



TAMPEREEN TEKNILLINEN YLIOPISTO  
TAMPERE UNIVERSITY OF TECHNOLOGY

ANTTI KYLMÄNEN  
GENERAL DATA PROTECTION REGULATION – REQUIREMENT  
ANALYSIS OF CUSTOMER PERSONAL DATA: CASE STUDY

Master Thesis

Examiner Professor: Nina Helander  
Assistant Professor: Henri Pirkkalainen

## ABSTRACT

**Antti Kylmänen:** General Data Protection Regulation – Requirement Analysis of Customer Personal Data: Case Study

Tampere University of Technology

Master of Science Thesis, 60 pages, 1 Appendix page.

August 2018

Master's Degree Program in Information and Knowledge Management

Major: Information Management and Systems

Examiners: Professor Nina Helander and Assistant Professor Henri Pirkkalainen

**Keywords:** general data protection regulation, agile requirements engineering, customer data

Multiple companies in EU have their core business running around digital information holding data about individual people. A new GDPR – general data protection regulation aims to harmonize data protection laws in the EU giving individuals a better understanding and control of their personal data. This master thesis is a GDPR case study which investigates customer data change requirements in a company's IT systems.

The research investigated what GDPR regulation is and what is required to consent the regulation. As the case business utilizes an agile development philosophy in their software development, agile requirement engineering was researched to support the requirements analysis. By combining GDPR literature, agile requirements engineering, and case company's requirements with a deductive qualitative research approach a conceptual model for GDPR customer data requirements was made to support the case study.

The case study proceeded from general GDPR approach and semi-structured interviews to an analysis where the most critical IT systems and the then most critical change requirements were detected. The final elicited implementation descriptions including two IT systems were written in a form which the SCRUM team developers can understand, implement and create test cases for the requirements. The case study also researched the empirical effects of GDPR on the business.

The final implementation descriptions included four features for two different systems. The entity system of portal, mobile and warehouse UI required a GDPR consent. Furthermore, portal and mobile being web-based services a requirement for cookie statement was identified. The last two requirements were related to access rights. The service support tool required a group limitation feature ensuring that only relevant personnel can access the customer warehouse data. Lastly, the entity of systems required a mandatory password change improving data security.

## FOREWORD

I would like to thank Professor Henri Pirkkalainen for the continuous support and guidance during the thesis work. Also, I would like to express gratitude to the case company for giving me an opportunity to make this case study. Furthermore, I want to thank the case company's team members who encouraged me and were taking part in the work on multiple occasions. Lastly, I want to thank my fiancé and closest friends for supporting me during the thesis work.

Tampere, 20.8.2018

Antti Kylmänen

## TABLE OF CONTENTS

1.	INTRODUCTION .....	1
1.1	Motivation .....	1
1.2	Structure of the Thesis .....	2
2.	GENERAL DATA PROTECTION REGULATION .....	4
2.1	Origins of regulation .....	4
2.2	Purpose and key terms .....	5
2.3	Challenges for companies .....	7
2.4	Benefits for companies .....	8
2.5	Specific changes in customer data .....	9
2.6	GDPR compliance frameworks .....	11
3.	AGILE REQUIREMENTS ENGINEERING .....	15
3.1	Requirement elicitation .....	15
3.2	Requirement analysis .....	16
3.3	Documentation & Validation .....	17
3.4	Management .....	18
4.	RESEARCH METHODOLOGY .....	20
4.1	Research Objectives .....	20
4.2	Case Company .....	22
4.3	Semi-Structured Interviews .....	25
4.4	Use Case Diagram .....	29
4.5	MoSCoW – Prioritization Method .....	31
4.6	Nymity’s Privacy Management Accountability Framework .....	31
4.7	JIRA for Documentation .....	32
5.	CONCEPTUAL FRAMEWORK .....	33
6.	ANALYSIS AND RESULTS .....	35
6.1	Customer Data Systems .....	35
6.2	Systems Triage .....	39
6.3	Requirement integration .....	41
6.4	Implementation description .....	44
6.4.1	Information Provisioning & Collection of consents .....	44
6.4.2	Cookie banner statement .....	46
6.4.3	Access rights .....	47
6.5	Use case diagram with changes .....	50
7.	DISCUSSION & CONCLUSION .....	51
7.1	Results & Validation .....	51
7.2	GDPR implementation guidelines .....	54
	REFERENCES .....	57

## **ABBREVIATIONS**

API – Application interface; code that allows two or more programs to communicate with each other

Article 29 Working Party (WP29) – An advisory body made up of a representative from the data protection authority of each EU member State, EDPS and EU

Customer Data – Derived term to describe GDPR personal data of customers.

GDPR - General Data Protection Regulation

SCRUM – Framework for project management that emphasizes teamwork, accountability, and iterative progress toward a well – defined goal.

European Data Protection Supervisor (EDPS) – Ensures that EU institutions and bodies respect people’s right to privacy when processing personal data

European Commission – The executive of the European Union and promotes its general interest

European Union (EU) – Economic and political union between 28 European countries.

# 1. INTRODUCTION

## 1.1 Motivation

Digitalization and its applications have become a normalized resource in almost every business segment. Multiple companies in EU have their core business running around digital information that holds data about individual people leaving the individuals with poor control and understanding for which purposes, how and where their personal information is being used. Thus, the current legislative landscape has been fragmented with the old EU's data protection directive which doesn't take in to account the modern worlds privacy needs of EU residents.

A new GDPR – general data protection regulation aims to harmonize data protection laws in the EU giving individuals a better understanding and control of their personal data. The GDPR law aims to simplify data security rules in EU so that 28 separate member states of EU can all follow and fall under the same principles and rules. This makes business more transparent and fair both nationally and globally in the EU. To business, GDPR means more responsibilities but also helps to improve data protection legislation. GDPR can also improve data quality, service quality, systems quality and overall business performance.

The GDPR first came to discussion in 2012 in both European Parliament and the European Council and has come into effect in May 2016 with two years period of transition. The GDPR law currently is in the two years period of transition meaning that on date 25.5.2018 the new regulation will start to apply. This requires that the amendments must be in force by this date.

One of the major elements of the GDPR law is the substantial fines for businesses if the regulation is not complied. If GDPR implementation in business doesn't meet the requirements of the regulation the monetary penalties can result in fines up to 10 million € or two percent of a company's global revenue. However, this only cannot motive businesses to change their view of data protection, but the motives should arise from the quality perspective of the provided business services. If GDPR is implemented correctly the organizations can also enhance their data and information transparency not only to customers but also to their own employees. Things like trust, leadership, work motivation, performance, and creditability can also potentially increase due to GDPR as people get a better understanding of their personal data, what for the data exists and where that data is kept. Individuals also understand their rights to their personal data. Big corporations are required to make the GDPR changes in-line to apply for each business units. If

the changes are done well it can uniform these individual business units and improve the business processes by increasing overall efficiency corporation-wide. These aspects act as the baseline for this company case study.

To bring more value to the case study this work aims also to test new conceptual framework with the case organization. Typically, new features suggestions come straight from the customer but because GDPR is a mandatory regulation for all the companies within EU, the requirement investigation and allocation for the case company systems brings new challenges. Not only is the GDPR an extensive regulation but also having multiple unique systems handling customer data creates challenges in allocating the most critical GDPR requirements. The case study also examines how well the collaboration between the two different business units can work out.

## **1.2 Structure of the Thesis**

This section covers the structure of the thesis. The thesis consists of seven sections. First, the introduction part describes and presents the topic of the thesis, the motivation behind it and research methodology. The second part describes the GDPR literature overview, key terms, pros and cons, key changes generally and further goes more into details what are the GDPR requirements for customer data. Four different GDPR compliance frameworks are also introduced and explained in this part, one of which gets chosen to support the analysis.

Third part introduces agile requirements engineering which will be part of the empirical observation giving support to the analysis and implementation planning section. This section introduces traditional requirements engineering and combines it with Agile SCRUM philosophy which is utilized within the case business unit for software development and the technical implementation of GDPR.

Fourth part consists of information about the research process, the empirical study. On this section the case company is introduced, interviewee sampling size is presented and the interview structure is presented. Also, the organizational data protection structure, chosen GDPR framework, use case diagrams and JIRA documentation platform are described.

Fifth part forms a deductive conceptual model for the thesis work by combining agile requirements engineering, GDPR literature, and corporative requirements. One of the goals in this thesis work is to test how well agile requirements engineering works with GDPR and corporative stakeholders such as GDPR team and lawyers.

Sixth part contains analysis and results. This part introduces the customer data related systems based on the interviews. Then the most critical customer-related systems are

analyzed and picked into further analysis. The corporative GDPR requirements are then integrated with the chosen systems where requirement's necessity will be determined. Finally, the most crucial requirements get an implementation description with the support of the chosen GDPR framework, shared tacit knowledge, and agile requirements engineering methodology. The goal is to bring the final implementation descriptions in a form that the SCRUM team can understand and develop the new feature correctly.

Seventh part is the conclusion of the case study. The most critical findings are presented by answering the research questions. This section wraps up the thesis work and assesses the significance of the research. Also, based on empiricism, general advice for GDPR development are suggested and the future of the regulation is discussed.

## 2. GENERAL DATA PROTECTION REGULATION

GDPR – general data protection regulation is a new legal regulation on data protection and privacy for all individuals within the European Union and will affect every organization that collects and handles data relating to EU residents. This chapter goes through the GDPR timeline, general overview, key terms and definitions going more into details on detected change requirements within the presented thesis scope. Last part of this section provides insight into different GDPR frameworks that are popularly used to support the GDPR customer data implementation.

### 2.1 Origins of regulation

The origins of GDPR started on 25.1.2012 when an initial proposal for updated data protection regulation was presented by the European Commission. This proposal started a new discussion to strengthen online privacy rights and boost Europe's digital economy. Soon after 7.3.2012, EDPS – European Data Protection Supervisor adopts an opinion on the Commission's data protection reform package about accountability, one of the key fundamentals the GDPR law is based on. Accountability means that organizations and any third parties who help them in their data processing activities must be able to demonstrate that they comply with data protection principles. This is one of the key fundamentals of GDPR. (European Commission b)

Within same year WP29 gives an opinion on data protection reform proposal about consent, another essential part of GDPR. Consent of the individual is one of the few circumstances under which an organization may lawfully process personal data. It must be freely given, informed and unambiguous. The same facet WP29 introduced also within the same year an update concerning data breaches. Data breach notification means that organizations must notify data breaches to their data protection authority within 72 hours. These events lead the European Union to start reworking old data protection law to fit the modern era. (European Commission b)

In 2014, EP – European Parliament votes about GDPR renewal and gains 621 votes in favor, 10 against and 22 abstentions. This lead to creating the European Data Protection board a year later in 2015 replacing old Article 29 working party. New European Data Protection Board was responsible for guidelines, opinions, and decisions corresponding GDPR. A year later on 24.5.2016 the new regulation entered into force and starts to apply two years after on 25.5.2018 replacing old Data Protection Directive 95/46/EC. (European Commission b)

## 2.2 Purpose and key terms

GDPR, in general, is a massive reform of the old EU Data Protection Directive. The new data protection regulation aims to fit Europe in the digital age. The General Data Protection Regulation is an essential step to strengthen citizens' fundamental rights and facilitate business by simplifying rules for companies in the digital single market. (European Commission a)

A lot of discussion about GDPR implementation has already taken place. One of such is the capability of the organizations to meet the requirements of the regulation. The GDPR will affect every organization smaller or bigger which handle or monitor any type of personal data regardless of where they are based (Tikkinen-Piri, Rohunen et al. 2018). Thus, the implementation of the GDPR requirements demands substantial financial and human resources as well as training of the employees. "The economic impact, particularly of this unified regulation, will be significant because currently, European and non-European market participants have to deal with 28 separate legal frameworks" (Tikkinen-Piri, Rohunen et al. 2018). This will cause a lot of interpretation challenges and with the combination of potential fines of up to €20 million or 4% of company income (Mansfield-Devine 2017), creates fear in many businesses.

GDPR affects primarily on information and knowledge-intensive companies such as software houses, online advertising companies, banks, telecommunication companies and data analytics companies. Thus, the regulation crosscuts many information and knowledge management related fields such as quality management, information security (Mansfield-Devine 2017), risk management (Gellert 2018), user-centered design (De Hert, Papakonstantinou et al. 2018), customer management (van Caspel MSc). This explains why GDPR is not only about meeting mandatory requirements but businesses can also benefit from GDPR by detecting flaws in systems and business processes. For example, as customer management is an essential part of achieving and retaining customers, it is crucial to ensure that their personal data is handled correctly.

The GDPR reforms many terms and renditions of the old data protection directive such as the personal data and individual rights, data breaches, consent, compliance, entitlement to data and utilization of technology such as cookies and pseudonymization. *Table 1.* covers the most essential terms concerning this thesis' topic of customer personal data.

Term	Definition	Example
Data Subject	A natural person whose personal data is processed by a controller or a processor.	A user whose information gets collected by a website.
Personal data	Any information relating to an identified or identifiable natural person ('data subject')	First name, last name, phone number, address, age, gender.
Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data	Responsible authority for showing consent of data when a data subject first time uses a web site.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller	The processor has made a technical solution for the controller to show consent to the data subject. The processor might also show consent to data subject if controller so demands.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data.	The website requires user information to give and verify access to service.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her	The controller provides GDPR terms of use for a user in the web portal. The user clearly selects a tick-box and accepts the consent for his/her personal information to be used on the website.

Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information	A software developer programs a pseudonymization solution where user's first name and last name are replaced with "xxxxxxxx".
------------------	--	---

*Table 1. GDPR terms*

### 2.3 Challenges for companies

With the content of many new terms and articles, the welcoming of the regulation has increased lots of mixed feelings, uncertainty and even criticism within organizations and data protection experts. According to (Tankard 2016) 52% of organizations believe that the GDPR will result in fines for their businesses and 68% feel that it will dramatically increase the costs of doing business in EU. One of the problems is how to prove that you've done all you can do to protect the data as data breaches can still occur even if GDPR requirements are implemented as well as possible.

According to (Mansfield-Devine 2017) meaningful GDPR engagement will force you to take a step back and think more at the information and business process level. Why are we storing this information, where is it stored, why is it there and who has the rights to access it? According to (Tikkinen-Piri, Rohunen et al. 2018) the GDPR will strongly affect information – sensitive, small-, and medium-sized enterprises that drive their revenue from online advertising. GDPR requires to maintain data security transparently but the regulation itself can be interpreted rather loosely. Businesses vary a lot in type and size which makes it even more difficult to estimate the real effects of the regulation. (Lachaud 2016) argues that GDPR may create new discrimination between the businesses that are able to afford the GDPR certification and those that cannot. This means that especially the smaller companies might not be able to afford the expenses of GDPR. On the other hand, bigger companies which manage multiple systems will face challenges to implement GDPR correctly on each system as it will demand time, effort and money to be able to deliver these requirements on such many systems.

Another matter that worries many organizations is the pool of required skills to implement GDPR. Often, the people tasked with security have multiple roles and handling security is sometimes a voluntary additional role carried out by a software developer. As (Mansfield – Devine 2016) express: "The GDPR is about to make life worse in that regard by forcing companies to appoint a data protection officer". GDPR is a regulation meaning that it will also require juridical skills to interpret the regulation correctly.

GDPR is also seen far from trivial to implement (Koops, Leenes 2014). Moreover, as the GDPR includes a mix of the juridical and IT terms, not many jurists are familiar with the IT terms or vice versa, the IT personnel not familiar with the juridical terms. Lastly, there hasn't been any sort of indication of what logic the possible penalties will follow. For example, a data breach of multiple accounts should be a more severe issue than not having data portability-feature implemented to a system and should be penalized based on the severity.

## **2.4 Benefits for companies**

According to (Mansfield-Devine 2016) getting ready for GDPR requires data discovery and mapping which makes the GDPR so major of an event. "So far, companies have got used to just collecting the data and harvesting it for commercial reasons but that data has never been really well controlled" (Tankard 2016). Poor control, on the other hand, means lack of trackability and transparency of the data. Thus, investing in GDPR can benefit companies as they are able to utilize their data more efficiently and on the other hand improve customer trust which is an essential part of maintaining long-term customers.

According to (Tankard 2016) what is required is to implement appropriate technological and operational safeguards for securing data, including putting place strong privacy controls. Furthermore, all security systems should be continuously monitored taking into account all the risks associated with data processing and storage, including inadvertent loss or destruction. This includes also the human capital as GDPR isn't only about implementing the technical solutions but also requires effort from the employees with good working processes, habits and information security education. By understanding collectively the meaning of data privacy, companies can save money, time, customers and make work processes more efficient. With correct procedures, data security practices may enhance a general feeling of safety among customers and staff which in turn is proved to result in better work and customer satisfaction. The businesses should look GDPR more as an opportunity to enhance the business and reputation and not think of it as a mandatory regulation where the only incentive is the fines. According to (Garber 2018) GDPR compliance will force businesses to greater clarity across the enterprise.

Another benefitting approach is to get rid of all the unnecessary data or even systems. According to (Liwier 2018) if possible, to improve cost-effectiveness and provide optimal security, it is recommended to use one platform for all cloud services. The idea behind this is that it's much easier to manage one platform instead of multiple different platforms and security risks are higher with multiple and separated individual systems. According to (Mortleman 2018) technology-centered companies have been more aware of GDPR. They have applied frameworks which are good for getting basic security controls in place and realized that GDPR isn't just about looking at how you protect the data but what data you're holding in the first place and why. Businesses are then

modeled into more formal shape allowing to find efficiency savings, simplify and improve how things are done in business. (Mortleman 2018) also mentions that the GDPR process has improved business decision-making capability in terms of storing and processing data and protecting data. So, the GDPR acted as a catalyst for much broader business changes.

## **2.5 Specific changes in customer data**

This section goes through what are the key changes in GDPR related to customer data and the focus of this thesis work. The changes are covered according to the legislation and the importance of each change will vary between different businesses, countries, and sizes of organizations.

First major change to the old 1995 data protection directive is that GDPR extends the territorial scope and applies to all EU – based controllers and processors. This applies regardless where the processing takes place, personal data processing related to goods or services offered to the data subjects in the EU, and monitoring of the data subjects' behavior within the EU (Tikkinen-Piri, Rohunen et al. 2018). Unlike the 1995 directive, GDPR specifically applies to processors of the personal data of individuals. In addition, non – EU controllers of data would be subject to the GDPR provisions if they process personal data of EU residents related to the offer of goods or services in the EU (Voss 2013). According to (Kim 2018) the first step to take is to name a contact person, the data protection officer for European data protection authorities and European consumers to address questions, complaints, and requests that they are entitled to make under the GDPR. Secondly, it is essential to start monitoring all personal information related activities and processes to shape them meet the GDPR requirements. Companies are required to create data protection statements which include all information of processed data.

Data subject consent to personal data processing has been one of the much-talked cornerstones of GDPR. The GDPR adds conditions to be met with regard to the data subject's consent in order for it to serve as a legal basis for processing. First, the consent must be given for one or more specific purposes and secondly it must be also a freely given specific, informed and explicit indication of data subjects wishes (Voss 2013). According to (Tikkinen-Piri, Rohunen et al. 2018) under the GDPR, the controller bears the burden of proof of the data subject's consent to the processing of his or her personal data. This means that the controller must have a method to verify that a consent for personal information processing has been given and typically this requires some technical

solution. Consent clause also involves email advertising and cookie statement where each of the systems is required to collect a consent for these from the users.

GDPR also clarifies which users are entitled to which data. According to (Tankard 2016) organizations need to put in place strong privacy controls. This requires the companies to audit their systems access controls, data security protocols and working processes to ensure that the data is secure and that every individual can only access relevant information to them. This doesn't limit to individual personal data but to access other than your own data you need to have a solid purpose for the data processing.

The next major change in GDPR is data portability. The GDPR introduces a right for a data subject to receive his or her data in a format allowing transmittal into another data processing system, which allows them to be "portable". For example, providing a functionality to export your personal information on an excel sheet on your computer is data portability.

In addition, there is a right for the data subject to require that his or her data be "forgotten" through erasure of the personal data under certain circumstances (Voss 2013). In practice, this means implementing ways for electronic requests by data subjects, responding to the data subject's request within a defined deadline of 30 days and providing information about the reasons for possible refusals (Tikkinen-Piri, Rohunen et al. 2018). The request to be forgotten requires that all of the personal data that is inadequate, irrelevant or no longer relevant needs to be permanently removed or pseudonymized. This will require that organizations know exactly what information they hold and where it is stored (Tankard 2016).

One major requirement corresponding GDPR is the data breach notification. This means that the processor is obligated to give notification of a personal data breach to the controller within 72 hours if data breach of personal data occurs. Following an evaluation of the privacy risks, the controller and the processor must take the necessary measures to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, particularly any unauthorized disclosure dissemination or access, or alteration of personal data (Tikkinen-Piri, Rohunen et al. 2018). However, GDPR states one exception to the data breach notification. Encryption along with pseudonymization is specifically called out as an appropriate safeguard for securing data (Tankard 2016). This means that if the data is encrypted properly, organizations that suffer a data breach are not obligated to notify data subjects as the data is considered to be adequately protected.

## 2.6 GDPR compliance frameworks

This section covers few GDPR frameworks that are used to support GDPR process and implementation analysis. There already exists many different frameworks for achieving GDPR compliance, for example, a list by (Alweis 2018) but these 4 frameworks were seen as the most potential frameworks for this case study. The first basis for framework selection was the existing literature. For example, (EU GDPR Institute 2018) recommends GAP – analysis for GDPR and ISO 27001 is also mentioned in the literature by (Tankard 2016). However, as the amount of scientific GDPR literature is still rather scarce, the selection was mostly based on a conjecture between the initial material given by the GDPR team and the interview data. Thus, GDPR priority areas and Nymity's Privacy Management were seen to have integrity with the GDPR-team's material. Also, as the goal of this case study is to detect the most critical requirements for customer systems, the frameworks that included prioritization (GDPR Priority Areas) and comprehensive advice list (Nymity's Privacy Management) were seen as potential frameworks.

The chosen frameworks seem to take into account the business unit, the product/service and what GDPR requirements exist. In *Table 2.*, these different frameworks are introduced and described.

GDPR Priority Areas	Nymity's Privacy Management
<ul style="list-style-type: none"> <li>➤ Framework for prioritizing GDPR impacts</li> <li>➤ 8 GDPR core areas for priority</li> <li>➤ 8 GDPR key questions</li> <li>➤ General tips for implementation</li> <li>➤ Useful resources</li> </ul>	<ul style="list-style-type: none"> <li>➤ 39 detected Articles under GDPR that require evidence of a technical or organizational measure to demonstrate compliance</li> <li>➤ Consists of the listed table that withholds technical and organizational measures with mapping to GDPR articles</li> <li>➤ If technical or organizational measure applies to your organization, corresponding activity description will be read and implementation should follow the description</li> </ul>

GAP – analysis	ISO 27001
<ul style="list-style-type: none"> <li>➤ Consists of 10 major areas</li> <li>➤ Steps start from governance, risk management and naming DPO further going more into detail with the scope, processes, systems, and data subject needs</li> <li>➤ Good for assessing an organization’s current level of GDPR compliance but takes a lot of time and effort</li> </ul>	<ul style="list-style-type: none"> <li>➤ International management standard that provides a framework for managing information security</li> <li>➤ Consists of regular steps to identify and manage data security risks</li> <li>➤ Achieving ISO 27001 certification can provide evidence that your organization has taken necessary measures to comply with GDPR</li> </ul>

***Table 2 GDPR compliance frameworks***

The first of the proposed frameworks is “GDPR Priority Areas” by Resourcing Insight visual dashboards and reports experts company. According to (Katie Barr 2017) Priority Areas approaches the GDPR requirements by focusing the key facts concerning GDPR such as security breach conditions, individual rights, consent, and DPO. When these requirements are understood the model leverages these areas with key questions such as “do we understand how our data is utilized across the business”, “do we have a process in place to allow data subjects to request data storage and usage” and “are we using any sensitive data and does it require consent?” Lastly, according to these questions, the GDPR impacts can be prioritized. The pros of this model are that it clearly states what are the most important fields of GDPR but the con is that the model doesn’t mention how the prioritizing of the GDPR impacts should be done. A possible reason for this is that, because this is a commercial model, the measuring is purposely kept secret as well as other more detailed information about how this model should be practically executed step by step.

The second potential framework is called Nymity’s privacy management framework for GDPR. Nymity-company markets itself as the number one Research-Based Privacy Compliance Software and has also attended on LIBE – Committee meeting, a standing committee of the European Parliament on civil liberties, justice, and home affairs. This may mean that the proposed GDPR framework has some credibility.

First, the user of the framework is required to read the overview of the privacy management categories table included in the framework and check which GDPR articles refer to each category. After that, the second table of the framework shows a list of how the technical and organizational measures should be implemented. Then the user of the framework checks each of the mandatory technical and organizational measures, reads the corresponding GDPR articles and determines if the act applies to the organization.

For each of the recognized applicable technical and organizational measures to the organization, activity column is read giving information about how that activity may help the organization to comply with the obligation. Lastly, after determining the organization's primary technical and organizational measures and creating the unique organizational framework there exists additional technical and organizational measures helping to produce additional documentation to help to demonstrate compliance.

The third introduced framework is GAP – analysis for GDPR. (EU GDPR Institute 2018) recommends GAP – analysis tool with support of ISO 27001/02 standard. Although, GAP – analysis and ISO 27001 share similarities, in this thesis' work they are seen as different frameworks. At the very beginning GAP – analysis reminds a lot of GDPR priority areas and Nymity's privacy management model. GAP – analysis for GDPR consists of focusing on 10 major areas which remind a lot of the GDPR priority areas framework. Furthermore, GAP – analysis aims to determine how far organization's current practices are from being compliant within each of these areas. The challenge with this framework is how to bridge the "GAP" between current and desired outcome meaning that the GAP – analysis will require some other analysis process tools assistance such as SWOT analysis, 7S framework or Nadler – Tushman model.

(Addagada Tejasvi 2012) gives a simple to understand example of GAP – analysis. First, we identify the existing process: fishing by using fishing rods. Then we identify the existing outcome: we can manage to catch 20 fish a day. Then we identify the desired outcome: we want to catch 100 fish per day. Then comes the "GAP" which is a difference of 80 fish where simple subtraction mathematics is the analysis tool to bridge the GAP. Then we identify the process to achieve the desired outcome: use a fishing net instead of the rod. Lastly, the fishing net gets tested and verified that it works properly and meets the desired outcome. The example is simple but its effective way to understand how GAP – analysis works.

The last of the introduced frameworks is ISO 27001. According to (ISO/IEC 2013) it is the best-known standard in the family providing requirements for an information security management system (ISMS). Although ISO 27001 is older than GDPR, it concerns GDPR a lot because GDPR is based on information security. (ISO/IEC 2013) specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization". This sounds like a solid framework but ISO's official web page doesn't provide more detailed information of how the framework works. There is a catch, as in order to get a better understanding of how the framework works you need to buy a commercial license for it which costs 100€.

Some literature exists where ISO 27001 is mentioned to be a suitable approach for GDPR. (Tankard 2016) says that security standards such as ISO 27001 will help organi-

zations to ensure that they have effective information security programs in place. The use of ISO 27001 will help to ensure the principle enshrined in the GDPR that appropriate technological and organizational measures are in place to protect information. But the question how the ISO 27001 standardization process actually goes requires the explanation.

The most practical way to define how ISO 27001 works are to check the mandatory requirements for certification. According to (ISO/IEC 2013) there exist various mandatory requirements which are systems high-level design description, information security management system scope, information security policy, information risk assessment and treatment process and information security objectives. Softer values are mandatory as well such as the evidence of the competence of the people working in information security and made decisions regarding information risk treatment. It is also required to keep evidence of monitoring security, top management reviews, nonconformities identified and corrective actions arising and run an internal ISMS audit program. Thus, if an organization achieves ISO 27001 it will likely fulfill most of the GDPR requirements as well.

### **3. AGILE REQUIREMENTS ENGINEERING**

This thesis work aims to seek an approach to answer how to implement GDPR requirements. The chosen approach on that is to combine Agile Requirements Engineering theory with GDPR theory. This chapter first presents the theory of software requirements engineering and connects it to the modern agile development philosophy. According to (Curcio, Navarro et al. 2018) requirements engineering is concerned with identifying, modeling, communicating and documenting the requirements of a system and the context in which the system will be used. In this case study, the R&D unit is utilizing agile software development called SCRUM. Thus, it was suitable to choose a requirement engineering approach supporting the SCRUM development philosophy. According to (Paetsch, Eberlein et al. 2003) requirements engineering process consists of five main activities: Elicitation, Analysis and Negotiation, Documentation, Validation and Management.

#### **3.1 Requirement elicitation**

Elicitation aims to discover requirements and identify system boundaries by consulting stakeholders (e.g clients, developers, users) (Paetsch, Eberlein et al. 2003). According to (Mishra, Aydin et al. 2018) the primary measure of success for a software is the degree to which it meets the purpose which it was intended for. For example, Semi-Structured Interviewing is one method for discovering facts and opinions held by potential users and other stakeholders. Other popular requirement elicitation methods are Use case / Scenarios, Observation, Focus groups, Brainstorming and Prototyping.

According to (Mishra, Aydin et al. 2018) every technique has certain advantages and disadvantages and selection of the methods should be based on the familiarity of a method to requirement analysts and participants, preference of methods, conformance to the methodology adopted for elicitation and analysts' mindset, and relevance to the situation. This can be a difficult choice because according to (Carrizo, Dieste et al. 2014) software engineers tend to choose often a technique which is the only technique they are familiar with, it is their favorite technique, or they guess that the technique is effective under existing circumstances which might not always be the best solution.

One way to determine the elicitation process by (Mishra, Aydin et al. 2018) goes in three steps. First identify contextual situation: determination of the values associated with the attributes or features of the development context. Then evaluate the adequacy of possible techniques for the context. Lastly, obtain a Session plan where you select one or more techniques in order of priority and application for the following session.

For example, in the case of GDPR, the customer data requirements for systems can be the context. Types of customer personal data can act as attributes and their severity level can act as the values. Then based on this information, adequate techniques are chosen for the context, for example choosing MoSCoW-method to execute the severity level prioritization and choosing GDPR – framework or Use Cases to support the implementation description.

## 3.2 Requirement analysis

Requirement analysis checks the requirements of necessity, consistency, completeness, and feasibility (Paetsch, Eberlein et al. 2003). According to (Zamudio, Aguilar et al. 2017) analysis includes the creation of conceptual models or prototypes with which to achieve the completeness of the requirements and deals with understanding an organizations structure, its business rules, goals and tasks, and the data that is needed.

According to (Curcio, Navarro et al. 2018) the requirements analysis and negotiation activities enable a better understanding of the whole business and checks if the elicited requirements are consistent, complete and feasible. Sometimes, during these activities, the requirements can be modeled to make them clearer for developers. It is also possible to prioritize the requirements to satisfy some limitations such as time, resources or technical capabilities. Joint application development, requirements prioritization, and modeling are examples of requirement analysis.

Requirements prioritization is defined as an action during which the significant system requirements are identified and ordered based on their importance. The requirements are then developed iteratively as releases or iterations. The idea is that the highest priority requirement has to be implemented first before the others (AL-Ta'ani, Razali 2013). The prioritization process consists of determining which requirement should be implemented as releases. For example, daily SCRUM's and sprint planning sessions provide an opportunity to negotiate with the developers and product owner and define the priorities. This prioritization approach is heavily based on the SCRUM team's tacit knowledge. According to (Ryan, O'Connor 2013) tacit knowledge, as opposed to formal or explicit knowledge, refers to a category of knowledge that is difficult to transfer to another person by means of writing it down or verbalizing it. Thus, social interaction is necessary for transferring the knowledge and making the prioritizations in agile development. The study has also proved that face-to-face conversations are a more efficient way to share tacit knowledge than conversations through information technology. (Ryan, O'Connor 2013)

### 3.3 Documentation & Validation

Requirements documentation is to communicate requirements between stakeholders and developers (Paetsch, Eberlein et al. 2003). Documentation is an essential part of requirements engineering and information source for development. According to (Curcio, Navarro et al. 2018) in the documentation activity, the requirements are written and become a baseline for specifying all types of functional and non-functional requirements. Furthermore, the validation checks if the requirements statements are consistent and if they satisfy customer's needs. This typically involves test cases to reveal the ambiguities and vagueness in written requirements.

In SCRUM common stakeholders are the product owner, SCRUM master, and developers where the biggest responsibilities of documentation and task prioritization are the product owner's job. According to (Sverrisdottir, Ingason et al. 2014) product owner is responsible for the financing of the project during its life-cycle and he/she puts forwards the requirements and objectives of the project typically documenting the requirements electronically in some agile development platform. However, documentation is considered one of the biggest weaknesses of agile requirements engineering (Curcio, Navarro et al. 2018). This is described as problematic through the insufficiency of the user story formats. However, according to (AL-Ta'ani, Razali 2013) agile methods have been proposed in the 1990's with an aim to minimize process bureaucracy by avoiding unnecessary milestones due to the extensive documentation. The methods are intended to deliver a software system quickly to users, who can then propose and change new business requirements to systems in an iterative manner.

The terms epic and product backlog are important terms of SCRUM development documentation. The easiest way to explain an epic is by user stories. User stories are requirements in the most granular form. Stories are negotiated by the team and the Product Owner in the Sprint Planning meeting at the transition point between sprints (McKnight 2014). According to (Ellis 2016) the product backlog is the container for all the work the team will do on a product. The backlog can be thought of as an evolving specification where only the stories about to be worked on are defined in detail. The requirement gets then refined and prioritized. For example, with GDPR requirements, it would be suitable to create an epic which contains all the requirements related to the GDPR.

According to (Paetsch, Eberlein et al. 2003) requirements validation is to certify that the requirements are an acceptable description of the system to be implemented. Inputs for the validation process are the requirements document, organizational standards and organizational knowledge (Paetsch, Eberlein et al. 2003). Techniques used for requirements validation are requirement reviews and requirements testing. In SCRUM the first part of the requirements validation can be seen when a requirement is documented in an agile management platform such as JIRA.

Organizational standards can vary from SCRUM philosophy to the corporate policies and rules. Knowledge can be seen as the cognition of the SCRUM team where each of the team members has their own unique role to fulfill.

In SCRUM the requirement reviews are done before a SCRUM sprint starts. Once a new feature is implemented, a software engineer then tests the requirement. According to (Bertolino 2007) more than the act of testing, the act of designing tests is one of the best bug preventers known. This means that the requirements can be validated before the actual implementation starts to find the most critical flaws in the requirement itself so that the developer doesn't program new feature because of misinformation or because the requirement is irrational.

### **3.4 Management**

According to (Zamudio, Aguilar et al. 2017) management consists of recognizing changes through the use of continuous requirements elicitation, and includes techniques for configuration management and version control. From an agile perspective, the management of requirements engineering consists of following SCRUM development philosophy and SCRUM master's responsibilities who manages the SCRUM team process. As SCRUM is an iterative software development philosophy, the biggest responsibility in elicitation is on Product Owner who talks with the customers and updates the requirement to the SCRUM team.

Agile is a general concept used for different methods for software project management and – development (Sverrisdottir, Ingason et al. 2014). One of the primary motivations for Agile is the need to avoid the problems created by long planning cycles (Ellis 2016). Thus, agile development works well for those projects that have a low cost of iteration (Ellis 2016). Out of all the different agile methods, SCRUM is the most widely used agile software development and management method (Schuh, Dölle et al. 2018). It emphasizes product control and an important part of SCRUM is dividing people into teams and empower them to carry the tasks they are working on. All in all, agile SCRUM defines a project team and how they interact with each other (Ellis 2016)

Agile Scrum teams are typically rather small as according to (Ellis 2016) the study has shown that small teams (four to nine members) were more effective than large teams. This supports the agile ideal of self – organized teams with transparency meaning that the team members are encouraged to come up with new ideas (Sverrisdottir, Ingason et al. 2014). All in all, the Scrum team consists of a SCRUM master, a Product owner, and team members. The members are typically software developers and testers but can be something else such as CAD – designer or hardware purchaser depending on business.

The SCRUM master is responsible for SCRUM process success and management. When a team member needs help, the SCRUM master should be there to remove barriers.

ers and review current process in order to drive improvement (Ellis 2016). The SCRUM master protects the team, reducing incoming workload when the team is stressed and also pushes the team when he/she sees they are able to take on more (Ellis 2016). The SCRUM Master also runs the daily meetings and typically will run the project and report progress to upper management quantitatively and dispassionately (McKnight 2014). Where the product owner is responsible for what to do, the SCRUM master is responsible for how to do it (Sverrisdottir, Ingason et al. 2014). This creates constant interaction with all the stakeholders making sure that requirements are realistic to implement within the given schedule.

In Scrum, the project is divided into fixed-time iterations called sprints; sprints are typically 2 – 4 weeks long. During a sprint, a new iteration of software is planned, designed, coded, and tested creating a potential release (Ellis 2016). As mentioned the product owner prioritizes and assigns tasks for team members in each sprint. Each sprint is almost a mini-project, lasting just a few weeks (typically 2 – 4 weeks) and ending with a new product that could be released (Ellis 2016). According to (Ellis 2016) holding every sprint unchanged is ideal but can be changed by the customer.

## 4. RESEARCH METHODOLOGY

### 4.1 Research Objectives

This master thesis is a GDPR case study for a company about GDPR change requirements and implementation from customer's personal data point of view. The purpose is to meet the GDPR requirements and avoid possible penalties, but more importantly to give the customers a better control over their personal data and to enhance customer experience. The case company sells cranes and maintenance services as its core business but this case study focuses on one smaller individual business unit that manufactures automated material handling systems to industrial business and logistics.

The case unit of the company is small but growing unit consisting of SCRUM/R&D - team, service team and sales team. The case company has named a data protection officer and GDPR team responsible to ensure that the GDPR change requirements take place and most of the internal implementation corresponding mainly own employee data of the company. In turn, each individual unit has their own responsibility to track their own unique systems, investigate and implement the requirements for their own company cross-border systems. As the case automated material handling system utilizes many supportive information systems which contain customer data and the main product being information system itself, it is important to ensure that GDPR changes are made on each system in time before the law starts to apply.

This thesis aims to find answers to the following research questions and sub-questions.

- How to implement GDPR requirements into existing systems?
  - What to take into account in GDPR?
  - What are the most important changes in the case business?
- How did the implemented GDPR changes match the requirements and affect the business?
  - How suitable was the conceptual framework of requirements engineering for the case study?
  - How does the GDPR collaboration with two different business units within corporation work out?

The research framework utilized in this thesis is a case study based on (Saunders, Lewis 2009) research model consisting of research approaches, research strategy, choices, time horizons, data collection, and analysis. The research approach to this thesis is the qualitative deductive approach. According to (Silverman 2013), qualitative deductive

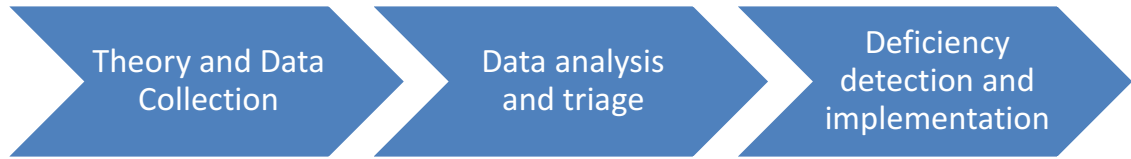
approach develops the hypothesis upon pre-existing theory and then formulates the research approach to test it. The goal is to develop the thesis from general to the more specific point of view by going through the GDPR literature and frameworks, Agile Requirements Engineering and then this will be applied into business specific context in real life.

Because the thesis is a case study for a small company unit the qualitative approach is the more suitable approach for gathering data. According to (Bryman & Allen, 2011) the aim of the qualitative approach is to investigate how the respondent interprets their own reality. For this thesis, the interviews were chosen as an effective way to collect qualitative data about the company's information systems and customer personal data to formulate an understanding of the GDPR change requirements and implementation suggestions.

The research strategy for the thesis describes how the research is carried out and this master thesis work is executed as a case study. According to (Bryman, 2015) it is an assessment of a single unit in order to establish its key features and draw generalizations. The approach is empirical which investigates a contemporary phenomenon within its real-life context where boundaries between phenomenon and context are not clearly evident. Thus, the GDPR is seen as a phenomenon whereas the context is the small company unit where the GDPR will apply to. As the information systems are unique, the case study approach is a suitable strategy to investigate the connection between the GDPR customer data requirements and the case company's customer data and systems.

Choices answers how many and which methods in research are used. According to Saunders et al. (2007), there exists mono, mixed and multi-methods to choose from to answer the choices part. In this thesis, the mono method is utilized meaning that one research approach for the case study is chosen which is called a qualitative deductive approach. This means that by combining agile requirements engineering, corporate requirements and GDPR requirements on qualitative data, we can define and assess the critical GDPR implementation descriptions on customer data related systems.

Time horizon is described as: "the time framework within which the project is intended for completion" (Saunders et al., 2009). The thesis work time horizon is estimated to last six months. *Figure 1* shows the thesis target milestones beginning at 1.3.2018 and ending on 31.8.2018. First two months are used for theory writing sections and data collection. Then data is analyzed and system prioritization is made. After that this thesis aims to integrate corporate requirements one by one on chosen systems, detect deficiencies and form implementation descriptions for the development team.



*Figure 1 Time horizon*

According to (Bryman, 2015) data collection defines how the research data is collected and is dependent on the methodological approach used. In this thesis, data collection method is a semi-structured interview where sample size will be around 10 persons which are reasonable compared to the 20 personnel which GDPR mostly concerns within case company unit. Each interview is estimated to last 1 hour ensuring that all questions can be covered sufficiently and qualitatively. The interview questions aim to discover first on which occasions an individual employee handles customer data. This way it is easy to discover each system where the customer data is stored and managed. The final system analysis is required to follow the company's GDPR team's pre-made material.

The scientific literature view, journal articles, books and official site of EU parliament and GDPR are used as literature references in theory sections. The scientific literature about GDPR is still rather scarce because the phenomenon is rather new but reasonable amount of material can be found to support the analysis section. Agile requirements engineering utilizes also existing literature of traditional requirements engineering further combining it with the agile development philosophy.

## 4.2 Case Company

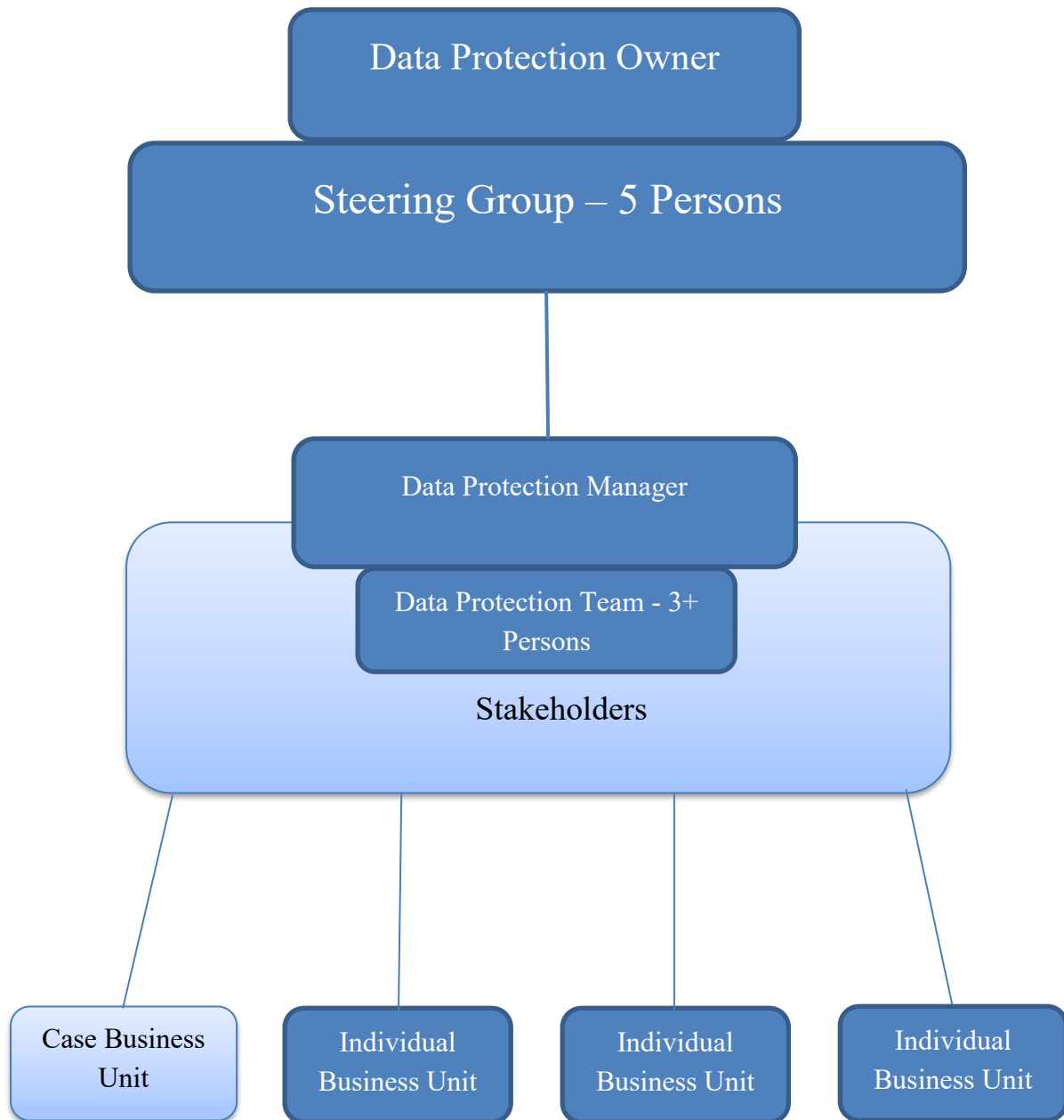
The case company is a large corporation which core business functions in industrial crane business field having approximately 750 million € revenue and 225 million € net profit during the year 2017 annual period. Most of the revenue the company makes comes from the crane business; sold machines and the maintenance services.

The company has around 600 service locations in 50 countries providing specialized maintenance service for all types of industrial cranes, hoists and port equipment operations varying from a single piece of equipment to full operations. The business contains hoists, cranes and material handling solutions for a wide range of customer business areas such as paper, forest, automotive and metals production. All in all, the sold products vary from industrial cranes, port cranes, workstation lifting systems to automated warehouses, warehouse management systems and material handling.

The case business unit is part of the company's growing investments plan to provide automated material handling solutions. The unit is located in Tampere consisting of approximately 40 personnel working among the automated material handling system. Altogether the unit has approximately 20 people that GDPR applies to, the people that work daily with the information systems and personal data. R&D team is responsible for designing and developing the sold system meaning that the GDPR findings from this thesis will be initially produced by the R&D team. The service team is responsible for the direct customer service and maintenance meaning that they work around the customer data a lot. The service utilizes maintenance tools that include lots of customer information and is also a big part of this thesis. Lastly, the sales team makes the leads of new potential customers and works face-to-face with the customers daily. They have customer relation management system where they keep customer lead information as well as contracts which are an essential part of GDPR as well.

The provided material handling solutions contract consists of an automated warehouse and its devices, maintenance and repair, remote service, software updates, data integrity and product training. Currently, the solution is provided to approximately 50 different customer companies. Also, the solution is used internally corporation-wide in multiple locations.

After GDPR came to two years transition period the company composed a data protection organization responsible for creating the GDPR project plan. Data protection team consists of Data Protection Owner, Steering Group, Data Protection Team which is led by Data Protection Manager. Each individual business units are required to implement changes to their unique systems and business processes which are not in common use corporation-wide.



***Figure 2 Case Data Protection Organization***

The upper-level Data Protection Organization was assigned to run GDPR change requirements project ensuring that the core business meets the GDPR requirements and internal company employee data is secured as well as internal processes were updated meeting the GDPR requirements. This left out the smaller individual business units and their commercial information systems. This master thesis work was made for one of these individual business units (highlighted in light blue). Each of the smaller individual business units was responsible to track their own systems and processes and make the necessary GDPR changes on these with the support of the Data Protection Team. To be

more precise GDPR implementation changes are software changes meaning that the SCRUM team was responsible for the final implementation.

This case study started in the middle of the GDPR project where Data Protection Team had already made instructions to individual business units for GDPR requirements. This case study was based on 10 customer data related topics requested by the Data Protection Team.

### 4.3 Semi-Structured Interviews

Semi-structured interviews were utilized for data collection. According to (Wilson 2014) a semi-structured interview combines predefined questions with open-ended exploration. Typically interview form goes followingly:

- An introduction to the purpose and topic of the interview
- A list of topics and questions to ask about each topic
- Suggested probes and prompts
- Closing comments

The empirical study consisted of interviewing ten people where three of them were part of the Data Protection Team and seven of them were from the case business unit. Each of the interviews lasted approximately one hour to ensure the qualitative approach of the interviews. The case study also involved many GDPR work-related meetings and communication with persons out of the interview scope but offered critical tacit knowledge to the work. Here's a list of the interviewed people and their responsibilities.

Interviewee	Job description	Business unit	Interview length	Repetition
SCRUM master	Responsible for Q&A and R&D/SCRUM team	R&D - team	53min	1
GDPR consult	Responsible for GDPR preliminary report work	Data protection team	53 min	1
Data Protection Manager	Responsible for data protection team management	Data protection team	21 min	2

IT service manager	Responsible for GDPR implementation and data security on main core business services	Data protection team	1h 12min	1
Test Engineer	Responsible for software testing and quality assurance	R&D – team	46min	1
Software Engineer/Server Specialist	Responsible for the data center, servers, software development and data security	R&D - team	50 min	2
Product Specialist/Product instructor	Responsible for training and instructing new users to use the product	Service team	1h 11min	1
Customer Service Administrator	Responsible for answering customer calls and solving errors with the customer's product remotely	Service team	58 min	1
Product Owner/UI - designer	Responsible for managing and prioritizing R&D – team tasks and designing soft-	R&D – team	1h 14min	1

	ware UI's.			
Salesperson	Responsible for acquiring and negotiating customer contracts	Sales team	1h 4min	1

**Table 3 Interviewees**

As the idea was to track all possible systems and processes of the business unit which might withhold customer data or customer rights, semi-structured interviews were seen as an effective approach. Here is the question structure utilized during the interviews.

*This interview's purpose is to gather a collection of our information systems and which customer data we store in them. The goal is to understand which systems are used in which processes, what types of customer data there moves and finally to compare them to the GDPR legislation and define GDPR tasks for the R&D team.*

1. *Could you introduce yourself, your job title and responsibilities?*
2. *Now that you have introduced yourself could you describe of information systems and/or processes that contain customer data? You can approach this question by reflecting on your everyday work and situations where you handle customer data.*

*Now that we have a perception about the customer data systems that concern your work, we shall go through 10 major GDPR customer data requirements. These questions are meant to be leading and open conversation/answers are recommendable.*

1. *Information provisioning and collection of consents. The controller is required to demonstrate that a consent for data processing has been given. How would you implement this on the systems you use? (Show an example of technical implementation)*
2. *Data protection requests by electronic means. In GDPR the data subjects have request rights concerning their personal information such as the purpose of their personal data processing and categories of personal data concerned. How would you implement this on the systems you use? (Show an example of technical implementation)*

3. *Restriction of Contact data processing. Under certain conditions, the data subjects have a right to restrict their processing for ex. with a flag. How would you implement this on the systems you use? (Show process description)*
4. *Removing of Contact data records. GDPR defines that contact data that has no use for any longer must be removed or anonymized either automatically or manually. How should this be implemented? (Show an example of anonymization). Which one is more practical approach automatic or manual? (Show an example of the manual process)*
5. *Right to access data. Data subjects have the right to gain access to their personal data. How would you implement this?*
6. *Opt – out from direct marketing. Data subjects have the right to opt-out from direct marketing. Does this feature already exist? If not then how would you implement this?*
7. *Access rights. Data subjects have the right for appropriate security and confidentiality of data such as preventing unauthorized access. How is this taken care of in your mentioned system? How would you improve access to data privacy?*
8. *Data security testing. Organizations must be able to test their technical and organizational data security. How the systems that you are using are tested? Do you have any improvement suggestions?*
9. *Cookie banner & statement. Organizations are required to implement cookie banner statements on all of their websites. Is this implemented in the system you use? (Show an example.)*
10. *Data Minimization. Organizations are required to minimize unnecessary personal data processing. This means that all of the customer data collected must be fit for purpose. Could you tell if in your systems there are any unnecessary customer data or access to it?*

All interviews were audio recorded and the answers were verified afterwards with auditing. The answers were first written in bullet points and later analyzed with the chosen framework. The experience showed that some interviews and questions didn't get as

much in detail answers as others. This was because of the difference in the daily working environment and the detected systems being outside of the works scope. For example, the salesperson emphasized CRM systems which do include a lot of customer data but because the CRM systems were in common use within the whole corporation, the responsibility of the requirements was on GDPR team. Also, many of the requirements were noticed to be compliant with the GDPR already so they didn't require further investigation as much as others.

The listening of the recorded audio was the beginning of the systems triage. The systems which were mentioned the most were brought into further analysis. Also, once the systems were identified, the systems were then further inspected based on the opinions of each ten GDPR categories. For example, if an interviewee was worried of access rights in service support tool, then the problem was discussed in the next sprint planning session. Sharing information directly with the SCRUM team members was seen as the most effective approach at this point of the case study compared to repeating the interviews as the discussions were part of the SCRUM team's habits naturally.

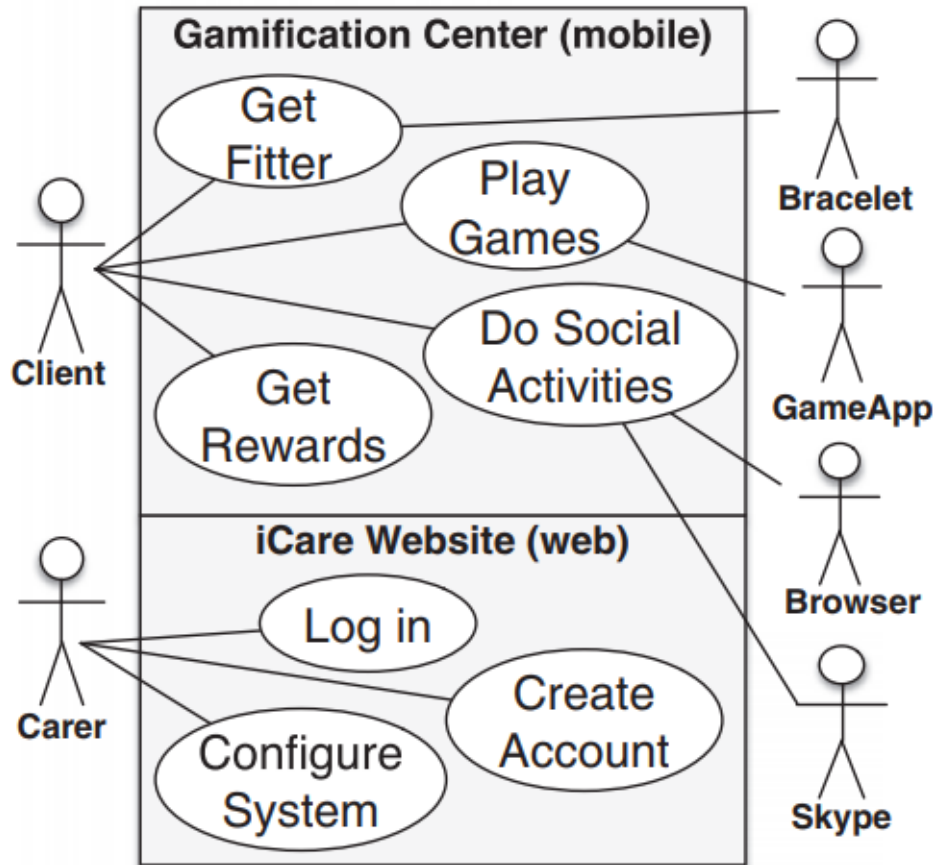
In sprint planning and daily SCRUMS the team could share tacit knowledge and judge whether to investigate a possible requirement further. Once a new change requirement was verified, it got specified during the meetings. For example, the decision of where to put logically the GDPR consent was one aspect which required attention. There were two different developers implementing features on different parts of systems. One developer was responsible of mobile and warehouse UI and another was responsible of the portal and the service support tool. For example, in order to ensure that the GDPR consent logic was the same in portal, mobile and warehouse UI, the implementation description was required to be made in sufficient detail so that both developers understood the implementation description in the same way.

The specification required also communication with the GDPR team manager and lawyers via Slack and email in order to ensure that the GDPR texts, translations and cookie banner template were in line with corporation's policies. Once the initial draft of the implementation descriptions was made a use case picture was drawn to clarify the descriptions. There were also two unrecorded meetings which contained indirectly GDPR matter of the customer contracts. However, as this work's scope was in technical implementation, the customer contracts were not covered.

#### **4.4 Use Case Diagram**

According to agile requirements engineering literature, documentation was seen lacking due to the insufficiency of user story formats. Also, the theory of requirements engineering suggests that requirements can be modeled to make them clearer for developers.

Thus, a use case diagram is utilized to support this issue with implementation descriptions. According to (Armour, Miller 2000) use cases are the base for defining functional requirements, they provide a tool for requirements traceability as well as drive development activities. (Mai, Goknil et al. 2018) introduce a common way to create use case diagram using UML – language followingly:



**Figure 3 Use case diagram example**

According to (Armour, Miller 2000) the stick figures describe the actors in the system. They aren't necessarily humans but commonly they fill the role where they'll be the users interacting with the system. The actors provide perspectives on why the use case is needed. The interaction between an actor and the system is called association. These are described with the white boxes and they are a description of what an actor can do with the system. Lastly, interfaces are the protocol and medium by which actors interact with the complex system such as the mobile and web interfaces in the example picture.

## 4.5 MoSCoW – Prioritization Method

The analysis part of the case study is based on the requirements engineering theory. MoSCoW-method was chosen to support the systems and GDPR requirements prioritization. It is a numerical assignment technique consisting of four priority groups which are MUST have, SHOULD have, COULD have and WON'T have (Khan, Rehman et al. 2015). To prioritize requirements, each requirement will be in place in one of the groups based on their priority. *Table 4* shows each of the priority levels and a description of each.

Priority	Description
Must have	The requirement in this group must be implemented in the software before it goes to release.
Should have	Important but not vital. It is considered to be important and of high value to users.
Could have	Requirements are desirable but not necessary and could improve user experience or customer satisfaction for little development cost.
Won't have	Means that requirements present in this group can't be implemented in the current iteration and are left out from the delivered solution.

*Table 4 MoSCoW prioritization*

MoSCoW – prioritization is formed based on the interaction with the SCRUM – team members and other business unit's GDPR – team. The initial material of semi-structured interviews and company's GDPR material acted as a catalyst for tacit knowledge sharing conversations and final prioritizations of systems and requirements.

## 4.6 Nymity's Privacy Management Accountability Framework

One of the introduced GDPR compliance frameworks was chosen to be utilized in the case study. Although many articles prefer using GAP – analysis along with the support of ISO 27001 for achieving GDPR compliance, the GAP - analysis was found a bit too vague to support the issues of rather specifically described need to track customer data.

The GDPR priority areas was an interesting framework option as well because it was meant to focus on GDPR areas that are the most important. The issue with the priority areas framework was that it did introduce the most important aspects about GDPR, but it didn't give any accurate advice for customer data requirement implementation. Practically what these frameworks had to offer was the preliminary mapping similar to what the data protection team had offered at the beginning of the work. What these frameworks were not able to deliver was the practical approach for the implementation phase.

The remaining of the presented frameworks, Nymity's privacy management accountability framework had aspects that were focused the most on implementation. On the higher-level analysis, Nymity's privacy management model is quite a wide approach having 12 different areas to focus on. The advantage though, was that out of these 12 areas you could easily pick what was related to customer data and your particular system requirements as the model includes over 130 privacy management activities that can support the implementation. For example, some of the 12 different areas are: managing information security risks, maintain training and awareness program, manage third-party risks, respond to requests and complaints from individuals. The framework user chooses then one of those fields and looks if it includes some useful activities that can support the implementation.

## **4.7 JIRA for Documentation**

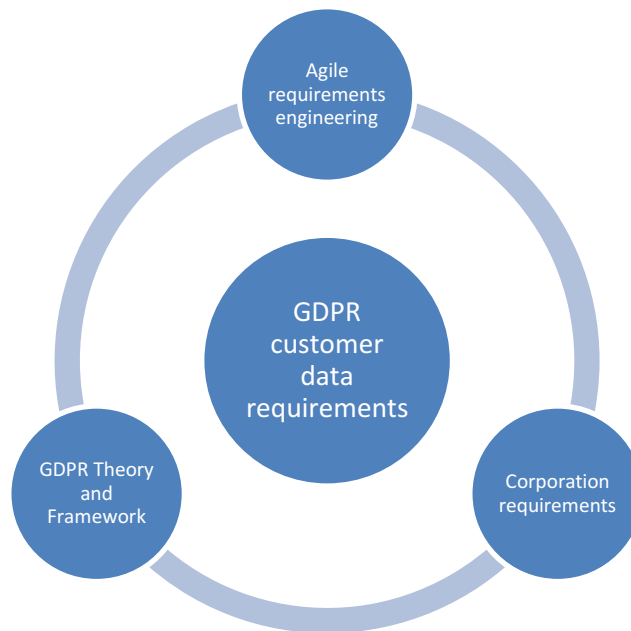
JIRA is an issue tracking and project management tool meant for agile software practitioners. According to (Atlassian Company 2018), JIRA provides planning, tracking, releasing, reporting activities. There's also an option to integrate test environments to JIRA. The case study company also had a test management platform Zephyr integrated with JIRA which provides full-featured test management, planning, and execution for the system validation.

In SCRUM development Jira supports out of the box solution to prioritize created requirements with similarity to MoSCoW-method where the severity of task typically gets accepted by product owner who then assigns the requirement to a developer in an upcoming sprint. The progress of each requirement in development is also monitored with build in status indicators of JIRA such as to do, pending, in implementation, in testing and done.

For this case study a new epic called "GDPR requirements" was created where each of the recognized requirements were initially put with implementation description and story points. Based on the company analytics, one story point is quadrated to one man – working day which makes it efficient to estimate the workloads of given tasks using SCRUM terms.

## 5. CONCEPTUAL FRAMEWORK

This section introduces the conceptual framework for GDPR customer data requirements consisting of three parts: Requirements engineering, GDPR framework, and Corporation requirements. The Conceptual framework is a combination of introduced theory sections. The framework will be utilized in the analysis & results section to finally describe the GDPR implementation requirements.



*Figure 4 Conceptual framework*

The first part, agile requirements engineering consist of elicitation, analysis, and negotiation, documentation, validation, and management which give the base for the case study analysis. Elicitation part consisted of interviewing employees in a semi-structured manner to detect customer data related systems and to find the most critical systems for further analysis. After that the most important part, the analysis consisted of first detecting the most critical systems with the MoSCoW-method based on the information given in the interviews.

After the systems analysis, the chosen systems were integrated with the corporation requirements. In practice, this required meetings and collaboration with the GDPR team and company's lawyers as well as with the SCRUM team. This part aimed to check all the given corporative requirements to find out which parts of the systems already com-

ply with the GDPR, which parts are not necessary to be implemented and which parts are required to be implemented.

Finally, with the support of the GDPR theory and the chosen GDPR framework the initial description could be made. Nymity's model is utilized by picking one of the key area fields from the model that would be related to recognized MoSCoW-“must have” features and look for a suggestion's written in the model. For example, if Electronic Data Requests would have been noticed as a “must have” feature, Nymity's model part 9. Respond to Requests and Complaints from individuals is checked. Then there are multiple options under that section which give guidance on what activities can support forming the implementation description.

Finally, the description for SCRUM team is written in JIRA for the upcoming SCRUM sprint. The issues in JIRA typically include story points, the developed system, severity level, description, SCRUM story points, assignee developer, and tester. Once the issue is put on a SCRUM sprint and assigned to a developer, the developer creates subtasks in JIRA based on the initial description to reach the goal. During the next print, the new developed GDPR feature is put to test to find possible bugs and to validate that the description matched with the new feature.

Use Case - Diagrams were also utilized for supporting the final implementation descriptions. The use case diagrams gave a better understanding to a developer of how the system should work and how the GDPR implementation can be made. Use case – diagram also supports creating test cases.

## 6. ANALYSIS AND RESULTS

This section first introduces the identified systems that fall under customer data requirements of GDPR. The systems that might reveal the case company identity were replaced with a description such as service support tool. The second part describes the identified customer personal data within these systems. This gives justification for prioritizing the most critical systems for further analysis. Third part integrates the recognized customer data and systems with the GDPR requirements and lastly in the fourth part analysis is made with the support of the chosen frameworks forming the critical change requirements as a result.

### 6.1 Customer Data Systems

This section introduces all the identified systems that hold customer data and are utilized by the business unit. *Table 5* integrates all these systems together with the description of responsibilities. Those systems which are identified as business unit's internal systems are brought to further analysis and those which are identified to be corporation-wide systems are left out of the analysis due to the responsibility for making GDPR integrations on corporation-wide systems are GDPR team's responsibility.

System	Responsibility
Portal, Mobile, Warehouse UI	Case business unit
Service support tool	Case business unit
Service Trac & QlikView	Case business unit
Network Drive	Case business unit
Siebel	GDPR team
Pactum	GDPR team

*Table 5 Identified systems*

The first identified system is the main B2B service consisting of three major software. Most of the interviewees mentioned that they either use or develop warehouse web portal daily and considered it to be an essential part of where customer data is kept. Web portal being the main source for handling the customer data, also the warehouse UI and mobile UI are integrated with the same back-end and database having similar functionalities with minor differences in UI and functionality. As one of the participants expressed "...portal, mobile, and the warehouse UI they all use a mutual database where each customer personal data is initially stored and fetched. This database is physically located in our business unit's basement".

From customer data point of view, the portal is the most critical software. Its purpose is for managing item – names, individual packets, picking lists, balance alerts, cost centers, vendor contracts and users and user groups. From the portal, you can also create reports of consumption such as transaction amounts in the warehouse, inventory information or balance consumption reports by users, user groups or cost centers on selected time. So, basically, the customer admins can customize their warehouse to be fit for purpose. The portal requires a login with username and password. As one of the participants expressed "...after user has got his/her account information from admin he logs in to the portal via login screen where terms of use are accepted, and the user can access a warehouse where they have access rights.

The portal access rights make sure that customer's users can only access their own warehouse. As one of the participants expressed "...a typical use case is that when a new warehouse is assembled to the customer, all of their users are first exported from a pre-defined file by our super admin. This gives customer users the access right on their particular warehouse which cannot be accessed by any other accounts. The access rights are also customizable as you can limit the basic users not to edit or see other warehouse users. With user groups, you can also limit item access so that the user can only see and retrieve their work-related items from the warehouse. Mobile works similarly as the portal with restrictions to user management and editing.

Warehouse UI is mostly used software of the three. As one of the participants expressed "...in warehouse UI is a front-end user interface located in front of the loading station, the place where packets are stored and retrieved. After you log in with your personal ID, fingerprint or access card you can access and see stored packages or picking lists and make a retrieve from the warehouse using the touchscreen. The doors will open, you put the package in and then warehouse robot will do the rest by moving the package into shelves. When you want to retrieve any stored package, you choose it from the UI and then the robot will know where to pick it up and bring it to the loading station". In some configurations, you can also create new items and packages with given information such as the item name, description, serial number, cost center and balance. The loading stations have scales which automatically measure the packet weight and they are used for automated inventory.

The second most mentioned system during the interviews was a service support tool which the remote service personnel utilizes daily to manage all of the customer warehouses. This includes viewing and controlling the warehouse robots and seeing the transactions of each individual packet and virtual shelves where the packages are stored. Service support tool also provides logs of packet transactions. One of the participants expressed "...it is meant for us, the system providers to fix remotely occurring problems in any of the customer warehouses. With the access to task manager logs and robot controls, we can locate and return some skewed packets manually back to the right position in shelves to give an example. Sometimes the customer warehouse may malfunction, some parts of the robot may have broken, warehouse PC may have broken or some software bug might occur...in situations like these, we need a remote control to investigate the situation.

Service support tool is also used for warehouse configurations such as the warehouse installations and is also an essential part of system testing because it gives constant information of warehouse robot movements and provides logs which are important when finding bugs of the provided system. As one of the participants expressed "...service support tool is useful for testing but it is a bit unclear whether a tester would need access to all of the customer warehouses. So far, most of the testing has been done with our internal test warehouses located in our business unit but all of, the warehouses can be accessed via the service support tool. On the other hand, a tester could act as second tier support if they might notice an error in customer warehouse before service does and then inform the service for further action. Thus, the access rights should be precisely described in the job description."

The next one of the recognized systems is service issue tracking web portal called Trac. It is a web portal where service manages their customer issues that occur in the field. As one of the participants expressed "...for customer warehouse issue tracking we have own database where we store abnormal behavior of warehouses and aim to find and solve the root cause of the problems that occur in the field...if we encounter a customer case that requires maintenance operations such as fixing the parts of the robots we create a ticket in Trac containing a description of the case and key information such as customer contact data and maintenance district's responsible personnel. Then servicemen go and make the required repairs to customer and after that the issue ticket gets closed. Thus, Service Trac is an essential part of the maintenance work.

One of the recognized systems which the case unit utilizes is the network hard drive located physically in case unit's basement including lots of unstructured data. In fact, as many of the participants mentioned the shared hard drive none of them could easily tell where and what kind of customer data there exists. As one of the participants expressed "...if a demand for erasing all information related to some particular customer person would come, it would take some manual investigation time as the hard drive has multiple folders which hold PDF's, power points, excels and many other file formats." How-

ever, network hard drive is still seen as useful. As another participant expressed "...The Hard drive also acts as a centralized database where important and old documents are centralized. Also, the positive thing about the shared hard drive is that it has access controls in place and it can be only accessed in a local network or via VPN. For example sales personnel can only access documents related to customers".

Sales personnel use a software called QlikView for business intelligence for turning big data into knowledge. As one of the participants expressed "...big data accumulates and this data itself is of no use but with QlikView, we can generate reports of sales, markets and customer transaction counts which can benefit the sales work. We have built some CRM functionality on QlikView including tasks which need to be done in cooperation with the customer." This CRM functionality was recognized as part of the GDPR requirements as these tasks come via integration from Trac, the system mentioned before. Basically, these customer tasks viewed in QlikView originate from Trac and have the same customer information and task details them meaning that they are kept for the triage analysis as one entity of software.

Sales personnel also use two other systems worth mentioning. First of them is called Siebel and it is the main CRM of the whole corporation. Siebel consists of customer contact details for possible sales leads, sales cases, and has some reporting functionality build in. However, as Siebel is one of the biggest systems within the corporation, it is excluded from this thesis' work. This is due to GDPR change requirement implementation responsibility being GDPR team's job. The interviews actually implied that Siebel was already complying GDPR to some extent having access controls in place, data security protocols and options not to send any surveys to contact persons.

The other recognized corporative system is called Pactum which is for service lease contracts. Where Siebel is used mainly for customer leads and sales cases, Pactum is used for keeping track of the customer contracts. As one of the participants expressed "...Pactum is a corporate level system and surely is already noticed by the GDPR team...however, if I could express improvement suggestion to GDPR team I would say that quick searching customer data from Pactum is pretty bad and needs improvement." This means that if a customer might want to state a GDPR demand to obtain all personal information it would require a lot of effort and time." Similarly, as Siebel, Pactum is a corporative system meaning that the change requirements responsibility lies in the GDPR team and was left out of the thesis' scope.

## 6.2 Systems Triage

This section lists previously introduced systems and lists a collection of identified customer data on each system. With the support of requirements engineering, MoSCoW - method, and sharing of tacit knowledge each of the listed systems gets a requirement severity level and the most critical “must haves” are then brought for the further analysis.

The first of the identified systems is an entity of 3 software: portal, mobile, and warehouse UI. Customer data types in these are first name, last name, and email which is the username to log in to the portal. During the first log in the user is required to accept terms of use and give or not give consent for newsletters, surveys, and marketing materials. All the personal information can be later modified and viewed from the settings: first name, last name, language, and email. The unique password to log in to warehouse UI is also generated and can be viewed from the settings.

The rest of the identified customer data in the portal are managed by the users and groups tab in some particular warehouse. This view is meant for customer master users where they can view and modify all of their employee’s privileges, access control card ID’s which are used to log in to warehouse. You can also modify the company attribute for users as some customers utilize third-party suppliers and thus these third party users can be easily identified and verified as trusted users.

Fingerprints are listed as sensitive data and are used to log in to warehouse UI. After the user first time logs in to warehouse UI using his PIN code, he can add a fingerprint to get an alternative way to log in. As one of the participants expressed “many customers utilize fingerprint to log in as their primary login method”. With the combination of being sensitive data and of heavy usage, the fingerprint login is seen as critical personal data and thus goes under “must have” priority. The entity of 3 systems are all used mostly directly by the customers, they include many personal information attributes and so supports the priority of “must have” for further analysis.

In service support tool there's an option to view and modify users of all of the warehouses. Personal data which can be processed here are user's first and last name and language which can reveal a person's cultural or social identity. The tool has one severe confidentiality problem as any user by the service or a developer in the SCRUM team can access support tool and view all the customer users, their pin codes, and emails. Service support tool also shows users marked as active and status of accepted terms of service. Also, the users marked as in-active are removed from the system but technically still exist in the database and system. This requires also a further investigation to make sure that a complete user removal can be executed. These deficiencies in data protection made service support tool in inspection level of must have as according to GDPR a

there must be a way to completely remove a user. GDPR also requires service tool users to have a reason in order to access customer personal data.

As it was found out, QlikView is an integration of Service Trac and thus they were brought together as an entity of systems. The stored customer information in Service Trac is name and email. The contact persons are typically controllers in GDPR terms in a customer company and the only necessary information is used for keeping track of the issues. Service Trac can be accessed only directly via an internal network which enhances data security. However, the HTTPS – network protocol in Service Trac is self-signed meaning that all of the web browsers rank it as a not trusted network. Having some personal information and lack of HTTPS – protocol Service Trac was listed in should have-category which is not brought to further analysis but will be discussed in Conclusions part as a potential subject.

Network drive has a lot of unstructured data of text documents which might contain personal data of customers such as first names, last names, phone numbers and emails. However, access to these unstructured documents is well implemented. Only sales personnel who will need these contact information can access the network drive folder with their user accounts and passwords. This means that those who have a purpose for the customer information can only access it and none of the customers handle network drive either. However, as the text documents are still in unstructured form, network drive gets the MoSCoW level of “could have”. Network drive could be sorted more systematically to improve transparency and in case of data removal request the data can be found, delivered or erased faster and easier. Similarly, as Service Trac, Network drive doesn’t get into further analysis part but will be discussed to some extent in conclusions part.

<b>Information systems</b>	<b>Identified customer data</b>	<b>Severity</b>
Portal, Mobile and Warehouse UI	First name, Last name, Email address, Company, User name, PIN code, Password, Access card identifier, Email consent for marketing, newsletters and surveys, Fingerprint identifier, the decision of direct marketing and newsletters	Must have
Service warehouse tool	First name, Last name, Username, PIN code, Email,	Must have

	language (Finnish/English/German)	
Service Trac and QlikView	First name, Last name, Email	Should have
Network Drive	Unstructured data; text documents that contain First name, Last name, Company, Phone number, Email	Could have

*Table 6 Identified customer data types*

### 6.3 Requirement integration

This part introduces initial corporative requirements assigned by the GDPR team corresponding customer data. Based on this information this part aims to annex the initial GDPR requirements with the chosen systems. The goal is to first find out which parts of the systems already comply with GDPR and which parts of the systems do not require changes. This will leave those requirements left which will be finally implemented to the chosen systems. *Table 7* shows the initial requirement list created by GDPR team which all of the business units need to inspect. If any of the requirements are not yet implemented either as an IT system requirement or as a process requirement they are required to be fulfilled.

#	Requirement	IT system requirement?	Process requirement?	Similar or identical requirement in Employee Data	Risk/sanction category in GDPR (low/high)
1	Information provisioning & collection of consents	X	X	Yes, similar	High
2	Data protection requests by electronical means	X		Yes, similar	High
3	Restriction of Contact Data processing	X	X	Yes, identical	High
4	Removing of Contact Data record(s)	X	X	Yes, identical	High
5	Right to access to data	X	X	Yes, identical	High
6	Opt-out from direct marketing	X	X	No	High
7	Access rights	X	X	Yes, identical	Low
8	Data security testing	X	X	Yes, identical	Low
9	Cookie banner & statement	X		Yes, identical	High
10	Data minimization	X		Yes, identical	High

*Table 7 Summary of initial requirements by GDPR team*

The systems triage left out two critical systems: the entity of portal, mobile and warehouse UI and service support tool. Based on these systems a table was created to check each GDPR requirements, the status of implementation necessity with MoSCoW and description of why or why not the system consents given GDPR requirement. MoSCoW method was extended with status “Implemented” which means that the system already consents with GDPR. Must have status requirements were brought to final implementation.

<b>System</b>	<b>Requirement</b>	<b>Status</b>	<b>Description</b>
Portal Mobile Warehouse UI	Information provisioning & Collection of consents	Must have	When the customer user logs in to portal, mobile or warehouse UI he must give consent for their data processing. Service support tool is not used by the customers but information of collecting their transaction data in various places is required to be part of the customer-side portal, mobile, and warehouse UI.
Portal Mobile Warehouse UI	Data protection requests by electronic means	Should have	The user has a right to request their personal data erasure. However, as the customer company owns the data these requests are seen as a rare possibility so that an individual user might demand data protection requests. This functionality can currently be done manually but will be automated if multiple requests occur.
Portal Mobile Warehouse UI Service support tool	Restriction of Contact Data processing	Implemented	Contact data subject has the right to request his/her contact data processing to be restricted. System admins can put the inactive flag of a customer user which restricts further processing of the user. Service personnel can access all the users from Service support tool as it is part of their job and thus relevant.
Portal Mobile Warehouse UI	Removing of Contact Data Records	Should have	It is prohibited to store such contact data that business has no use for any longer. It is possible to remove entire warehouse data once a contract with the customer ends as well as individual

Service support tool			data manually. If multiple individual requests occur this will be automated.
Portal Mobile Warehouse UI	Right to access to data	Implemented	Customer users have the right to gain access to their Contact Data. Customer master users have access to all of their users personal and transactional data in the portal, mobile and warehouse UI which can be printed out in excel from the portal. Customers don't use service support tool.
Portal Mobile Warehouse UI	Opt – out from direct marketing	Implemented	Customer users have the right to opt – out from any direct marketing. When the user first logs in portal or mobile he/she can opt out from direct marketing. Service support tool is not used by the customers.
Portal Mobile Warehouse UI Service support tool	Access rights	Must have	Businesses are obligated to ensure appropriate security and confidentiality of Contact Data. In the portal, there are multiple ways to manage secure access rights: hashed fingerprints to log in in warehouse UI, user groups with permissions, individual passwords to portal and mobile and individual pin – code to warehouse UI. However, in the portal, if a new user is generated anyone can see their automatically generated passwords before the user has changed his password. In service support tool anyone such as testers can access customer data. This requires a feature which can limit access to customer warehouse for only relevant employees such as service personnel and system admins.
Portal Mobile Warehouse UI	Data security testing	Could have	Businesses shall implement appropriate technical and organizational measures to ensure an appropriate level of security. New features are tested with the security in mind and corporation tests

Service support tool			regularly security protocol effectiveness of all of their systems. Data security testing could also include external audit to improve creditability.
Portal Mobile	Cookie banner & statement	Must have	Businesses shall implement so-called cookie banner to all its websites to fulfill its obligation to inform about the use of cookies in advance. Currently web portal and mobile don't have this functionality. Warehouse UI and service support tool are not web-based so they do not require Cookie banner & statement.
Portal Mobile Warehouse UI	Data minimization	Implemented	Businesses are obliged to minimize customer data processing so that no unnecessary customer data is collected or otherwise processed. All of the customer warehouses are configured according to the customer contract meaning that the data processing is minimized.

*Table 8 Requirements status on systems*

## 6.4 Implementation description

As the MoSCoW analysis pointed out in requirement integration, three “must have” condition requirements were identified. These are Information provisioning & Collection of consents for the portal, mobile and warehouse UI, Access rights for service support tool and Cookie banner statement for Portal, Mobile, and warehouse UI. This section creates task descriptions for each of these requirements with the support of Numinity Model, GDPR law, and corporative requirements.

### 6.4.1 Information Provisioning & Collection of consents

(GDPR 2016d) states in Art. 7 Conditions of consents.

1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

2. *<sup>1</sup>If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. <sup>2</sup>Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*
3. *<sup>1</sup>The data subject shall have the right to withdraw his or her consent at any time. <sup>2</sup>The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. <sup>3</sup>Prior to giving consent, the data subject shall be informed thereof. <sup>4</sup>It shall be as easy to withdraw as to give consent.*
4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

Based on this article there needs to be a demonstration that the data subject has consented to their processing and that there needs to be a clear way to establish the consents. Numity's privacy management framework proposes in part 8 a data privacy notice at all points where personal data is collected but this needs to be done only once per account. In order for the collection of consents to be uniform with the corporation policies, the notice is also required to contain the corporation's GDPR statement and information about the collected customer data and customer's rights for their individual data. GDPR team had implemented a web page of the corporation's GDPR policy which is required to be shown when the user first logs in to any of the systems. Based on all this information a final implementation description for the requirement was made.

### **Implementation description**

As the systems already have terms of use and collection consent for marketing implemented the best solution is to add the GDPR statement to the same context when a user logs in for the first time with their account ID and password. After the user has clicked login button a pop - up notification for GDPR statement is shown. The pop up includes a short description of why the consent is required and the purpose of the customer data processing. The pop up is required to clearly show a hyperlink for the corporation's contact data protection description. The user cannot proceed until he/she has clicked "I have read and understood the contact data protection statement. After this, the already implemented notification pop up for marketing consent and terms of use is shown. The implementation needs to be identical logically within all of the systems: portal, mobile, and warehouse UI.

From a technical point of view and based on discussions with the SCRUM team the new feature requires changes in backend and databases, new pop – up UI – design, UI functionality, language localization and test planning and execution. These tasks are esti-

mated with Agile requirement engineering's story points. Backend and database changes (1 story point), Pop – up UI design (1 story point), functionality to UI (1 story point), language localization (0.5 story points), test planning and execution (2.5 story points). Altogether before possible bug reports, bug fixes and validations the estimated story point amount is 6 story points. As 1 story point is estimated to be 1 man - workday it means the feature can be implemented within 6 days. However, in order to successfully validate the functionality of new feature, it is recommended to reserve at least 2-week man - workday time slot as the whole development time because of the possible bugs, regression, and fixes to all of the three systems.

### **6.4.2 Cookie banner statement**

Cookie banner statement is induced from (GDPR 2016e) Recital 30 online identifiers for profiling and identification.

*Natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*

Based on this a consent for cookies in portal and mobile is required as they both are web pages and utilize cookies in order to function. Numity's privacy management model suggest in part 4. "Embed Data Privacy Into Operations" to integrate data privacy into the use of cookies and tracking mechanisms. As no other tracking mechanisms in these web pages were identified, a cookie banner for portal and mobile will fulfill this requirement. Similarly, as with the GDPR statement consent, a corporative requirement for cookie banner is to make a hyperlink to corporation's cookie statement page.

#### **Implementation description**

The implementation description for cookie banner statement is pretty similar to GDPR consent feature. Once a user goes to either portal or mobile web page, a cookie statement will be shown and then a user can open up a hyperlink, read the cookie consent and click the OK button to confirm understanding that the web page utilizes cookies and continuing using the service.

From an agile requirement engineering point of view, new feature requires changes to the back-end (1 story point), cookie pop – up UI - design (0.5 story point), functionality to UI (0.5 story points), language localization (0.5 story points) and test planning and execution (2 story point). All in all, this means 4.5 story points which can be estimated

at 4.5 man – working days. As there are only two systems to test and validate the whole development and releasing is possible to make within one sprint week.

### 6.4.3 Access rights

Access rights requirement comprehend multiple GDPR articles: 24 - Responsibility of the controller, 29 – Processing under the authority of the controller or processor and 32 – security of processing. Since there are multiple GDPR articles and they are expressed really long in regulation, key points corresponding detected systems are brought as the basis for implementation description.

(GDPR 2016a, GDPR 2016b, GDPR 2016c) state the following:

#### Art. 24 – Responsibility of the controller

1. *Taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. <sup>2</sup>Those measures shall be reviewed and updated where necessary.*
2. *Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*

#### Art. 29 – Processing under the authority of the controller or processor

*The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller unless required to do so by Union or Member State law.*

#### Art. 32 – Security of processing

*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.*

Based on these three articles the access rights requirement can be summed up to ensure appropriate security and confidentiality of contact data. This means preventing unau-

thorized access to or use of contact data and the equipment used for the processing. In requirement integration, access rights deficiency was detected in all of the chosen systems: portal, mobile, warehouse UI, and service support tool. Numity's privacy management model's part 6. "Manage information security risks" guides to maintain procedures to restrict access to personal data, for example, having role-based access and segregation of duties. The identified service support tool deficiency in access rights was related to this issue.

### **Implementation description (Service support tool)**

In service support tool the detected deficiency relates in unauthorized access by business unit employees which currently can access any of the customer warehouses and see customer personal data. This is unconventional because although service support tool is used mainly by the authorized service personnel which naturally require using the tool for their service work, also for example testers which need access to the internal test warehouses can access customer warehouses as well. Thus, there needs to be a new feature to create user groups for having access only to work-related and relevant warehouses. For service personnel, this means of course access to all of the warehouses but the testers will only need access to test warehouses.

The description for the access control goes followingly. Once a user logs in to service support tool a table of warehouses is shown. The software should show only those warehouses which the users have access to and only users of these warehouses. In order to manage the access control, there also needs to be a mechanism for admin users to create user groups and give relevant warehouse access rights to employees.

In agile requirement engineering the implementation requires changes to back-end (1 story point), new groups tab with UI to user manager (0.5 story point), functionality to UI (1 story point), test planning and execution (2 story points). Altogether the work requires 4.5 SCRUM story points and thus 4.5 man – work days. As the system is used for managing all the existing warehouses the possible regression risk and bug fixes might expand the development time. Thus, it is recommended to reserve at least two sprint weeks for development and testing altogether before release to ensure the quality of the new feature.

### **Implementation description (Entity of portal, mobile, and warehouse)**

In entity of systems, one major deficiency regarding access rights was noticed. Portal is used for managing access control in the portal, mobile, and warehouse. When a new user is created, a randomly generated password is shown in the portal which the portal master user can print to a new user or send it directly to the new user's email. The problem is that this password is visible to anyone who can access the user's tab as long as the

original password is unchanged. Thus, there needs to be a mechanism that forces new users to change their random generated password right after the first time login to the portal. This new feature will be implemented to portal and mobile but it will affect warehouse UI as well because all the personal data is managed in portal such as warehouse UI's log in pin – code. Once released the new feature will prevent unauthorized access and enhance the security of all the three systems.

The description for compulsory password change goes followingly. The generated passwords can be known by anyone which is why they are required to be changed during the first portal or mobile login. Once a user logs in with the generated password a pop up will show which asks the user to change the password to a new one. Password change can be canceled but portal or mobile cannot be accessed until the user has changed his/her password. The given password must fulfill the following rules:

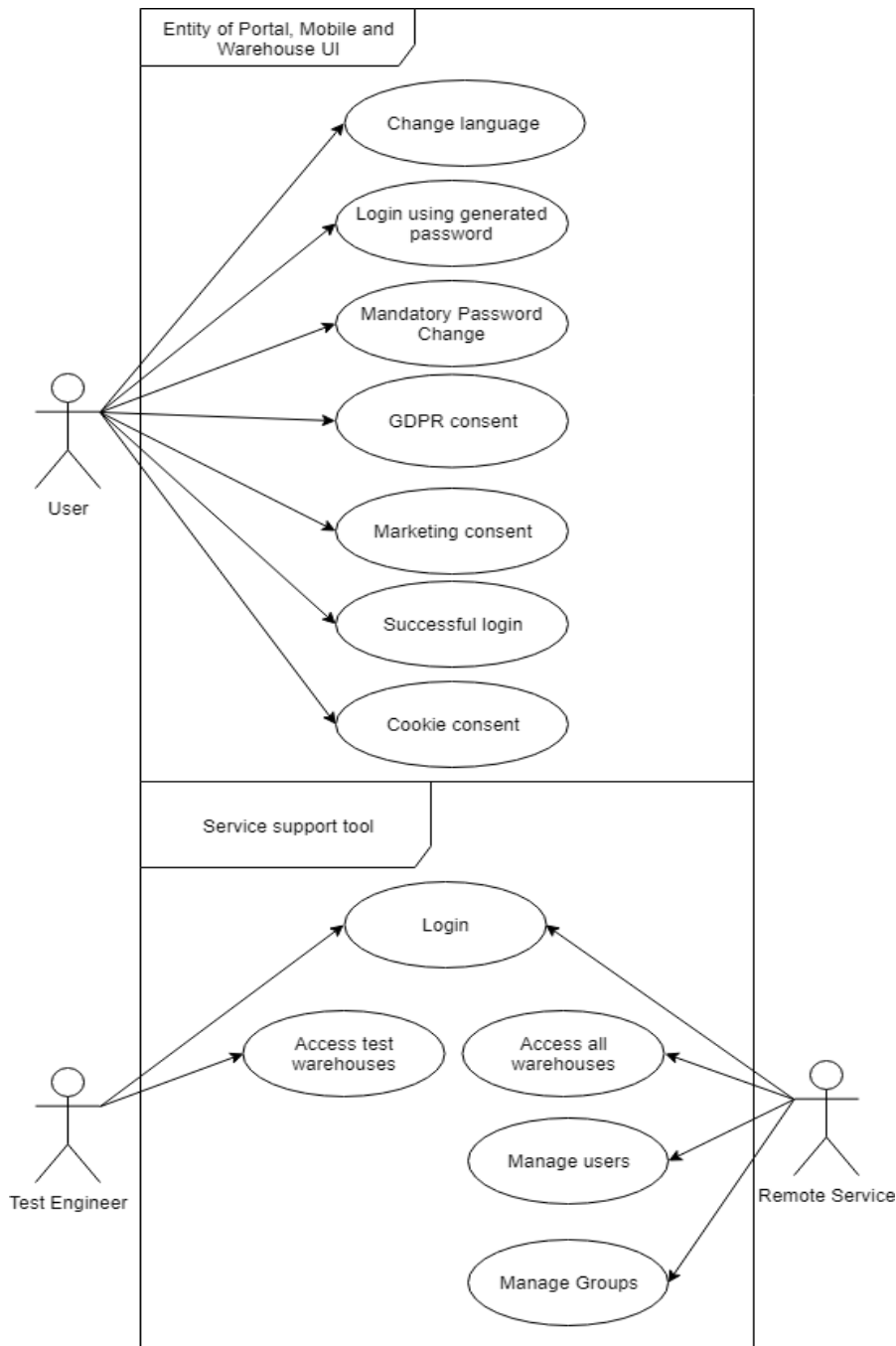
- Password must be at least six characters long
- Password cannot be longer than 72 characters
- Username and password cannot be the same
- In addition, at least three of the following conditions must be fulfilled:
  - Password must contain at least one digit (0-9)
  - Password must contain at least one lowercase letter (a-z)
  - Password must contain at least one uppercase letter (A-Z)
  - Password must contain at least one special character

With agile requirements engineering the given task can be estimated to include following changes to the portal: Mark to back – end of password changed (0.5 story point), UI – design (0.5 story point), Functionality to UI (0.5 story point) and Localization (0.5 story point). Once these tasks are done the mobile implementation can replicate the portal design using the same back-end, UI – design, and functionality (altogether 1 story point). Finally, it is required for both portal and mobile to make test planning and execution (2 story points).

Mobile implementation is estimated to take less time than portal because once portal implementation is ready, mobile can use the same back-end, UI – design, and localization which saves implementation time. Also, test planning for both portal and mobile will be similar but test execution is still required to be made for both portal and mobile as well as possible bug findings and fixes. All in all, releasing new feature requires 5 story points and thus 5 man – workdays. It is possible to make the new feature within one scrum sprint week, but there should be time reserved for possible issues with development and testing.

## 6.5 Use case diagram with changes

The use case picture below demonstrates how the systems can be used after the GDPR changes are implemented. New changes are mandatory password change, GDPR consent, and cookie consent. The service support tool required a new feature enabling to create and manage user groups to limit the access only to relevant warehouses.



*Figure 5 Use case diagram with the GDPR changes*

## 7. DISCUSSION & CONCLUSION

This section discusses and validates the final results. What was developed, how well did the process go and did the final implemented features match the original requirements? Validation part also aims to review the utility of the conceptual framework. Was it useful for the particular case study? Lastly, future research discusses possible topics related to GDPR's state, agile requirements engineering and the future of the company.

### 7.1 Results & Validation

This thesis' goal was to recognize the most critical customer data systems and describe the change requirements on these systems in order to consent GDPR. The following questions were described to support the objective.

- How to implement GDPR requirements into existing systems?
  - What to take into account in GDPR?
  - What are the most important changes in the case business?
- How did the implemented GDPR changes match the requirements and affect the business?
  - How suitable was the conceptual framework of requirements engineering for the case study?
  - How does the GDPR collaboration with two different business units within corporation work out?

The first question was aimed to first seek a theoretical background for what to take into account in GDPR requirement implementation and then describe how this case study resulted utilizing the deductive conceptual framework. The literature showed that it is important to get familiar with the purpose of the GDPR and with the most essential terms as the new regulation has reformed many terms of old EU Data Protection Directive. The incentive of potential fines is also important to assimilate but the reasons for GDPR implementation should arise from the business continuance so that businesses can also benefit from the new regulation.

Many companies lack the transparency and security of data and GDPR should be seen as an opportunity to also enhance these areas (Mortleman 2018). One approach to this is to get rid of all the unnecessary data or even systems (Liwier 2018). GDPR demands to appoint a data protection officer in each organization (Kim 2018). This shouldn't only be seen as an obligatory requirement but as a catalyst to the better data protection practices which in the long term can benefit organizations (Mortleman 2018). Data protec-

tion officer needs to lead the GDPR changes within the organization and start to systematically monitor all personal data that gets collected. That way an organization can create the data protection statements which are required for the GDPR consent.

From the GDPR implementation perspective, one of the biggest challenges are the required skills to implement the requirements (Mansfield – Devine 2016). The GDPR literature also showed that businesses are worried about achieving the GDPR consent (Tankard 2016). The regulation is seen as far from trivial to implement consisting of a mix of juridical and IT terms meaning that the organization might need some consultancy or start to educate themselves (Koops, Leenes 2014). Also, there are many existing frameworks that can support the GDPR implementation such as ISO 27001 and GAP – analysis but choosing the correct framework and measures depends on the context and can be challenging (Koops, Leenes 2014). The common similarity with most of the frameworks is to start the GDPR implementation work with perceiving and detecting the most critical deficiencies in systems or processes and start to implement GDPR changes on them. When the most important changes are made, then it is easier to iteratively continue the requirements engineering (Ellis 2016).

The second sub-question was aimed to identify the case business unit's systems that hold customer data, analyze their criticality for GDPR changes, and finally create the implementation descriptions for these GDPR changes. This question was approached with a deductive conceptual model consisting of agile requirements engineering, case corporation's requirements and GDPR theory and frameworks.

Out of the recognized six systems, the analysis pointed out that four of these were managed by case business unit: Entity of portal, mobile and warehouse UI, Service support tool, Service Trac & QlikView and Network Drive. Finally, two of these systems were chosen to be the most critical customer data systems based on the attributed amount of personal data and tacit knowledge shared via semi-structured interviews and meetings. These systems were service support tool and entity of portal, mobile and warehouse UI. The portal, mobile, and warehouse UI are used by multiple customers having multiple personal data attributes and data subjects. They are also sold as a product family with joint API which is why they were presented as an entity of systems. Service support tool is used by multiple employees within the case business unit including an access to all of the customer warehouses and customer personal data. Thus, these two systems clearly stood out from the rest of the recognized systems.

Based on the company's initial change requirement material, the two systems were analyzed with the support of GDPR articles, Nymity's privacy management framework, and MoSCoW-prioritization method. The final detected critical changes to these systems are:

- Information provisioning and collection of consents

- Company's GDPR compliance statement and consent in Portal
  - Company's GDPR compliance statement and consent in Mobile
  - Company's GDPR compliance statement and consent in Warehouse UI
- Cookie banner statement
    - A pop up that requires consent for using cookies in Portal
    - A pop up that requires consent for using cookies in Mobile
  - Access rights
    - Mandatory password change from a generated password for Portal and Mobile
    - User Group limitation for service support tool

All of the recognized critical requirements were possible to be implemented with the SCRUM team's and GDPR – team's resources. All in all, these GDPR changes required approximately 20 story points meaning 20 man–workdays including testing, bug fixes, and acceptance. Three developers and two testers were involved to achieve these GDPR changes meaning that roughly four working days per each were required. However, developing a new feature goes mostly in turns meaning that most of the work requires one task to be finished first before the next task can be done. Thus, these requirements couldn't be done within one sprint week but required two weeks of development time to obtain stable release status.

The second question was aimed to validate the conceptual model. Based on the outcome the model worked efficiently. The model emphasized a lot of sharing tacit knowledge via semi-structured interviews and SCRUM meetings. This part could be seen as the elicitation part of the requirements engineering. After this, the MoSCoW-prioritization was important tool in order to limit the focus of the study to the most critical changes. The biggest challenge was the amount of systems and requirements but with the support of analysis, documentation and proper SCRUM management the prioritization was able to be done. Having six recognized systems at the beginning and combining it with the 10 GDPR team's requirements was rather wide scope to start the analysis. This part especially emphasized the importance of the agile requirements engineering.

The conceptual model was able to support the limitation of the systems to the two of most important systems. After that it was easier to look the requirements and systematically give MoSCoW-value on each requirement. The extended attribute "implemented" for MoSCoW was also necessary to describe the requirements which already consented the GDPR. Lastly, once the critical requirements were identified, they were described in Jira using the story points and use case picture. The final use case diagram was particu-

larly helpful to show effectively how the systems are supposed to work after the implementation. The system requirements were finally validated in the software testing process after which the new features were released.

The biggest challenge and flaw during the case study was the communication between the GDPR team. As the members of the SCRUM team were seen daily and they were easy to approach, the emphasis of sharing knowledge in meetings was effective. However, with the external GDPR team choosing to use information technology for communication wasn't as effective. Thus, the conceptual model requires an adjustment to emphasize more the communication between external stakeholders. Also, choosing the correct persons for the interviews could utilize some supportive model. A lot of time was spent recording and auditing the interviews but some of them didn't prove as much valuable information as others.

## **7.2 GDPR implementation guidelines**

The made changes were mandatory in terms of GDPR and critical in order to achieve customer personal data security. Most of the customers were aware of GDPR's date of coming to force and thus it gave a positive impression that the case business unit had made effort to consent the GDPR. The cooperation speed with the GDPR team wasn't as agile as with the internal SCRUM team. This was due to not having enough face-to-face meetings which made it difficult to share tacit knowledge between the GDPR team and SCRUM team. Agile requirements engineering literature suggests that sharing tacit knowledge is more efficient face-to-face than conversations through information technology (Ryan, O'Connor 2013). Thus, it is recommended to physically meet the other stakeholders even if it requires traveling long distances. Also, communication verbally can be more efficient than using direct messages such as slack and email. Thus, video chat can be a more efficient approach as well.

When implementing features required by law or regulation, there should be enough allocated time for the unpredictable scenarios. Case study's empirical experience indicated that similar projects should have a soft deadline to ensure that the system is validated as comprehensively as possible early enough. However, this can be difficult as agile software engineering prefers iterative action over comprehensive documentation which would require changes in developers working habits (AL-Ta'ani, Razali 2013). The idea of SCRUM is to deliver and then make the adjustments based on the customers' opinions in an iterative manner. The challenge with this scenario is that when developing features based on a law or regulation demands that when the regulation starts to apply the implemented feature should already be perfect and comply with the law. Releasing and fixing the feature iteratively early on can fix this issue but requires convincing

the developers to understand why the release is required to be made early before the regulation starts to apply.

Before the regulation started to apply there was much of speculation. Possible “what if” scenarios were thought of which could be fatal to business if such scenario might occur. If multiple people would request their personal data, the employees would have been overworked to manually fetch the data from multiple systems. The utilized approach was outcomes-based so that if multiple requests would occur then the automation would be implemented later. If multiple personal data requests would occur the business might not be able to answer customer requests fast enough, the process would also consume normal working time and in the worst case scenario result in fines (Tankard 2016). However, with SCRUM philosophy it was more natural to first make the most necessary implementations on systems and then start to iterate and enhance the solutions. (Ellis 2016).

It is important to understand that GDPR doesn't represent customers' needs but more vaguely every EU citizens' needs. To be more precise, it was made in EU parliament by politicians, not by the customers which is why the businesses should primarily seek for the most benefitting approaches for the changes. This means that the changes to systems should aim to increase customer satisfaction and make the access to data easier and transparent. This is in line with the literature as it suggests that GDPR shouldn't be only done because it is a mandatory regulation, but the companies should also seek possible business value out of the GDPR process (Tankard 2016). When only necessary data of customers is collected it can improve for example information analytics and decision making in business. The challenge is that businesses won't always recognize easily or fast which of the customer data is the most important for business continuity and the customers themselves. Furthermore, if changes are made on a tight schedule, there is a possibility to make harsh decisions resulting in worse. For example, if there isn't enough time for testing and validation it can lead to losing customers and increasing developing expenses. Literature has shown that poor quality assurance and validation will cost a lot to businesses (Mead, Stehney 2005).

Although no GDPR conflicts have occurred in case company, the first GDPR precedent has already occurred elsewhere. According to (Virtanen 2018) in Germany, a sister company of a U.S domain names company declined to collect personal data of people purchasing domains because they didn't have any justification for that. Court of law stated that the German company was correct but the U.S company complained about the decision to higher court later. This means that the incentive of fines should be taken seriously. This also proves that the made implementations of GDPR consent and access control of service warehouse tool are justified.

The initial idea of general data protection is good. People require a right to see more transparently where their personal data is used and more importantly what kind of per-

sonal data about them is actually collected. This might surprise many people in an era of internet where many things are seen as “free”. When individuals understand more about the data privacy, they assimilate that they often trade their own privacy with the free content for example.

The decision making is now on users. Now that the GDPR exists, people are given choices about using the services. At the moment, most of the services are either yes- or no-choices where you can only either use the service by giving out all of your information or not using at all. In the future, one possible competitive advantage for IT services could be that the users can still use the services partly or completely without sharing their personal data. This could be one approach to investigate further as the literature suggests that companies should seek advantages from the GDPR.

It seems that GDPR isn't fair for all of the business. Commercial companies' services are dependent on knowing personal data about their customer. Thus, it is difficult to see that commercial companies could make their business work without getting GDPR consent for customer data. Before the GDPR came into effect, for example, the CEO of Facebook got a lot of pressure in media about accidentally enabling customer data harvesting for wrong purposes (Naughton 2018). Although the outcome was not intentional, it implicates that GDPR can force businesses to make better and more thoughtful decisions which in the long run can benefit the businesses.

GDPR is still waiting for its shape in EU. The purpose for the existence of the regulation is justifiable but the content of the regulation left some room for improvement as the regulation is ambiguous and vaguely expressed in the literature (Koops, Leenes 2014). However, as the first precedent has finally occurred the regulation shouldn't be taken lightly. There might occur many more of this kind of warning cases in the near future where companies can only but learn. One of the interesting future research cases would be investigating the loopholes of GDPR as during this thesis work some incoherent parts of the regulation were noticed. There's also a possibility to research topics such as would it be possible to abuse GDPR for wrong purposes because of the vagueness. It is highly likely that strifes related to GDPR will be seen in the court similarly as with the precedent of domain name companies. Another interesting future research topic would be to interview the case company's customers and their opinions about GDPR and what do they think about the regulation and the made changes to the systems. With this information and agile practices, the current solutions could be improved iteratively. The research could also focus on questions like has the GDPR improved the customers' life or has it been vice versa? The research would further extend the comprehension of the regulation.

## REFERENCES

ADDAGADA TEJASVI, 2012. Do We Need a Mature GAP analysis. *Business Analyst Times*, , pp. 1.

AL-TA'ANI, R.H. and RAZALI, R., 2013. *Prioritizing Requirements in Agile Development: A Conceptual Framework*.

ALWEIS, Jan 1, 2018-last update, Top 10 GDPR Frameworks. Available: <https://alpin.io/blog/top-10-gdpr-frameworks/> [13.8., 2018].

ARMOUR, F. and MILLER, G., 2000. *Advanced use case modeling: software systems*. Pearson Education.

ATLASSIAN COMPANY, 2018-last update, The #1 software development tool used by agile teams. Available: <https://www.atlassian.com/software/jira> [17.8., 2018].

BERTOLINO, A., 2007 Software testing research: Achievements, challenges, dreams, *2007 Future of Software Engineering 2007*, IEEE Computer Society, pp. 85-103.

CARRIZO, D., DIESTE, O. and JURISTO, N., 2014. *Systematizing requirements elicitation technique selection*.

CURCIO, K., NAVARRO, T., MALUCELLI, A. and REINEHR, S., 2018. *Requirements engineering: A systematic mapping study in agile software development*.

DE HERT, P., PAPAKONSTANTINO, V., MALGIERI, G., BESLAY, L. and SANCHEZ, I., 2018. *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*.

ELLIS, G., 2016. *Chapter 8 - Agile Project Management: Scrum, eXtreme Programming, and Scrumban*. Boston: Butterworth-Heinemann.

EU GDPR INSTITUTE, 2018-last update, Conduct a GDPR GAP Analysis. Available: <https://www.eugdpr.institute/conduct-a-gdpr-gap-analysis/> [13.8., 2018].

EUROPEAN COMMISSION, a-last update, Data protection in the EU. Available: [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_en#fundamental-rights](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#fundamental-rights) [19.4., 2018].

EUROPEAN COMMISSION, b-last update, The History of the General Data Protection Regulation. Available: [https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation\\_en](https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en) [19.4., 2018].

GARBER, J., 2018. *GDPR – compliance nightmare or business opportunity?* .

GDPR, 14.4., 2016a-last update, Art. 24 GDPR Responsibility of the controller. Available: <https://gdpr-info.eu/art-24-gdpr/> [1.8., 2018].

GDPR, 14.4., 2016b-last update, Art. 29 GDPR Processing under the authority of the controller or processor. Available: <https://gdpr-info.eu/art-29-gdpr/> [1.8., 2018].

GDPR, 14.4., 2016c-last update, Art. 32 GDPR Security of processing. Available: <https://gdpr-info.eu/art-32-gdpr/> [1.8., 2018].

GDPR, 14.4., 2016d-last update, Art. 7 GDPR Conditions for consent. Available: <https://gdpr-info.eu/art-7-gdpr/> [1.8., 2018].

GDPR, 14.4., 2016e-last update, Recital 30 Online identifiers for profiling and identification\*. Available: <https://gdpr-info.eu/recitals/no-30/> [1.8., 2018].

GELLERT, R., 2018. *Understanding the notion of risk in the General Data Protection Regulation*.

ISO/IEC, 2013-last update, ISO/IEC 27001:2013(en). Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en> [10.8., 2018].

KATIE BARR, Sep 15, 2017-last update, RTT – GETTING TO GRIPS WITH GDPR IN RECRUITMENT AND HR. Available: <https://resourcinginsight.com/2017/09/15/rtt-getting-to-grips-with-gdpr-in-recruitment-and-hr/> [13.8., 2018].

KHAN, J.A., REHMAN, I.U., KHAN, Y.H., KHAN, I.J. and RASHID, S., 2015. Comparison of requirement prioritization techniques to find best prioritization technique. *International Journal of Modern Education and Computer Science*, 7(11), pp. 53.

KIM, S., 2018. The Year of the GDPR. *Research World*, 2018(68), pp. 48-49.

KOOPS, B. and LEENES, R., 2014. Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law. *International Review of Law, Computers & Technology*, 28(2), pp. 159-171.

LACHAUD, E., 2016. *Why the certification process defined in the General Data Protection Regulation cannot be successful*.

LIWER, D., 2018. GDPR: one size does not fit all. *CSO (Online)*, , pp. n/a.

MAI, P.X., GOKNIL, A., SHAR, L.K., PASTORE, F., BRIAND, L.C. and SHAAME, S., 2018. *Modeling Security and Privacy Requirements: a Use Case-Driven Approach*.

MANSFIELD-DEVINE, S., 2017. *Meeting the needs of GDPR with encryption*.

MCKNIGHT, W., 2014. *Chapter Sixteen - Agile Practices for Information Management*. Boston: Morgan Kaufmann.

MEAD, N.R. and STEHNEY, T., 2005. *Security quality requirements engineering (SQUARE) methodology*. ACM.

MISHRA, D., AYDIN, S., MISHRA, A. and OSTROVSKA, S., 2018. *Knowledge management in requirement elicitation: Situational methods view*.

MORTLEMAN, 2018. Case study: Becrypt discovered unexpected benefits in preparing for GDPR. *Computer Weekly*, , pp. 20.

NAUGHTON, 2018, Apr 7,. How Facebook got into a mess – and why it can't get out of it. *The Guardian*, 1.

PAETSCH, F., EBERLEIN, A. and MAURER, F., 2003Requirements engineering and agile software development, *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on 2003*, IEEE, pp. 308-313.

RYAN, S. and O'CONNOR, R.V., 2013. *Acquiring and sharing tacit knowledge in software development teams: An empirical study*.

SAUNDERS, M.L. and LEWIS, P., 2009. P. & Thornhill, A.(2009). *Research methods for business students*, 4.

SCHUH, G., DÖLLE, C., KANTELBERG, J. and MENGES, A., 2018. *Identification of Agile Mechanisms of Action As Basis for Agile Product Development*.

SILVERMAN, D., 2013. *Doing qualitative research: A practical handbook*. SAGE Publications Limited.

SVERRISDOTTIR, H.S., INGASON, H.T. and JONASSON, H.I., 2014. *The Role of the Product Owner in Scrum-comparison between Theory and Practices*.

TANKARD, C., 2016. *What the GDPR means for businesses*.

TIKKINEN-PIRI, C., ROHUNEN, A. and MARKKULA, J., 2018. *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*.

VAN CASPEL MSC, E., The Return to the Customer: Three Strategic Choices of Privacy Management.

VIRTANEN, 2018, Jul 10,. Saksa ehti ensimmäisenä – GDPR-päätös napsahti, tärkeä ennakkotapaus. *Kauppalehti*, 1.

VOSS, W.G., 2013. ONE YEAR AND LOADS OF DATA LATER, WHERE ARE WE? AN UPDATE ON THE PROPOSED EUROPEAN UNION GENERAL DATA PROTECTION REGULATION. *Journal of Internet Law*, 16(10), pp. 1-24.

WILSON, C., 2014. *Chapter 2 - Semi-Structured Interviews*. Boston: Morgan Kaufmann.

ZAMUDIO, L., AGUILAR, J.A., TRIPP, C. and MISRA, S., 2017A Requirements Engineering Techniques Review in Agile Software Development Methods, *International*


*Conference on Computational Science and Its Applications* 2017, Springer, pp. 683-698.

# ANNEX A: NYMITY PRIVACY MANAGEMENT ACCOUNTABILITY FRAMEWORK

UPDATED JUNE 2018

## Nymity Privacy Management Accountability Framework™

*A Menu of Privacy Management Activities (Technical and Organizational Measures)*



innovating compliance

**1. Maintain Governance Structure**  
Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

**Privacy Management Activities**

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment
- Integrate data privacy into business risk assessments/reporting
- Maintain a Privacy Strategy
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

**2. Maintain Personal Data Inventory and Data Transfer Mechanisms**  
Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

**Privacy Management Activities**

- Maintain an inventory of personal data and/or processing activities
- Classify personal data by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain documentation of data flows (e.g. between systems, between processes, between countries)
- Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, regulator approvals)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

**3. Maintain Internal Data Privacy Policy**  
Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

**Privacy Management Activities**

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)

**4. Embed Data Privacy into Operations**  
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

**Privacy Management Activities**

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and/or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into data protection purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)

**5. Maintain Training and Awareness Program**  
Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

**Privacy Management Activities**

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training (e.g. HR, marketing, call centre)
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain qualifications for individuals responsible for data privacy, including certifications

**6. Manage Information Security Risk**  
Maintain an information security program based on legal requirements and ongoing risk assessments

**Privacy Management Activities**

- Integrate data privacy risk into security risk assessments
- Integrate data privacy into an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Maintain regular testing of data security posture
- Maintain a security certification (e.g. ISO)

**7. Manage Third-Party Risk**  
Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

**Privacy Management Activities**

- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct due diligence around the data privacy and security posture of existing vendors/processors
- Review long-term contracts for new or evolving data privacy risks

**8. Maintain Notices**  
Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

**Privacy Management Activities**

- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)

**9. Respond to Requests and Complaints from Individuals**  
Maintain effective procedures for interactions with individuals about their personal data

**Privacy Management Activities**

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Monitor and report metrics for data privacy complaints (e.g. number, root cause)

**10. Monitor for New Operational Practices**  
Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

**Privacy Management Activities**

- Integrate Privacy by Design into data processing operations
- Maintain PIA/DPIA guidelines and templates
- Conduct PIAs/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

**11. Maintain Data Privacy Breach Management Program**  
Maintain an effective data privacy incident and breach management program

**Privacy Management Activities**

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

**12. Monitor Data Handling Practices**  
Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

**Privacy Management Activities**

- Conduct self-assessments of privacy management
- Conduct Internal Audits of the privacy program (i.e. operational audit of the Privacy Office)
- Conduct ad-hoc/walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

**13. Track External Criteria**  
Track new compliance requirements, expectations, and best practices

**Privacy Management Activities**

- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes