is considered in Estonia to be a person under the age of 18. By recital 38 of the GDPR, children merit special protection in regard of processing their personal data, because they might not be aware of the possible risks, consequences and safeguards available with regard to using services offered directly to them (Council of the European Union, 2016). As per GDPR article 8, the processing of personal data based on consent is lawful from age of 16, the parental agreement is required for children under 16. Member States are allowed to lower the age requirement to a minimum of 13 (Council of the European Union, 2016). It is possible to request the working ability allowance by the age of 16 but working ability assessment can be done for children under 16 (Riigi Teataja, 2018). As such, the article 8 is applicable to Töötukassa.

Article 9 defines the lawfulness of processing sensitive personal data. Paragraph 2h of article 9 states that the paragraph 1 of the article does not apply if processing is necessary due to social care systems and services in the Member State law, which applies to Töötukassa based on Work Ability Allowance Act (Riigi Teataja, 2018). Based on article 9 paragraph 2h and the Estonian Work Ability Allowance Act, the sensitive personal data processing by Töötukassa is lawful.

Article	**Summary**	**Keywords**	**Applicability (Y/N)**
#5	Principles relating to the processing of personal data.	Processing lawfulness, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability	Y

#6	Lawfulness of processing.	Processing lawfulness	Y
#7	The article describes the conditions for data subject consent for processing to be valid.	Data subject consent, consent withdrawal	Y
#8	Conditions applicable to child's consent in relation to information society services.	Child’s consent	Y
#9	Processing of special categories of personal data.	Identifying data subject, the lawfulness of processing	Y
#10	Processing of personal data relating to criminal convictions and offenses.	Processing criminal convictions and offenses	Y
#11	Processing which does not require identification.	Maintenance of personal data, informing the data subject	Y

Table 2. Principles.

4.3.3. Chapter III: “Rights of Data Subject”

Chapter “Rights of Data Subject” introduces and expands multiple concepts that ensure the lawful and correct processing of personal data of the subject. The full review of additions and changes of principles to the processing of data is introduced in section 3.

There are multiple articles in this chapter which could be translated differently by organizations that are conducting the compliance analysis or following the Regulation in the day to day business activities. As such, my conclusions are not final and each organization should thoroughly review these in their business context and laws applicable to them. One of those articles is Article 17 concerning the principle right to erasure (right to be forgotten). Although the data subject has the right to demand deletion of his or her personal data, in situations mentioned in paragraph 1 of the article, there are cases where that article does not apply, which are explained in paragraph 3 (Council of the European Union, 2016). In there are two sections, in which case the requirement of erasure of personal data would not apply:

- 3b, which states that the article does not apply in cases where data processing is required for obligations set by Member State law to which the controller is subject (assessment of working ability for social services);
- 3e, where it says: “for the establishment, exercise or defence of legal claims”, where Töötukassa case would apply due to the requirement of traceability, reasoned by possible fraud cases (data subject receives payments due to incorrectly presented personal data).

Due to these exceptions, my conclusion is that Article 17 does not apply to Töötukassa in the context of business processes analyzed in this thesis.

The reason for Article 20 is not applicable to Töötukassa comes from the article paragraph 3, which states that the right does not apply when processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller (Council of the European Union, 2016). The article 23 allows the Member States to restrict articles 12-22, 34 and 5. This would mean that these restrictions would apply to Töötukassa as well, but at the time of writing this thesis, there are no additional restrictions added by Estonia.

Article	**Summary**	**Keywords**	**Applicability (Y/N)**
#12	Transparent information, communication and modalities for the exercise of the rights of the data subject.	Informing of data collection, data identification, the timeline for data identification, handling of data subject requests	Y
#13	Information to be provided where personal data are collected from the data subject.	Informing of data collection, data storing period, rights of the data subject, automated decision-making notification	Y
#14	Information to be provided where personal data have not been obtained from the data subject.	Informing of data collection, data storing period, rights of the data subject	Y

#15	The right of access by the data subject.	Article 46 safeguards, access to processed personal data	Y
#16	Right to rectification.	Data correction	Y
#17	Right to erasure ('right to be forgotten').	Erasure of personal data, consent withdrawal	N
#18	Right to the restriction of processing.	Restriction to use personal data	Y
#19	Notification obligation regarding rectification or erasure of personal data or restriction of processing.	Notification of restrictions or erasure	Y
#20	Right to data portability.	Data portability	N
#21	Right to object.	Objecting processing, the lawfulness of processing, direct marketing purposes	Y
#22	Automated individual decision-making, including profiling.	Automated decision-making, profiling, human intervention	Y
#23	Restrictions on the scope of obligations by legislative measure.	Restriction, member state legislative measures	Y

Table 3. Rights of Data Subject.

4.3.4. Chapter IV: “Controller and Processor”

This section assesses Chapter IV articles applicability on the scenarios under the view of this thesis. The Chapter IV defines the responsibilities of the data controller and data processor and defines the relationship between them. Since the controller is responsible for GDPR compliance when processing personal data (also responsible to be able to demonstrate that compliance), it

must take measures to ensure the compliance. Some of these measures can be data minimization, pseudonymization and data protection impact assessment.

Chapter IV of GDPR introduced responsibilities for processors, this means that data controller is not the only one who is liable for data protection, which is explicitly state in Article 28: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." (Council of the European Union, 2016). Another interesting part in Article 28 is paragraph 4, where it states that if processors engage another processor for carrying out activities on behalf of the controller, the initial processor will be fully liable to the controller for the performance of that processor obligation (Council of the European Union, 2016).

Article 30 states the requirement to maintain the records of all processing steps. This is means that each time personal data is being modified, added or removed, the steps and the initializer of these steps must be recorded. This should be viewed as possible means to discover data breaches and secure and maintain proper roles for data management.

An additional concept that this chapter introduces is the assignment of data protection officer, the position role and tasks that DPO is expected to fulfill, such as advising the controller or processor, monitoring compliance, provide advice of data protection impact assessment and cooperation with superior authority.

Both articles 35 and 36 are applicable to Töötukassa, because the assessment of the envisaged processing operations on the protection of personal data is required every time where there is a change in processes, technologies or in development of new services. Article 36 is applicable because prior consultation is required if data protection assessment mentioned in article 35 finds the possibility of high risk in personal data processing activities.

Article	**Summary**	**Keywords**	**Applicability (Y/N)**
#24	The responsibility of the controller.	Compliance to regulation, certification	Y

		mechanisms to prove compliance	
#25	Data protection by design and by default.	Data-protection principles, data minimization	Y
#26	Joint controllers.	Joint controllers	N
#27	Representatives of controllers or processors not established in the Union.	Controller or processor outside of Union, representative	N
#28	Responsibilities and regulations on processor.	Processing behalf of a controller, guarantees, controller authorization, informing the controller of changes on other processors, legal act, documented instructions from controller, confidentiality	N
#29	Processing under the authority of the controller or processor.	Process only what is instructed	N
#30	Records of processing activities.	Record of processing activities	Y
#31	Cooperation with the supervisory authority.	Cooperation on request	Y
#32	Security of processing.	Security appropriate to the risk, pseudonymization, encryption, confidentiality	Y
#33	Notification of a personal data breach to the supervisory authority.	The data breach, breaches documentation, notification deadline 72h max, recommendations	Y

#34	Communication of a personal data breach to the data subject.	Communication of breach to the data subject, recommendations	Y
#35	Data protection impact assessment.	Impact assessment, cooperation with DPO, public list of processing required to be assessed	Y
#36	Prior consultation.	Consultation prior to processing, authorization for processing in the public interest	Y
#37	Designation of the data protection officer.	Assigning DPO, monitoring processing operations	Y
#38	The position of the data protection officer.	DPO involvement, supporting DPO, fulfilling other tasks, conflict of interest	Y
#39	Tasks of the data protection officer.	Advisement, monitoring, cooperation with supervisory authority, acting contact point	Y
#40	Codes of conduct.	Best practices, safeguards, approval of the draft code	N
#41	Monitoring of approved codes of conduct.	Monitoring compliance with the code of contact, accreditation	N
#42	Certification.	Data protection certification	N/A

		Mechanisms, demonstrating compliance, voluntary certificating	
#43	Certification bodies.	Issuing and renewal of certificates, conditions to be eligible for certification	N

Table 4. Controller and Processor.

4.3.5. Chapter V: "Transfer of personal data to third countries or international organisations"

As companies and different organizations are working on more global scale, cooperating between multiple countries and continents has become common. This means that also data is being exchanged between international companies. Chapter V is focused exactly on the management of personal data transfers to third countries and international companies. As the processes that are being evaluated in this thesis do not have activities that involve transferring personal data to third countries or international organizations, most of the articles do not apply. There are overall seven articles, where first two (44 and 45) are focused on the definition of transfers to the third party, as such the applicability for them is assessed as N/A.

Article	Summary	Keywords	Applicability (Y/N)
#44	The general principle for transfers.	Transfer of personal data, international organizations, third country	N/A
#45	Transfers on the basis of an adequacy decision.	Commission decision, monitoring of protection level, grounds of urgency	Y
#46	Transfers subject to appropriate safeguards.	Transfers without decision pursuant,	Y

		safeguards for transfers	
#47	Binding corporate rules.	Approving binding corporate rules, specified content in corporate rules	N/A
#48	Transfers or disclosures not authorized by Union law.	International agreement	Y
#49	Derogations for specific situations.	Data subject consent, necessary for the contract with data subject, legal claims, public interest	Y
#50	International cooperation for the protection of personal data.	International cooperation mechanisms	N/A

Table 5. Transfer of personal data to third countries or international organizations.

4.3.6. Chapter VI: "Independent supervisory authorities"

Table 6 covers the Chapter VI of the GDPR, which describes the nature, general rules and responsibilities of supervisory authority. As such the articles in Chapter VI are not applicable to Töötukassa.

Article	Summary	Keywords	Applicability (Y/N)
#51	Supervisory authority.	Assigned public authority	N/A
#52	Independence.	Independence for the authorities, free from external influence, financial control	N/A
#53	General conditions for the members of the supervisory authority.	General conditions	N/A
#54	Rules on the establishment of the supervisory authority.	Member State obligations,	N/A

		supervisory authority confidentiality	
#55	Competence.	Competency of authority	N/A
#56	Competence of the lead supervisory authority.	Competency of authority, handling of cases	N/A
#57	Tasks.	Tasks of supervisory authority	N/A
#58	Powers.	Investigative and corrective powers, authorization and advisory powers	N/A
#59	Activity reports.	Annual reports, available publicly	N/A

Table 6. Independent supervisory authorities.

4.3.7. Chapter VII: "Cooperation and consistency"

This section reviews the applicability of Chapter VII to this case study business processes, which are represented in Table 7. Similarly, to the previous section, the chapter describes the rules of cooperation and consistency between supervisory authorities and defines the role and responsibilities of the European Data Protection Board. As such the articles represented in Table 7 are not applicable to Töötukassa.

The Chapter of the GDPR introduces cooperation mechanism to cover cases where controllers and processors with activities in multiple EU countries are primarily subject to the authority of one lead supervisory authority, supervising all cross-border processing activities of this data controller or processor. In the example of Nortal Group, the lead authority is the Estonian Data Protection Authority (AKI).

Article	**Summary**	**Keywords**	**Applicability (Y/N)**
#60	Cooperation between the lead supervisory authority and other supervisory authorities concerned.	Exchange of information, mutual assistance,	N/A

		cooperation between authorities	
#61	Mutual assistance.	Cooperation between authorities	N/A
#62	Joint operations of supervisory authorities.	Joint operations	N/A
#63	Consistency mechanism.	Cooperation for consistency	N/A
#64	The opinion of the Board.	Authority to communicate the draft, Board opinion	N/A
#65	Dispute resolution by the Board.	Binding decisions for disputes	N/A
#66	Urgency procedure.	Urgent opinion or decision from the Board	N/A
#67	Exchange of information.	Exchange of information with authorities and the Board	N/A
#68	European Data Protection Board.	Board members	N/A
#69	Independence principality for the Board.	Board independence	N/A
#70	Tasks and activities performed by the Board.	Tasks of the Board	N/A
#71	Reports of activities created by the Board.	Annual reports	N/A
#72	Board decision-making procedures.	Procedure	N/A
#73	The Board chair and deputy chairs.	Chair	N/A
#74	Tasks and responsibilities of the Chair.	Tasks of the Chair	N/A
#75	The Board Secretariat and its responsibilities.	Secretariat	N/A

#76	Confidentiality principle.	Confidentiality	N/A

Table 7. Cooperation and consistency.

4.3.8. Chapter VIII: "Remedies, liability and penalties"

Chapter VIII defines the rights for effective judicial remedy (against controllers, processors and supervisory authority), proceedings handling, liabilities and penalties for failure to comply with the GDPR. As such most of the articles are applicable to Töötukassa or the processing of personal data done in the use cases covered in this thesis.

Aside from overall proceedings handling definitions and regulation, there is one notable aspect of Article 82 is paragraph 4, which states: „Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject" (Council of the European Union, 2016). This means that controllers should be motivated to make sure that not only themselves but also processors or joint controllers are processing personal data with compliance to GDPR and sufficient safeguards or they will be liable for non-compliance of others as well.

One of the most interesting (and spoken of) articles in this chapter is Article 83, which defines the administrative fines which vary in size, dependent on given non-compliance categories. The fact that non-compliance in some categories, for example, data subjects' rights, are fined up to 20 000 000 or up to 4% of the total worldwide annual turnover, is making companies and organizations so invested into GDPR and its compliance (Council of the European Union, 2016).

Article	**Summary**	**Keywords**	**Applicability (Y/N)**
#77	Right to lodge a complaint with a supervisory authority.	Lodging a complaint	N
#78	Right to an effective judicial remedy against a supervisory authority.	The right to an effective judicial remedy	Y

#79	Right to an effective judicial remedy against a controller or processor.	Proceedings against a controller or a processor	Y
#80	Representation of data subjects.	Mandating by the data subject	N/A
#81	Suspension of proceedings.	Proceedings concerning the same subject matter	N/A
#82	Right to compensation and liability.	Controller liability for damage	Y
#83	General conditions for imposing administrative fines.	Fine sizes, grounds for fines	Y
#84	Member States other penalties.	Penalties	Y

Table 8. Remedies, liability and penalties.

4.3.9. Chapter IX: "Provisions relating to specific processing situations"

This section covers the Chapter IX of the GDPR in Table 9, where only one article is directly applicable to this case study – Article 87. This article is applicable to Töötukassa only in the case where a Member State of the EU (in this case Estonia) decides to adopt specific condition for processing of the national identification number. The other articles are not applicable to the scope of this case study.

Article	**Summary**	**Keywords**	**Applicability (Y/N)**
#85	Processing and freedom of expression and information.	Journalism, freedom of speech, protection of personal data	N
#86	Processing and public access to official documents.	The public authority, public interest, right to the protection of personal data	N
#87	Processing of the national identification number.	National identification	Y

		number processing	
#88	Processing in the context of employment.	Employment relationship	N
#89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.	Scientific or historical research purposes, archiving purpose, statistical purpose	N
#90	Obligations of secrecy.	Extra obligations of secrecy	N
#91	Existing data protection rules of churches and religious associations.	Existing rules	N/A

Table 9. Provisions relating to specific processing situations.

4.3.10. Chapter X: "Delegated acts and implementing acts"

The Articles 92 and 93 in Chapter X, represented in table 10, are not applicable to this case study, because they define the Committee procedure and exercise of the delegation.

Article	Summary	Keywords	Applicability (Y/N)
#92	The exercise of the delegation.	Adopting delegated acts, a delegation of power, revoke of delegation	N/A
#93	Committee procedure.	The assistance of the Committee	N/A

Table 10. Delegated acts and implementing acts.

4.3.11. Chapter XI: "Final provisions"

Table 11 covers the overview of Chapter XI of the GDPR, although the articles are not directly applicable to use cases in this thesis. Chapter XI does not introduce any concrete new regulation or rules but states relationship and applicability of previous directives and also stating when the GDPR will take in force.

Article	Summary	Keywords	Applicability (Y/N)
#94	Repeal of Directive 95/46/EC.	Directive 95/46/EC repeal	N/A
#95	Relationship with Directive 2002/58/EC.	Additional processing	N/A
#96	Relationship with previously concluded Agreements.	Pre-GDPR international data transfer agreements	N/A
#97	Commission reports.	Regulation evaluation, proposals to amend the Regulation	N/A
#98	Review of other Union legal acts on data protection.	Other legal acts on personal data	N/A
#99	Entry into force and application.	Applying time	N/A

Table 11. Final provisions.

4.4. Summary

In section 4.1 of this chapter, I briefly introduced the overall context of the business processes in which are the subject of compliance analysis in this thesis. In section 4.2 I introduced data-centric business process models of working ability allowance and working ability assessment processes, along with the sub-processes belonging to the main processes. In section 4.3 I reviewed the applicability of each article in the GDPR to the processes introduced in section 4.2. The section was split between each chapter of the GDPR and the results of the applicability and keyword analysis were captured in the corresponding tables of that chapter, which helps with narrowing down to the relevant articles for compliance analysis done in next chapter.

5. COMPLIANCE EVALUATION

In this chapter, I will review all articles that are applicable to Töötukassa, based on keyword analysis done in previous chapter section 4.3. For each article, the degree of compliance is assessed using the results of keyword analysis, represented in the column "Degree of compliance", where possible values are: non-compliant, partial and full compliance. The article compliance is assessed based on activities in the models introduced with the initial business process modeling in section 4.2. In cases where current business processes are partially compliant or non-compliant, explanation of the reason is described.

5.1. Compliance with Chapter II: "Principles"

In this section is the compliance assessment of five articles that were applicable to processes under view in this thesis, presented in table 12. There were minor compliance issues – only three articles had partial compliance, which needs small improvements to fully comply with GDPR.

There are multiple issues with the compliance of article 5 – there are possible ways to minimize the amount of data stored by Töötukassa by reducing the logging. Currently, it is not possible for data subject to a request for data deletion. This needs to be addressed by Töötukassa, as GDPR places a requirement to provide a response to this request within one month, by offering case-by-case review for such requests for possible data erasure. Töötukassa could, of course, deny the erasure request if proportional reasons are provided.

Article 7 is partially compliant because currently the consent is being requested from the data subject, but the consent does provide all the information required by the GDPR. Consent information should consist a list of all activities personal data is processed and, if applicable, provide the list of third-party organizations (and their contact information) where additional queries for personal data is being made.

For article 8 the current system does require a parental agreement for children under age of 16 to apply for working ability assessment. As per current processes, there are no possible ways for a person to withdraw the consent, it becomes especially a problem for children giving the consent (ages on 16 to 18). As per Estonian Child Protection Act, a child is considered to be a person under age of 18 and per GDPR if the child has given consent, he or she should be able

to withdraw the consent whenever he or she feels necessary. This is because a child might not be aware of all the risks and possible dangers when giving the consent for personal data processing.

Article	Degree of compliance	Activity in model	Explanation of non-compliance
#5	Partial	All activities	Currently, there are no mechanisms to delete the existing personal data, even if it is not necessary for further processing. Additionally, it is possible to improve the data minimization of current data processing processes.
#6	Full	All activities	N/A
#7	Partial	A2, A3, A4	Currently, it is not possible for a person to withdraw consent.
#8	Partial	A2, A3, A4	Currently, it is not possible for a person to withdraw consent.
#9	Full	All activities	N/A
#10	Full	IA14	N/A
#11	Full	All activities	N/A

Table 12. Compliance with articles in Chapter II.

5.2. Compliance with Chapter III: "Rights of Data Subject"

This section covers the articles analyzed in section 4.4.3 of this thesis, which is captured in Table 13. Compared to the previous chapter, there are more issues with compliance, where for article 15 the current processes are non-compliant. Some articles are fully compliant due to either process under view currently do not have data deletion in place or there are separate processes in place which are not captured in the processes viewed in this thesis.

Article 19 required the notification of the data subject whenever their personal data has been fixed or deleted. Töötukassa currently has no process in place for the deletion of personal data and they do not modify the personal data of data subject themselves, the notification is not being done. As for Article 21, Töötukassa already has a process in place for data subject objection

rights, where applications are reevaluated as well as the calculation and eligibility of working ability allowance is done before each payment.

Töötukassa does automated individual decision-making and profiling of data subjects, which is authorized by Estonian law, as such Töötukassa is required, by Article 22, paragraph 3, to have suitable measures in place to safeguard the data subject rights. In my opinion, these safeguards are in place, demonstrated by the multiple validations and the data subject ability to object the decision made by Töötukassa.

Article	**Degree of compliance**	**Activity in model**	**Explanation of non-compliance**
#12	Full	All activities	N/A
#13	Partial	A2, A3, A4	Some of the information, that is required by new Regulation, is currently not explained and need to be added to the information documents and/or forms.
#14	Partial	IA3 – IA15	Some of the information, that is required by new Regulation, is currently not explained and need to be added to the information documents and/or forms.
#15	Non-compliance	All activities	Currently, there is no specific process or mechanism to gather the data or data sources being processed.
#16	Full	All activities	N/A
#18	Full	All activities	N/A
#19	Full	-	N/A
#21	Full	WAA22	N/A
#22	Full	IA3 – IA15, WAA9, WAA11, WAA22, WAA23	N/A
#23	Full	All activities	N/A

Table 13. Compliance with articles in Chapter III.

5.3. Compliance with Chapter IV: "Controller and Processor"

Chapter IV describes different roles and obligations of Controllers and Processors, as well as introducing the data process officer role and tasks. As such, most of the articles are either not directly applicable to Töötukassa or describe more overall organization procedures. The assessment of compliance is provided in Table 14, where we can see that overall compliance is very high – there is only one article with partial compliance and no non-compliant articles.

Article 24 and 25 are more general and define the responsibilities of the controller and data protection design. As Töötukassa is already in process of taking measures to meet the compliance requirements, I assess that these two articles are fully compliant.

As notification of data breach to superior authority and communication of breach to data subject is not particular to the processes that are under the view of this thesis, it is not possible to assess the compliance of articles covering these cases (Article 33 and 34). The process of notifying and communicating of a data breach is an organization-wide process which should be covered for all business processes (and thus all data processing activities). Additionally, during the writing of this thesis, Töötukassa has hired a data protection officer and adopted its responsibilities and tasks which were introduced with Articles 38 and 39, thus it is also now compliant with Article 37.

Article	Degree of compliance	Activity in model	Explanation of non-compliance
#24	Full	All activities	N/A
#25	Full	All activities	N/A
#30	Full	All activities	N/A
#31	Full	-	N/A
#32	Partial	All activities	Currently, all activities are logged into system logs and database logs without the pseudonymization and encryption of personal data.
#33	N/A	-	N/A
#34	N/A	-	N/A

#35	Full	All activities	N/A
#36	Full	-	N/A
#37	Full	-	N/A
#38	Full	-	N/A
#39	Full	All activities	N/A

Table 14. Compliance with articles in Chapter IV.

5.4. Compliance with Chapter V: "Transfer of personal data to third countries or international organizations"

Although Töötukassa does support foreign nationalities as well, for example, Latvians without national ID, it does not send their personal data to third countries or international organizations. With Article 45, Töötukassa does use international organization services for data processing (Amazon Web Services), but since Amazon is certified with Privacy Shield, the compliance degree of this article is full (Amazon, 2018).

Töötukassa does request personal data from third countries, in a case where the data subject is from such country and consent given. As there is no other activity which is to do with sending data to the third country or international company, the business processes in this case study have complete compliance with Chapter V (see Table 15).

Article	**Degree of compliance**	**Activity in model**	**Explanation of non-compliance**
#45	Full	-	N/A
#46	Full	-	N/A
#48	Full	-	N/A
#49	Full	-	N/A

Table 15. Compliance with articles in Chapter V.

5.5. Compliance with Chapter VIII: “Remedies, liability and penalties”

The liabilities and penalties which are introduced in Chapter VIII do apply to Töötukassa, but there is nothing on Töötukassa to not comply upon, as such applicable articles from that chapter are marked as fully compliant (see Table 16).

Article	Degree of compliance	Activity in model	Explanation of non-compliance
#78	Full	-	N/A
#79	Full	All activities	N/A
#82	Full	All activities	N/A
#83	Full	-	N/A
#84	Full	-	N/A

Table 16. Compliance with articles in Chapter VIII.

5.6. Compliance with Chapter IX: “Provisions relating to specific processing situations”

There is only one article of Chapter IX (represented in table 17) to be assessed for compliance, which is Article 87. Since Estonia has currently not stated of any extra regulation on the processing of the national identification number, which is already implemented by Töötukassa, the degree of compliance for that article is assessed as full.

Article	Degree of compliance	Activity in model	Explanation of non-compliance
#87	Full	All activities	N/A

Table 17. Compliance with articles in Chapter IX.

5.7. Summary

In chapter 5 I have reviewed the degree of compliance with the relevant articles that were identified as applicable to a current case study in section 4. Surprisingly, the overall compliance level of case study business processes is high, while there are some minor non-compliance issues and one fully non-compliance with Article 15. This means that Töötukassa has been serious about implementing safeguards to ensure their client's data is protected and processed lawfully, while there is some place for improvement. Additionally, Töötukassa has already hired, during the writing of this thesis, a data protection officer, covering the compliance of articles 37 – 39.

The results of compliance evaluation analysis done in this chapter will be used in next chapter to recommend changes in current business processes or to introduce new processes to comply with the upcoming GDPR.

6. PROPOSED SOLUTIONS FOR COMPLIANCE

In this chapter, I review all articles that were partially or fully non-compliant, based on analysis done in previous chapter 5, and propose solutions for solving these non-compliance issues, answering sub-research question two (SRQ2). The proposed solutions will be documented in table 17, with additional TO-BE models for relevant articles. Derived from the proposed solutions, section 6.2 will introduce requirements for system architecture to support the proposed changes.

6.1. Proposed solutions

Table 17 represents the proposed solutions which would, when implemented, make Töötukassa working ability allowance and working ability assessment business processes compliant with the identified non-compliance issues. The solutions themselves are offered in "Proposed solution" column, while some of the solutions have derived system requirements added in the column "Requirement ID" and some have introduced or changed activities and models linked to the solution.

With the Article 13 and Article 14 the existing consent documentation needs to be extended, to include the new rights that were introduced to the data subjects: the period of which the data is stored or how that period is determined; right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; right to withdraw consent; right to lodge complaint; etc. (Council of the European Union, 2016). Additionally, contact information about Töötukassa data protection officer, existence of automated decision-making, from which source the personal data originate and notification to data subject about recipients of personal data (all these within reasonable time, the latest one month), for example when expertise doctor is chosen (Council of the European Union, 2016).

As for article 15, the data subject has the right to access their data that is being stored and processed in the system, as such the controller shall provide the copy of that data. Additionally, person has the right of access to information about when and from where the information was collected and used for processing. All that information is currently stored and logged, but not explicitly shown to the data subject in the user interface (see requirement R1 and Appendix 1, Figure 8).

Article	Proposed solution	Introduced activity or model	Requirement ID
#5	1) Introduce the possibility of (partial) data subject personal data deletion. This is a requirement for cases where the data is not required for any further processing for what purpose the data was collected and data subject consent was given or cases where data subject request erasure of data. 2) Introduce data scanning to have a clear overview of where and what data is being stored in current databases.	-	R1, R2, R6
#7, #8	Introduce the possibility of data subject to request withdrawal of consent. The request could be submitted online and in person (possibly also with mail, if sufficient proof is added about the identity of the requester).	Refer to TO-BE model in Appendix 1, Figure 7	R3
#13	Information about personal data gathering, processing, and data subject rights should be modified to include information required as mentioned in Article 13, paragraph 1 and 2, in documentation and forms introduced to data subject when giving consent.	A2, A3, A4	
#14	Information about personal data gathering, processing, and data subject rights should be modified to include information required as mentioned in Article 14, paragraph 1 and 2, in documentation and forms introduced to data subject when giving consent.	IA3 – IA15	
#15	Introduce the sub-process where the user can ask information about if their personal data is being processed and get access to that process. Additionally, provide information stated in Article 15 paragraph1, sections a – h.	Refer to TO-BE model in Appendix 1, Figure 8	R1
#32	1) Use encryption for system and database logging when logging information about data subject's personal data. 2) Disable the logging of X-Road requests in TETRIS application and only use the logging of X-Road Security server.	-	R4, R5

Table 17. Compliance with articles in Chapter IX.

6.1.1. Consent withdrawal

The new TO-BE process introduced for the purpose of supporting the consent withdrawal, required for compliance with article 7 and 8, is captured in Appendix 1, Figure 7. The process can be started by electronically or in the Töötukassa office.

In order to withdraw the consent, the requester will have to identify him- or herself, for Töötukassa to make sure of the identity of the requester. Once the requester is authenticated, the consent can be withdrawn. For electronic methods, it is recommended to introduce possible means to avoid accidental withdrawal of consent.

When consent is removed, the system will stop all ongoing processing of personal data for processing is performed based on that consent. Once the processing has been stopped, the requester will be notified of the successful withdrawal of consent and stopping of all processing based on the consent. Additionally, if any personal data was shared to third-parties during these processes, notification of consent withdrawal will be sent to these parties as well.

6.1.2. Right of Access

The Right of Access model, represented in Appendix 1, Figure 8, introduces the possibility for the user to access his or her personal data that is stored in the system. Similarly to the consent withdrawal, the request can be submitted electronically and on-site after proper identification. Once the request is submitted, the system will generate the report of existing personal data in the system. In case of electronic request from the requester, the data will also be shared in machine-readable form. The report will include all personal data of the requester in the system, the procedures where that data is processed, recipients and contact info in case the data was shared.

6.2. GDPR impact on system architecture

In section 2 of this chapter, I will review the changes that need to be implemented in current info system (TETRIS) to support changes suggested in the previous section. The changes needed are provided in requirements templates with some explanation of the reasoning of the needed change. For each requirement, I assess the impact on the current system architecture and the reason the need for the requirement. The impact is assessed with three levels – high, medium and low, which are also included in the requirements template for each requirement. These requirements are not finalized, which means that further (business and system) analysis

needs to be done along with Töötukassa, to find the most suitable way to implement the recommended changes. The proposed changes are validated in chapter 7 with the Nortal system architect to understand the feasibility and scope of functionalities needed for the changes.

6.2.1. R1: Gather all data subject data in readable form

Requirement one is derived from the need to support the possible requests from the data subject and from authorized recipients, for example, social worker, to gather all his or her personal data stored in the system with the sources (and retrieval time) of the data being collected from. As there already is an existing storing of such information, it does not have a high impact on current system architecture and most changes are related to providing an endpoint for the front end and displaying that to the end user.

Requirement ID:	R1
Requirement Type:	Functional
Dependencies:	None
Description:	Add functionality to gather all data subject's personal data stored in the system and give it as output in readable form.
Rationale:	With the GDPR the data subject has the right to request all of his personal stored in the system in readable form. Currently, there is no such functionality implemented in the system, as such this is needed for reducing the manual workload for handling such requests.
Acceptance criteria:	The data subject can retrieve his or her personal data in the info system.
System Architecture Impact:	Low
Priority:	Critical

6.2.2. R2: (Partial) Erasure of data subject personal data

Personal data that is not used for the purposes of which it was gathered and is not needed for further audits (or for statistics for Statistikaamet) should be deleted from the system. There are already functions in place that support the deletion of the personal data, but there is no analysis of which set of data could be deleted, while also supporting the possibility of future audits or requests for statistical purposes. Additionally, it is not fully clear what are all the fields in the database where personal data is stored, as there are "free text" forms available in the system, which is not validated. As such, the impact to system architecture is assessed as high, displayed in the requirement template below. This requirement needs further business analysis to have direct guidelines on which set of data can be deleted from the system and what are the valid use cases to do so.

It should be noted that Töötukassa can deny the request for personal data erasure, so this should be reviewed case by case. Additionally, once the request is submitted, Töötukassa will need to notify of the request to the third-party recipients (if any) of that data subject personal data.

Requirement ID:	R2
Requirement Type:	Functional
Dependencies:	R1
Description:	Add functionalities to erase (partially) data subject's personal data.
Rationale:	With the upcoming GDPR data subject has the right to ask for erasure of his or her personal data. Along with the right to be forgotten principle, the controller should delete the personal data in the case where it is no longer needed for processing for which the data was initially collected. Additionally, it should allow partial deletion of the data, as there might need to have some data available (name, ID, contact information) for auditing and in case of fraud.
Acceptance criteria:	The info system has the possibility to delete the personal data.
System Architecture Impact:	High

Priority:	Critical

6.2.3. R3: Consent withdrawal

Per GDPR, the data subject has the right to withdraw their consent. Since it is not feasible to manage all these requests manually, it would be beneficial to implement a way to support this action automatically (see Appendix 1, Figure 7). Since the processing of personal data relating to health is currently based on data subject consent, the application needs to be denied and all further processing should be stopped. This denial is already supported in cases where the application is denied based on the evaluation. Due to the fact that there are already possible mechanisms to stop any further processing or use of personal data once the application is withdrawn or denied, these mechanisms should re-usable for the consent withdrawal. This means that the impact on system architecture should be medium.

Requirement ID:	R3
Requirement Type:	Functional
Dependencies:	None
Description:	Add functionality for data subject to withdraw consent.
Rationale:	The data subject has the right to withdraw the consent, that previously was given. This means that after that all further processing that was being done based on the consent will be stopped.
Acceptance criteria:	The data subject can withdraw consent.
System Architecture Impact:	Medium
Priority:	Normal

6.2.4. R4: Encryption of logging personal data

The initial idea was to use pseudonymization as a way to make the logging of personal data not directly linkable to the data subject. After validating the proposed solution with the system architect, it turned out that it is more feasible to support the encryption of the personal data logging, while still making it harder to link the logging to the data subject.

At the time of writing this thesis, all requests and activities are logged to database and system logs, without using pseudonymization or encryption. This means that anyone with access to mentioned logs can access the sensitive and personal data that is being used while processing data subject personal data. Additionally, such unencrypted data is a possible threat to a data breach, which needs to be fixed as soon as possible. After discussions with the system architect, the best option for removing the mentioned threat is to introduce personal data encryption, when logging activities and requests done in the system. This is still considered to be high impact on current system architecture because currently no such encryption method is being used. This means that new technology for encryption must be introduced, with additional decrypting functionality, where necessary.

Requirement ID:	R4
Requirement Type	Functional
Dependencies	None
Description:	Add encryption for data subject personal data when adding system or database logging.
Rationale:	Proper safeguards should be implemented to secure personal data being processed and logged.
Acceptance criteria:	The logging consisting personal data should have that information encrypted.
System Architecture Impact:	High

Priority:	Low

6.2.5. R5: X-Road response logging

Currently, the TETRIS info system logs all requests and responses from the X-Road into log files. Since the responses of the X-Road consist of personal data directly linkable to the data subject, the logging should remain only for service debugging purposes, meaning that in normal situations the application level logging of X-Road responses should be turned off. The X-Road Security server, managed currently by Telia, logs the X-Road traffic already, which means the logs can be accessed by that system, if necessary. Turning this logging off will additionally improve the safeguard of the current system on the data minimalization principle (Article 5). As the amount of work this change requires is extremely low, as the only change would be with the existing configuration, changing the logging level of the X-Road component, the impact for system architecture is low as well.

Requirement ID:	R5
Requirement Type	Functional
Dependencies	None
Description:	Disable X-Road response logging in application level.
Rationale:	X-Road response consists of personal data that should not be logged in application level, especially since it is already captured with the Security server. The access to the logs should only be needed in case of support or auditing cases.
Acceptance criteria:	The application logging does not include X-Road responses.
System Architecture Impact:	Low

Priority:	Normal

6.2.6. R6: Introduce data scanning

It is currently possible for person using the systems user interface to enter comments and additional details to textboxes or data fields, which are currently not validated. These text boxes or data fields can contain sensitive personal date, like information or comments about data subject health, as Töötukassa has no control over what is added there. Töötukassa should have a clear view of their current data structure and data being stored to make sure that nonintentional personal data storing is not taking place in which case the Töötukassa would be responsible of. Such sort of data mapping and scanning should be recurring activity, which could be achieved by using already existing tools, for example DeepScan (Nortal, 2018).

Although the data scanning and monitoring tools themselves impact the system architecture at low level, the possible findings of data misplacement (or misuse of data fields) can provide insight to data protection and data minimization needs that are not discoverable without proper monitoring. As such these findings of data misuse or possible gaps can improve on making the current data structure more secure and transparent, reducing the risks that personal data processing might introduce.

Requirement ID:	R6
Requirement Type	Functional
Dependencies	None
Description:	Introduce data scanning and validation for detecting unintended saving of personal data.
Rationale:	Currently, there are multiple “free form” fields which are used to comment data subject application or health examinations by Töötukassa doctors and expert doctors. As such, there is no control what the fields will contain.

Acceptance criteria:	There is a clear overview of data stored in the info system.
System Architecture Impact:	Low
Priority:	Normal

6.3. Summary

Chapter 6 introduced recommendations for compliance issues that were found with the GDPR evaluation analysis in chapter 5, answering sub-research question two (SRQ2). Although the overall compliance of business processes in the scope of this case study was quite high, there is still room for improvement. In addition to minor compliance issues, there were few noncompliance issues which require immediate attention – for example, unencrypted logging of personal data, no support for consent withdrawal or functionality to comply with the right of access principle.

7. VALIDATION

In order to understand the feasibility of the compliance analysis and the proposed solutions the thesis draft was sent to Töötukassa, Nortal Project Manager, System Architect, DPO, data specialist and lawyer.

7.1. Nortal feedback

The Nortal lawyer provided feedback to double check applicability of Article 8 (child's consent) and Article 9 (special categories of personal data) on Töötukassa processes. Additionally, he recommended making myself acquainted with the Child Protection Act and Directive 2015/1535 and ensure alignment between them. Derived by the recommendation, I reviewed the Estonian Child Protection Act, Directive 2015/1535, Work Ability Allowance Act and double-checked the applicability of the articles on Töötukassa business process, after which I added more discussion on the subject and fixed the mistakes I had regarding the applicability of Article 8 to the Töötukassa.

Additionally, the feedback I got from the lawyer was that I have incorrectly assessed the applicability of the Article 36 (prior consultation). As per Article 36, prior consultation is required in case a risk is discovered during the data protection impact assessment (Article 35).

Proposed solutions for the compliance were reviewed by TETRIS Nortal System Architect (SA), who assessed the feasibility of the proposed changes and double-checked my assessment on the system architecture impact. Prior to the final review, there were also multiple meetings with the SA to understand the current system procedures and checks (for example that in case of missing or incorrect data fix request to the data subject no personal data is being forwarded with the request mail). The biggest change I had to make was the correction of the recommendation regarding pseudonymization, which recommended the use of pseudonymization for the current system logging and personal data. After discussion with the SA, it became clear that the amount of work is way more than would be proportional to the purpose this recommendation was placed and would make the support case analysis harder. The encryption of personal data in logging was the far more feasible solution. Additionally, the SA provided knowledge of current personal data access recording (only people with sufficient rights per their work responsibilities have access to data subject's personal data and each such access request is being logged in system), necessity of longer period storage of the personal

data due to possible fraud cases, where data subject can get allowance based on wrong data presented.

Finally, the Project Manager from Nortal has shared his opinion of the subject and current thesis: ”With the GDPR going into effect, new and sometimes troublesome challenges present themselves. For instance, the principle of data minimization is orthogonal to how technical support is usually carried out, i.e., using as much data about an individual as possible to find the root cause and notice patterns that would remain hidden with fewer data to analyze. Part of the problem is where to start with anything, and this is where this work really shines. Through the information presented in this thesis, it is possible to gain a significantly better understanding of which chapters of the GDPR are applicable to the two business processes under scrutiny, and which cases need to be resolved with policy, rather than technological measures. For chapters of the GDPR that are not applicable due to circumstances specific to our client, a clear explanation is provided that functions as a safeguard against malicious or uninformed third parties. Furthermore, the analysis of the applicability of certain GDPR articles can be extended to examine other processes outside the scope of this work. Continuing on that note, one of the greatest challenges is to find the most critical areas of the application that are lacking in GDPR compliance and update them within strict time constraints. Hence the most practical, and immediately applicable, the value can be found from the chapters "Compliance evaluation" and "Proposed solutions for compliance" that can be used as a basis for discussion with the client and the Data Protection Officers from both sides, and for the subsequent design and implementation of the required features. All in all, one can be glad to discover that, more or less, the application has been GDPR compliant all along. On the other hand, the work still revealed certain deficiencies to be remedied, such as enhancing the system's logging abilities or implementing encryption/obfuscation in certain places that once again highlight the value of the analysis presented.”

7.2. Töötukassa feedback

The feedback of Töötukassa was provided in Estonian, which can be seen in Appendix 3. I will cover the major parts in this validation part.

Overall Töötukassa explains that the created business models are well presented and provides value for future activities. Besides the BPMN models, Töötukassa expressed their appreciation towards my in-depth explanation of each article and its relevance to their processes of working

ability assessment and working ability allowance processes. There were some non-compliance issues brought out, which Töötukassa is already working on or have fixed already, for example, notifications to data subjects and assignment of DPO.

There are some parts that Töötukassa feels that is incorrect: some processes which are marked as partially or fully non-compliant are actually existent outside of these specific processes or info system – for example fulfilling the right of access requests from the data subject. This is sadly one of the setbacks of conducting the GDPR analysis on few cases, instead all of the organization processes together. Additionally, Töötukassa suggested to include the regulations on which the personal processing is being done in the Töötukassa processes introduction chapter. This suggestion was implemented as requested.

One important remark that Töötukassa made with its feedback regarding collecting consent from the data subject: "Currently consent is only taken for a request for personal health data, but according to Article 9 paragraph 2h the processing of sensitive personal data for working ability assessment is possible without data subject consent". As Article 9 paragraph 1 states that sensitive personal data processing is prohibited and paragraph 2 states: "Paragraph 1 shall not apply if one of the following applies:" with section h stating: "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;", I see that there is nothing stating that the consent is not required. As such, this statement requires additional analysis.

In regard to the erasure of personal data they see the contradiction – at the beginning, I have pointed out that it is not possible to delete the personal data from the registry but after I recommend the partial erasure of personal data. They refer to Statute of the Unemployment Insurance Database and the inability to delete the data which was gathered for the decision and according to that statue. This contradiction should be double checked in further studies.

In conclusion, Töötukassa finds that the thesis is thorough and finely conducted. Problematic compliance issues are highlighted and possible actions are given

CONCLUSION

The aim of this thesis was to analyze the impact from new European General Data Protection Regulation (GDPR), which sets new requirements for personal data management, on a real-life case study. The analysis was conducted using case study methodology on two business processes of Töötukassa: working ability assessment and working ability allowance. The existing processes were mapped using BPMN, use of sensitive data was highlighted and then the GDPR compliance was evaluated. From the results of the evaluation, possible solutions were offered to fix the compliance issues. The solutions were offered as TO-BE models and system requirements with the assessment of the impact on the current system architecture.

The results found with the analysis were positive, where the two use cases in this study were compliant with most of the articles in the GDPR. There were some non-compliance issues as well – it was found that the current logging of personal data should be encrypted and some logging should be disabled completely, to support the compliance with the data minimization principle. Töötukassa also needed to support possible queries for data subject (like personal data access requests, consent withdrawal, and data erasure) and update their consent forms with necessary information.

It is possible to extend the scope of the current thesis by increasing the cases covered in the case study and looking at all the processes within the organizations. Each process should be analyzed carefully and the whole flow of activities should be considered (both the controller and processor side). Including all the processes within Töötukassa would give a much clearer overview on all the aspects concerning the data management compliance with GDPR, for example, processes handling the data breaches and cooperation between superior authority and the organization. Additionally, from the feedback received from Töötukassa, there are additional points to re-evaluate to improve the current analysis: the need for consent for requesting medical personal data for working ability assessment and the possibility of partial erasure of the personal data when it is not needed for the purpose it was initially gathered.

KOKKUVÕTE

Selle magistritöö eesmärgiks oli analüüsida uue Euroopa Liidu isikuandmete kaitse üldmäärusest (GDPR ehk General Data Protection Regulation), mis sätestab reeglid personaalsete andmete töötlemiseks, tulenevate nõuete mõju reaalelulises juhtumianalüüsis. Analüüs koostati kasutades juhtumianalüüsi metodoloogiat kahe Töötukassa äriprotsessil – töövõime hindamine ja töövõimetoetus. Olemasolevad protsessid kaardistati kasutades BPMN mudeleid, mille abil toodi välja sensitiivsete personaalsete andmete kasutamine ja vastavus GDPR-iga. Vastavuse analüüsi tulemustest moodustati soovitused, mida kasutada GDPR artiklitele mittevastavate probleemide lahendamiseks. Pakutavad soovitused on esitatud TO-BE mudelitena ning süsteemi nõuetena, millede puhul on hinnatud ka mõju olemasolevale süsteemi arhitektuurile.

Analüüsi tulemused olid positiivsed – kaks magistritöös uuritud protsessi olid peaaegu täielikult vastavuses GDPR-i nõuetega. Siiski leidus töö tulemusel mõned üksikud mittevastavused ja võimalikud edendamise kohad – personaalsed andmed süsteemilogides võiksid olla krüpteeritud ja osa süsteemsest logimisest saaks kinni keerata (mõistlikkuse piires). Neid soovitusi tasuks kaaluda andmete minimaliseerimise printsiibi juurutamisel ja olemasolevate protsesside hindamisel. Lisaks oli soovituseks toetada automatiseeritud kujul teabepäringuid – süsteemis töötlemiseks olevate isikuandmete päring, nõusoleku tagasivõtmine. Lisaks soovitasin kaaluda osalist andmete kustutamist andmete puhul, mida enam eesmärgipäraselt ei vajata ning mille arhiveerimisaeg on möödas.

Seda magistritööd saab laiendada suurendades juhtumianalüüsi all olevate protsesside arvu, kattes kõiki Töötukassa protsesse. Sellisel juhul tuleks vaadelda kõikide protsesside koosmõju ja tervikpilti kogu töövoona (nii vastutava töötleja kui ka volitatud töötleja vaates). Kõikide protsesside analüüs annab parema vaate andmete haldamisest ja selle vastavusest GDPR-iga – näiteks protsessid andmete lekkimisel, kasutajate teavitamise protsessid ja koostöö järelvalveasutusega. Lisaks saab parandada töö kitsaskohti analüüsides Töötukassa tagasisides välja toodud puudusi – nõusoleku andmise vajadus meditsiiniliste andmete pärimiseks, osaline isikuandmete kustutamine riiklikust registrist.

BIBLIOGRAPHY

About Töötukassa. (2013, October 20). Retrieved April 01, 2018, from Eesti Töötukassa: https://www.tootukassa.ee/eng/content/about-tootukassa

Alaküla, M.-L., & Matulevičius, R. (2015). An Experience Report of Improving Business Process Compliance Using Security Risk-Oriented Patterns. *The Practice of Enterprise Modeling* (pp. 271-285). Valencia: Springer.

Amazon. (2018). *EU-US Privacy Shield*. Retrieved April 29, 2018, from Amazon Web Services: https://aws.amazon.com/compliance/eu-us-privacy-shield-faq/

Ball, K. (2010). Data protection in the outsourced call centre:. *Human Resource Management Journal, 20*(3), 294–310.

Benbasat, I., Goldstein, D., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 369-386. Retrieved February 11, 2018, from http://www.jstor.org/stable/248684

Cornock, M. (2018). General Data Protection Regulation (GDPR) and implications for research. *Maturitas*, 1-2.

Council of the European Union. (2016, April 6). *General Data Protection Regulation.* Retrieved from European Council: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The Case Study Approach. *BMC Medical Research Methodology*.

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2013). *Fundamentals of Business Process Management.* Springer.

Eesti Töötukassa. (2016, April 22). *Principles and methodology*. Retrieved April 14, 2018, from Töötukassa Web site: https://www.tootukassa.ee/eng/content/work-ability-reforms/principles-and-methodology

Eesti Töötukassa. (2016, April 28). *Who has the right to receive a working ability allowance?* Retrieved April 14, 2018, from Töötukassa Web site: https://www.tootukassa.ee/eng/content/work-ability-reforms/who-has-right-receive-working-ability-allowance

Eesti Töötukassa. (2016, August 25). *Working ability assessment*. Retrieved March 04, 2018, from Eesti Töötukassa Web site: https://www.tootukassa.ee/eng/content/work-ability-reforms/working-ability-assessment

El-Bakry, H., & Mastorakis, N. (n.d.). Business Process Modeling Languages for Information System. 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS.

European Parliament and of the Council. (2015, September 9). Directive (EU) 2015/1535. Retrieved May 20, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_241_R_0001

Gerring, J. (2011, July). The Case Study: What it is and What it Does. (R. E. Goodin, Ed.) *The Oxford Handbook of Political Science*.

Hern, A. (2018, April 17). Far more than 87m Facebook users had data compromised, MPs told. Retrieved May 2, 2018, from https://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica

Kožíšek, F., & Vrana, I. (2017, September). Business Process Modelling Languages. *9*, 39-49.

Krivokapić, Đ., Krivokapić, D., Todorović, I., & Komazec, S. (2017). Mapping Personal Data Flow and Regulatory Compliance in Serbian Public Institutions. *Management: Journal Of Sustainable Business And Management Solutions In Emerging Economies, 21*(80), 1-10.

Linklaters. (2017). *The General Data Protection Regulation: A survival guide.* London: Hogan Lovells Publications.

Ltd., B. (2018, January 16). Case study: Becrypt discovered unexpected benefits in preparing for GDPR.

Nortal. (2018). *DeepScan*. Retrieved from Nortal homepage: https://nortal.com/deepscan/

OMG. (2011, January). *Business Process Model And Notation 2.0*. Retrieved February 12, 2018, from Object Management Group: http://www.omg.org/spec/BPMN/2.0/

Paiano, R., Caione, A., Guido, A., Martella, A., & Pandurino, A. (2015, September). Business Process Management - A Traditional Approach versus a Knowledge Based Approach. *6*(1/2), 54-69.

Ridder, H.-G. (2017). The theory contribution of case study research designs. *Business Research, 10*(2), 281–305. Retrieved March 22, 2018, from https://doi.org/10.1007/s40685-017-0045-z

Riigi Teataja. (2018, January 1). Child Protection Act. Estonia. Retrieved May 20, 2018, from https://www.riigiteataja.ee/en/eli/520122017002/consolide

Riigi Teataja. (2018, January 1). Work Ability Allowance Act. Estonia. Retrieved May 20, 2018, from https://www.riigiteataja.ee/en/eli/518122017009/consolide

Zainal, Z. (2007). Case study as a research method. *9*.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, 134-153.

White, S. (2004). Introduction to BPMN. *BP Trends*. Retrieved from http://www.bpmn.org

Appendix 1: Process models

Töötukassa BPMN models are included in Google Drive:

https://drive.google.com/open?id=1jIpIG-5lzuHfLku9Qf5vLOJ1KqlFMeZa

Appendix 2: Data Object tables

Data Object ID: TVHT*

Attribute	Type	Comments
id	long	
taotlusId		Application table id.
skaTaotlusId	long	Unique id in SKAIS2 application (joint application).
skaTaotlusNumber		Application number in SKAIS2.
skaEdastamiseAeg	date	Application submit date.
taotluseTaitja	tvhTaitja	Application submitter data.
hindamiseValikud	List	List of evaluation choises.
arstid	List	List of working ability evaluating doctors. Type ARST.
spetsialistid	List	List of working ability evaluating doctors. Type SPETSIALIST.
tootamine	Kontroll	Current working status.
toovoimeValistamine	Kontroll	Are there exclusive factors in working ability?
tookogemus	TvhTookogemus	Previous work experience.
oppimine	Kontroll	Is currently studying?
omandatudHaridus	TvhHaridus	Previous education information.
omandamiselHaridus	TvhHaridus	Current studies information.
hindamisJuhtum	hindamisjuhtum	Proceedings information.
vastused	list	Questionair information.
onOsaline	boolean	Is application 100% filled (can be filled partially, if toovoimeValistamine is true)?
taistaitmiseKp		Date of filling the application 100%.
taistaidetudLabivtKp		Date of 100% application review.
taistaidetudVastuvotja		Reviewer of 100% application.
skaOtsuseSaamiseViisKood	SkaOtsuseEdastamiseViis	Decision method.
skaOtsusEelteavitusEmail	boolean	The decision by Email?
skaOtsusEelteavitusTel	boolean	The decision by the phone?
skaKorduvhindAlgusKp	date	Reevaluation start date set in SKA.
skaKorduvhindLoppKp	date	Reevaluation end date set in SKA.
skaTvmMaar	string	Working ability % in SKA.
skaKuuSumma		SKA monthly payment of working ability allowance.
skaParingOnnestus	boolean	Did SKA request succeed?
oigustatudIsik	OigustatudIsik	Is person allowed to submit the application and data about the person?
terviseAndmeteVaadatavus	Kontroll	Is e-health data reviewable?

taotlejaVisiit	Kontroll	Has applicant visited the doctor and results are available?
onTaitmisestLoobutud	boolean	Did user withdraw from the application after person validation?
onRegistreeritud	boolean	Is application submitted with EL case?

Table 18. TVHTaotlus data object.

Data Object ID: TDK*

Attribute	Type	Comments
id		
staatusKood		Status code.
tyypKood		Application type.
taotlusNumber		Application number.
metaAndmed	MetaAndmed	Application metadata.
lisainfo		Proceedings handler or case manager notes.
saabumiseViisKood		Application recieval date.
otsusEelteavitusKood		Decision notification method.
esitamiseKp		Application submission date.
ennistamiseKp		
labivaatamiseKp		Reviewal date.
nkEsitamiseKp	s	Valid application date.
saabumiseKp		Application arrival date to Töötukassa.
vastuvotja		The receiver from Töötukassa.
menetleja		Case Manager.
muutja		Last editor.
kustutamiseKp		Application deletion date.
kustutamisePohjus		Application deletion reason.
kustutajaKontoId		Eraser account id.
otsuseSaajaKood		Decision receiver type.
otsuseSaamiseViisKood		Decision recieval method.
puuduseKorvaldamiseTahtaegKp		Missing data fix date.
tkoAadressTase1Kood		
klienditeenindusId		Client service id. Connected with *tkoAadressTase1Kood.*
taotleja		Applicant.
esindaja		Applicant representer.

esindajaKandidaadid		Representer candidates (received from RR).
dokumendid		Additional documents.
puudused		Missing data information.
puudusteKorvaldamiseTahtajaAjalugu		History of changes in missing data.
sisu		Application details.
itpEestkostja		

Table 19. Taotlus data object.

Data Object ID: TVTOtsus

Attribute	Type	Comments
Paevamaar		
ELPaevamaarad		
ToetuseSuurus		
PaevaSumma		
SKAKuuSumma		
SKAPerioodAlgusKp		
SKAPerioodLoppKp		
SKAEnnetahtLoppKp		
SKAKorduvhindTahtaegKp		
SKALisainfo		
OnKaalutletudEttemaks		
OnELOtsus		
ValistavadTingimused <*Kontroll 0..n*>		
SaamiseTingimused <*Kontroll 0..n*>		
RikkumiseTegevusKood		
RikkumineTaitmataKood		
TegevusId		
PoordumineId		
ItkId		
RikkumineTegevusTahtaeg		
RikkumineTegevusKatkestKp		
RikkumineTaitmataPohjus		
RikkumineTaitmataKoodMKp		
Makse KehtivadTingimused		
MuudetudPaevaMaaraSumma		

Table 20. TVTOtsus data object.

Data Object ID: OTS*

Attribute	Type	Comments
UlatusKood		
ekspertiisID		Expertise ID.
ekspertiisStaatusID		Expertise ID version.

HinnangPohjendus		Expertise reasoning. Ekspertiis::ValdkondKokkuvote*TegutsemisePiirangLause* Ekspertiis::EkspertiisKokkuvote.PiiranguAvalduminePohjus Ekspertiis::EkspertiisKokkuvote.ValistatudTegevused Ekspertiis::EkspertiisKokkuvote.PrognoosKood Ekspertiis::EkspertiisKokkuvote.PrognoosPohjendus
VastutavArst		Taotlus::HindamisJuhtum.*EkspertArstId -> Doctor's name*
TeenuseOsutaja		Taotlus::Taotlus::HindamisJuhtum::Leping::Asutus
SeisundiKestus		
EkspertiisAndmedPiiratud		Psychology decision
KorduvhindamineTaotlusAlates		
TVKaartValjastatud	Boolean	Working ability card has been given?
onVaideAluselKehtetu	Boolean	Decision has been objected successfully?
TVDuplikaatKontoID		
TVKaartValjastamine		

Table 21. TVHOtsus data object.

Appendix 3: Töötukassa feedback

Leiame, et skeemid on väga hästi koostatud ja kompaktselt esitletud. Kindlasti on need Töötukassa jaoks kasulikud ja ülevaatlikud edaspidiseks.

Hästi on välja toodud kõik GDPR-i artiklid, punktid ja võrdlus, mis puudutab Töötukassat ja töövõime hindamist ning töövõimetoetust. On hea, et välja on toodud kohad, kus meil on vajakajäämisi - nagu näiteks see, et kus ja kuidas me teavitame isikut, mille alusel ja kuidas töötleme isikuandmeid, mis andmeid töötleme jms. Nende probleemidega tegeletakse ja valmimas on kodulehele vastav teavitus. Lisaks on juba tööl juba ka andmekaitse spetsialist ehk Töötukassa on astumas samme soovitatud tulemuse saavutamiseks.

Mingitel juhtudel on töös välja toodud, et teatud protsess puudub, kuid leiame, et tegelikult on need protseduurid olemas. Neid ei ole lihtsalt vastavas infosüsteemis nagu näiteks teabenõuetele vastamine (kui inimene tahab tutvuda, mis isikuandmeid töödeldakse, artikkel 15). Leiame, et töös võiks kohe alguses ka välja tuua õigusliku aluse töövõime hindamise ja töövõimetoetuse menetluse käigus isikuandmete töötluseks (töövõimetoetuse seadus, töövõime hindamise ja töövõime toetuse andmekogu, haldusmenetlusseadus jms). Lisaks, et on olemas ka töövõime hindamise ja töövõimetoetuse protseduurireeglid, mis on kinnitatud Töötukassa juhatuse poolt.

Leiame, et magistritöös on kohti, kus võiks täpsustada, et töödeldavad andmed on ära toodud andmekogu põhimääruses, kus on ka ära toodud andmete säilitamine ja ka see, mis andmeid ei küsita andmesubjektilt ja saadakse teistest allikatest üle x-tee andmeid pärides. On ka oluline märkida, et inimene ei anna meile nõusolekut isikuandmete töötlemiseks, sest teeme seda seaduse alusel. Seega ei saa nõusolekut tagasi võtta. Samas on inimestel võimalus igal ajal avaldus tagasi võtta ja siis teeme sellele menetluse lõpetamise teate. On üks nõusolek – terviseandmete pärimiseks e-tervisest töövõime hindamisel ja seda infosüsteemi kaudu täna ära võtta ei saa, aga selle nõusoleku tagasi võtmine tähendab ka avalduse tagasivõtmist, sest terviseandmeteta ei saa töövõimet hinnata ja see tooks kaasa hindamata jätmise otsuse. Tänase seisuga on see hea tähelepanek, et seda nõusolekut võiks saada tagasi võtta, sest süsteemis ei ole otseselt võimalik nõusoleku tagasivõtmist märkida, kuid protsessi, et teha hindamata jätmine, saab teostada. Samuti ei toeta ka süsteem täna seda, et kui isik ei anna nõusolekut e-tervisest andmeid pärida ja esitab terviseandmed ise, siis piirata ekspertiisi käigus e-tervisest

andmete pärimine. Kuigi GDPR-i artikkel 9 lõige 2 punkt h võimaldab töövõime hindamiseks terviseandmeid töödelda ka ilma isiku nõusolekuta.

Isikuandmete kustutamise osas näeme väikest vastuolu. Töö alguses on juttu sellest, et isik ei saa lasta „olla unustatud“ ja andmeid registrist kustutada, kuid hiljem on kirjas, et peaks olema võimalik andmed kustutada. Tegelikult ei saa kustutada riiklikust registrist andmeid, mis on otsuse aluseks ja kogutud vastavalt andmekogu põhimäärusele. Me ei kogu lisaks põhimääruses toodud andmetele lisaandmeid, mis ei ole seotud menetlusega ja mida peaks saama kustutada.

Kokkuvõttes leiab Töötukassa, et magistritöö on väga põhjalik ja hästi koostatud. Välja on toodud problemaatilised kohad ja antud on vajalikud arengusuunad.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Robert Väljur**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose **Impact of GDPR on Personal Data Management - A Case Study**,

mille juhendajateks on **Jake Tom** ja **Maris Männiste**,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu alates **10.06.2023** kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus/Tallinnas/Narvas/Pärnus/Viljandis, **25.05.2018**