Challenges Involved in the Implementation of the General Data Protection Regulation (GDPR) in an Information System Development Organization
An Exploratory Study

Author: Kristiina Kutserenko
Supervisors: Despina Fyntanoglou, Elissavet Kartaloglou
Examiner: Jaime Campos
Date: 2018-05-21
Course Code: 18VT - 4IK50E, 15 credits
Subject: Information Systems
Level: Master
Department of Informatics
Abstract

The General Data Protection Regulation (GDPR) is a key regulation that deals with the protection of personal data in the European Union. It will be enforced on May 25, 2018. The GDPR brings in significant changes compared to the previous Data Protection Directive 95/46/EC (DIR95). Therefore, the organizations that fall within the scope of the GDPR are required to make their information systems compliant. Due to the complexity of modern software and the magnitude of changes required for the successful adoption of the GDPR, adopting such requirements could be a challenging task.

Various works have already been conducted in the past addressing different articles and principles of the GDPR. However, relatively new Legal Technology sector has not been the focus of the GDPR related research. The purpose of the thesis is to investigate how a Legal Technology organization is affected by the challenges of implementing GDPR related requirements into its information system. In order to address the aim of the study, a literature review was conducted, followed by a case study in Assently AB, a small-sized organization belonging to the Legal Technology industry. In order to gather detailed information about the challenges of implementing the GDPR in their information system, semi-structured interviews were conducted with the practitioners at Assently.

The result of this study is a collection of challenges. This collection of challenges relates to understanding the regulation in order to implement it into information system, creating new tools and processes, reviewing existing tools and processes, human resource availability for the support, management and development of information system and facing possible customer-related issues.

The study contributes to the GDPR and Legal Technology related research. Moreover, it can be used by the industry practitioners to prepare for the similar implementations in the future. Furthermore, it will be useful for the emerging Legal Technology organizations who may need to design their information systems in compliance with the GDPR.

Keywords: case study, General Data Protection Regulation, GDPR, information systems, Legal Technology.
Acknowledgements

I would like to thank my thesis supervisors, Despina Fyntanoglou and Elissavet Kartaloglou for their feedback, help and support. Also, module leader Sarfraz Iqbal for his valuable comments related to the GDPR.

I would like to thank Assently AB for agreeing to participate in this research. Special thanks to the following interviewees and practitioners at Assently AB:

Mikael Forsgren
Shahan Khan
Jörg Rosenauer
Qambber Syed

Furthermore, I am thankful to Syed Ali Shah for sharing his knowledge in the area of the GDPR.

Last but not least, I would like to thank my parents for their constant encouragement and continuous support.
# Table of Contents

1 Introduction

1.1 Background

1.2 Previous Studies

1.3 The Research Problem and the Significance of the Study

1.4 Purpose Statement and Research Question

1.5 Topic Justification

1.6 Scope and Limitations

1.7 Thesis Organization

2 Literature Review

2.1 GDPR Implications for the Organizations

2.1.1 Staff Training

2.1.2 Consent Policy

2.1.3 Increased Rights of Data Subjects (Right of Access, Erasure (“Right to be Forgotten”), Data Portability, Rectification, Restriction, Objection, Automated Individual Decision Making, Information to be Provided)

2.1.4 Documentation and Transparency

2.1.5 Data Breaches

2.1.6 Privacy by Design and Default

2.1.7 Pseudonomisation and Encryption

2.1.8 Data Minimization Principle

2.1.9 Data Protection Officer

2.1.10 Demonstrating GDPR Compliance

2.1.11 Penalties

2.1.12 Territorial Scope

2.1.13 Reviewing Terms with Third Party Processors/systems

2.2 Challenges Identified in the Literature

2.2.1 Interpretation of Regulation

2.2.2 Ad-hoc and Generic Solutions

2.2.3 Organizational Compliance

2.2.3.1 Continuous Compliance

2.2.4 Resource Allocation

2.2.5 Documentation and Monitoring

2.2.6 Legacy Systems

2.2.7 Competing Compliance Measures

2.3 Relevance of Findings from Literature for This Study

3 Research Methodology

3.1 Methodological Tradition
3.2 Methodological Approach
3.3 Research Strategy
3.4 Research Setting
  3.4.1 Software Development Life Cycle (SDLC) of IS at Assently
3.5 Data Collection
3.6 Data Analysis
3.7 Summary of Data Collection and Data Analysis
3.8 Reliability and Validity of the Study
3.9 Ethical Considerations

4 Empirical Findings
  4.1 Empirical Findings from the Interviews
    4.1.1 Theme 1: Understanding Regulation in Order to Implement it into Information System
    4.1.2 Theme 2: Creating New Tools and Processes
    4.1.3 Theme 3: Reviewing Existing Tools and Processes
    4.1.4 Theme 4: Human Resource Availability for the Support, Management and Development of Information System
    4.1.5 Theme 5: Facing Possible Customer-Related Issues
  4.2 Overview of Empirical Findings

5 Discussion
  5.1 Discussion of the Identified Themes
    5.1.1 Theme 1: Understanding Regulation in Order to Implement it into Information System
    5.1.2 Theme 2: Creating New Tools and Processes
    5.1.3 Theme 3: Reviewing Existing Tools and Processes
    5.1.4 Theme 4: Human Resource Availability for the Support, Management and Development of Information System
    5.1.5 Theme 5: Facing Possible Customer-Related Issues
  5.2 Significance of the Study

6 Conclusion
  6.1 Conclusions
  6.2 Contribution of the Study
  6.3 Reflections
  6.4 Suggestions for Future Research

References

Appendix A1: Interview Guide for the Introduction Meeting
Appendix A2: Interview Guide (GDPR Challenges)
Appendix B: Informed Consent Form for Master Thesis
Appendix C: Codes, Categories and Concepts Identified from the GDPR Implementation Interviews

50
List of Figures
Figure 1. Data collection process.................................................................18

List of Tables
Table 1. Information about interviewees and interviews.................................16
Table 2. Themes and main findings identified from the implementation related interviews..32
**List of Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B</td>
<td>Business-to-business</td>
</tr>
<tr>
<td>DIR95</td>
<td>Directive 95/46/EC</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data protection impact assessment</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IS</td>
<td>Information System</td>
</tr>
<tr>
<td>ISA</td>
<td>Information security awareness</td>
</tr>
<tr>
<td>ISP</td>
<td>Information security policy</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software development life cycle</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background

As digitalization is rapidly becoming a part of most industries, various laws, both international and regional, and conventions are required in order to protect the fundamental rights of individuals (Kabanov, 2016). Some of the core values of the democratic societies and their individuals involve information privacy and data protection of the users (Danezis et al., 2015). European Union (EU) member states have been trying to address the issue of information privacy and data protection of its individuals for quite some time. The efforts have been driven by the need of the citizens across EU member states. Hence with regards to such needs, on 27th April 2016, Regulation (EU) 2016/679 was passed (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016). The regulation is commonly referred to as General Data Protection Regulation (GDPR). The regulation is to be enforced from 25th of May, 2018 (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016).

The new regulation is replacing Data Protection Directive 95/46/EC (DIR95), which has previously been a central legislative instrument for personal data protection in the EU (Tikkinen-Piri, Rohunen and Markkula, 2017). The GDPR applies to all organizations, that process personal information connected with the EU citizens (Tankard, 2016). It also expands the definition of personal data and the rights of data subjects and introduces the requirement for breach notifications within a certain timeframe, as well as the need to appoint a Data Protection Officer in certain cases. (Tankard, 2016). The regulation comprises of several key features, such as accountability of processes involved in data handling, user consent and privacy by design, related to data protection.

The GDPR defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’)” (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 4 (1)). Two important definitions are also those of “controller” and “processor”. The former is defined as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data ” (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 4 (7)) and the latter as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 4 (8)).

For years, organizations have been processing their users’ data for various reasons. In the absence of any concrete regulation, different practices to process user data have been used. As the organizations have been moving increasingly towards globally distributed environments, the user data processing has become increasingly complex. With the upcoming enforcement of the GDPR, there is a huge risk of organizations getting heavily fined for their noncompliance (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016). The impact of such fines along with the bad publicity in the media can be huge for organizations of all sizes. With the complexity of software being developed in globally distributed environment, the implementation of such regulation in information systems can be a cumbersome and a daunting task. As the GDPR enforcement day comes closer, organizations are already struggling with many implementation challenges (for example, connected with the use of Big Data analytics and related technologies in organizations (Preuveneers, Joosen and Ilie-Zudor, 2016), complexity of personal data, agility and consistency and availability of experts (Kabanov, 2016), data process changes (Wipp Ekman and Billgren, 2017)). Performing
changes to accommodate GDPR requirements in complex software or information systems (IS) may be a difficult or challenging task. Before proceeding further, it is important to understand the context of the word “challenge” in relation to this thesis.

Oxford dictionaries (n.d.) define the word “challenge” as following:

"A task or situation that tests someone's abilities."

In order to avoid deviating from the scope of the study I derive my definition of the word “challenge” from Oxford dictionaries, as following:

Challenge is a task or situation that test an individual’s or a team’s ability by requiring additional effort or cost than the usual way of working.

One industry sector which may face challenges in the implementation of the GDPR in its IS, is the Legal Technology sector.

Due to the nature of business of law firms, creation of new or innovative service models that produce efficiencies is not their priority (CEB Leadership Council for Legal Executives White Paper, 2017). Contrary to this, alternative legal providers can focus on and add value to specific services, which allows to optimize the processes by using technology and allows lawyers to concentrate on their core business, instead of non-legal work (CEB Leadership Council for Legal Executives White Paper, 2017). Such technology that supports legal, or law related, business is referred to as Legal Technology, or Legal Tech in short.

Praduroux, de Paiva and di Caro (2016) provide a definition of Legal Technology:

“Legal Tech, like its older and more substantial ‘brother’ FinTech (Financial Technology) covers companies (mostly startups) utilising technology to build products solving problems faced both by the legal industry (i.e. law firms, corporates etc.) and consumers of legal services.”

There are several categories of services that Legal Tech may offer. Some of them are as following (Praduroux, de Paiva and di Caro, 2016):

- Document automation and assembly: set of services that assist in creating electronic work flows in the creation of electronic documents as well as services for document archiving.
- Predictive analytics and litigation data mining: category of services that help to perform analysis of data through statistical and mathematical models, which in turn helps in better decision making.

For the purpose of the current thesis, Legal Tech organizations are defined as:

Organizations that provide software based services for solving various legal problems.

This study aims to investigate the challenges faced by a Legal Technology organization in their effort to implement GDPR in its IS.

1.2 Previous Studies

A number of studies were conducted about data privacy and supporting regulations. Polański (2017) argues that research dedicated to international law should also include cyberspace, as this is where the increasing amount of international relations is taking place. Drewer and
Miladinova (2017) address the need to process large quantities of information under Europol regulation. Berg-Larsen (2015, p.4) conducts a qualitative study consisting of interviews and analysis or documents and demonstrates “how the introduction of data protection can be seen as a way of handling the unintended consequences of technological progress within ICT, and how the GDPR is an attempt at managing technology and mitigating risks”.

Various papers are dedicated to the issue of information system compliance. Becker et al. (2014) propose generally applicable meta-design that can be used in order to integrate regulations into information systems design and implementation. Bulgurcu, Cavusoglu and Benbasat (2010, p.523) identify “the antecedents of employee compliance with the information security policy (ISP) of an organization” and state that “employee’s attitude is influenced by benefit of compliance, cost of compliance, and cost of noncompliance”.

Butin and Métayer (2015) have systematically analyzed the requirements of personal data life cycle and have presented guidelines for the implementation of accountability measures in organizations. Some studies explored the principle of privacy by design, for example, Colesky and Ghanavati (2016) explored the changes in the GDPR and evaluated its impact on EU-US Privacy Shield agreement. This study provides recommendations for attaining near-compliance with privacy by design as part of an organization’s default modus operandi.

Smart products are uniquely identifiable by the organizations and many times user data is shared with third parties. Smart products make use of big data analytics or require persistence of large data quantity. In the study by Preuveneers, Joosen and Ilie-Zudor (2016) the impact of the GDPR in context-aware intelligent environments has been explored and guidelines have been suggested that may be used in order to address the challenges faced due to the prevalent use of Big Data analytics and related technologies in organizations. Several challenges and the strategies to address them have been explored by the study.

Hoel, Griffiths and Chen (2017) make a comparison of different data privacy frameworks, it helps to raise the question regarding how organizations outside of the EU will deal with the impact of the GDPR, while still complying with their region’s own data privacy framework. On the other hand the impact of the GDPR in cloud based environment and in e-health domain has been covered by another study (Ducato, 2016). The author describes the main GDPR innovations concerning data protection in the context of cloud environment and critically addresses the main open issues.

In the study by Kabanov (2016) the challenges related to complexity of personal data, agility and consistency and challenge of availability of experts have been explored. The project team of the same study developed a general framework that may enable organizations to address the stated challenges.

Bitar and Jakobsson (2017) looked at some of the GDPR requirements and investigated the possibility of using hardware security modules in order to reach compliance. Further, they conducted an empirical study in order to see the areas that organizations have to concentrate on in order to be compliant with the GDPR.

Tikkinen-Piri, Rohunen and Markkula (2017) analyzed the differences between the GDPR and DIR95 and identified practical implications of the GDPR. Moreover, the authors emphasized the need of future empirical studies among data intensive companies in order to see how these companies adapt to the new regulation. Furthermore, according to the authors, a study concentrating on how organizations of different sizes implement the GDPR and address its challenges will be beneficial. Such empirical research will help to collect and analyze the
approaches and solutions for implementing the changes, as well as field-specific practices of data usage and management (Tikkinen-Piri, Rohunen and Markkula, 2017).

In addition to that, a comprehensive study has been conducted (Wipp Ekman and Billgren, 2017), which explored GDPR-related challenges in different organizations. Firstly, the study has gathered several challenges connected with data process changes in general. After that, the authors conducted interviews in several organizations with personnel working in such positions as security, product and project management and identified seven challenges and one sub-challenge connected with data processing that organizations face when adjusting to the GDPR. However, the study itself notes that challenges need to be explored in specific industry domains, as different domains might face different challenges (Wipp Ekman and Billgren, 2017). Hence, there is still a need to explore specific industry domain related challenges.

1.3 The Research Problem and the Significance of the Study

Various works have already been conducted in the past addressing different articles and principles of the GDPR. A study that concerns the difficulties faced by certain industries would, however, be beneficial for the research community, industry practitioners as well as new start-up organizations. Each type of industry sector can face different types of challenges and such challenges might need to be addressed differently (Kabanov, 2016; Bitar and Jakobsson, 2017). The relatively new and rapidly developing Legal Technology sector (Rubin, 2014) in particular has not been covered by any of the previous studies.

1.4 Purpose Statement and Research Question

The purpose of the thesis is to investigate how Legal Technology organizations are affected by difficulties or extra effort that these organizations need to make in order to implement GDPR-related changes in their IS. As not all of the challenges can be experienced during their implementation, the purpose of this thesis is also to gather expected challenges of GDPR implementation as perceived by organization personnel. This will be done by conducting a case study in a small-sized Legal Technology organization, situated in Stockholm County, Sweden. An interpretivist qualitative approach will be used for the current thesis. The focus of the study will be on the perceptions of the Legal Technology organization employees. Hence, implementation challenges, as well as expected challenges will be analyzed from the perspective of the organization’s personnel.

The research problem can be summarized as the following research question:

RQ: How is a Legal Technology organization affected by the challenges of the GDPR implementation in its information systems?

1.5 Topic Justification

GDPR adoption can create difficulties for many organizations that process personal data of EU nationals. Therefore, research dedicated to various challenges faced by organizations is necessary in order to create better understanding of the potential issues that should be kept in mind by the industry practitioners.

Legal technology, or the technology and software used for providing legal services, is a rapidly growing industry (Rubin, 2014). This industry can require various types of private user data. Hence, it is important that a study is conducted to explore the challenges as faced by the Legal Technology sector. This study can then be used as a tool to address the challenges in a pragmatic way. Furthermore, emerging Legal Technology organizations can also benefit from this study, as these organizations will have to design their IS in compliance with the GDPR.
1.6 Scope and Limitations

The scope of this study is to understand the perceptions of the Legal Technology organization employees about the challenges they experienced or the challenges they expect in future when adopting the GDPR. A literature review combined with interviews will be used for this purpose. The interviews will be conducted with employees occupying roles such as developers and product manager.

Systematic literature review was not conducted; therefore, it is possible that some articles might have been missed. Only literature in English language was used, hence, the material in foreign languages was not reviewed.

The scope of the thesis contains only the management, usage, support and development of information systems, hence, challenges arising in other areas, for example, management of the organization or its employees, are not covered. Finally, as the case study organization is small (employing less than 25 people), the challenges might differ for the organizations in the similar industry, yet of different size.

1.7 Thesis Organization

Current thesis contains six chapters. Chapter one provides a short description of the GDPR, presents previous studies and introduces the research problem and the purpose of the thesis. Chapter two contains literature review and presents practical aspects and implementation challenges of the GDPR that were found in the literature. Chapter three provides information on the research setting and describes the methodology of the research, namely paradigm, methodological approach, research strategy and methods of collecting and analyzing data. Additionally, the chapter defines the ways of ensuring reliability and validity of the study and describes ethical considerations.

The empirical findings are presented in chapter four. The chapter describes the themes identified after the analysis of raw data from the interviews. Chapter five contains discussion of identified themes and describes significance of the study.

The thesis concludes with chapter six, where the findings of the thesis are summarized and contribution of the study is presented. Additionally, this chapter contains reflections of the researcher and suggestions for future research.
2 Literature Review

2.1 GDPR Implications for the Organizations

This subchapter summarizes the GDPR aspects and implications as identified in the literature that can pose certain implementation challenges for the organizations.

2.1.1 Staff Training

In their study on information security policy compliance, Bulgurcu, Cavusoglu and Benbasat (2010, p.542) state the following: “creating a security-aware culture within the organization will improve information security. Therefore, we suggest that organizations create appropriate training and security awareness programs that ensure employees’ ISA (information security awareness), as well as their self-efficacy about compliance”. Furthermore, according to Tikkinen-Piri, Rohunen and Markkula (2017), the lack of understanding and awareness from the organizations’ side poses a great challenge in the GDPR adoption. GDPR implementation means various implications for the organizations in information systems design, practices and processes, new responsibilities and corresponding training for the employees, which requires the organizations to review and possibly create new data protection and privacy practices (Tikkinen-Piri, Rohunen and Markkula, 2017). The employees should get the understanding about their responsibilities in regards to data processing (Cooper et al., 2017). It is not enough for the organizations just to adopt the GDPR, the employers also need to provide sufficient training to ensure the awareness among the employees and secure continuous adherence to the new practices (Cooper et al., 2017). In addition to that, multinational organizations should be aware of the possible country-specific consultation and information requirements with employee representatives (Cooper et al., 2017).

2.1.2 Consent Policy

Article 6 of the GDPR describes lawful bases for personal data processing (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016). In case the processing is based on consent, organizations “will be required to be able to demonstrate that such consent was given” (Gilbert, 2016, p. 6). GDPR stipulates that data subjects must give their clear, voluntary and informed consent for their data to be processed by the organization (Tankard, 2016). Meeting the consent-related requirements was identified as challenging by Wipp Ekman and Billgren (2017). Tikkinen-Piri, Rohunen and Markkula (2017) mention that getting a consent, that is separated from all the other information provided to the data subject, can mean implementation of a consent management system and additional costs related to it for organizations. Organizations might need to establish processes and systems for obtaining, recording and withdrawal of consent (Tikkinen-Piri, Rohunen and Markkula, 2017). The authors also mention that verifying the ages of data subjects and getting consent from parents or custodians can pose challenges for online companies (Tikkinen-Piri, Rohunen and Markkula, 2017). Cooper et al. (2017) note the possibility for the organizations to limit their reliance on consent, in case there is an alternative legal reason for information processing.

2.1.3 Increased Rights of Data Subjects (Right of Access, Erasure (“Right to be Forgotten”), Data Portability, Rectification, Restriction, Objection, Automated Individual Decision Making, Information to be Provided)

Under the GDPR, data subjects have the right to get the access to the information that the organization holds on them, they can also demand from organizations to delete data related to them (Tankard, 2016) or receive this data in an electronic format (Tikkinen-Piri, Rohunen and Markkula, 2017). Similarly to the consent, the reliance on such rights (especially, the right to
be forgotten), can be limited if there is an alternative legal reason for processing the data (Cooper et al., 2017). Wipp Ekman and Billgren (2017) mention these requirements as the potential areas where the implementation challenges may arise. Tikkinen-Piri, Rohunen and Markkula (2017) note that in order to address the data subject’s right of access, the information systems should be designed in the way that allows these requests to be made electronically. Ensuring the right to be forgotten requires the organizations to ensure they have the technical solutions and processes for data deletion within specific time, as well as informing third parties of such requests when necessary (Tikkinen-Piri, Rohunen and Markkula, 2017). Moreover, adequate documentation is crucial in order to establish what data is stored, where it is stored and who it is shared with (Tikkinen-Piri, Rohunen and Markkula, 2017). One of the difficulties connected with data portability in the absence of the uniform transmission standards is considering the format when exporting the data (Tikkinen-Piri, Rohunen and Markkula, 2017). In addition to that, organizations should keep in mind that the data, which is to be transmitted, can also be related to other data subjects, therefore, it is important that the privacy of these related data subjects is not compromised; one way of achieving this is providing adequate training to the employees (Tikkinen-Piri, Rohunen and Markkula, 2017).

The GDPR secures (similarly to DIR95) and specifies data subjects’ rights to rectification and restriction (Tikkinen-Piri, Rohunen and Markkula, 2017). Furthermore, new requirements for providing additional information to data subjects are stated (Tikkinen-Piri, Rohunen and Markkula, 2017).

Article 21 specifies data subjects’ right to object to processing of their personal data (Tikkinen-Piri, Rohunen and Markkula, 2017). Moreover, according to article 22, data subjects have the right not to be subject to measures that are based on automated decision-making processes (Tikkinen-Piri, Rohunen and Markkula, 2017). Hence, organizations need to identify and understand such processes and consider human decision-making alternatives when possible (Cooper et al., 2017).

2.1.4 Documentation and Transparency

Wipp Ekman and Billgren (2017) note that in preparation for the GDPR many organizations are working on making their systems more transparent. The importance of maintaining documentation is mentioned as one of the GDPR implications by Tikkinen-Piri, Rohunen and Markkula (2017), who note that the two main types of documentation, that organizations have to maintain under the GDPR, are a record of personal data processing activities and a data protection impact assessment. The requirement of maintaining a record of processing activities does not apply to organizations that employ less than 250 people, “unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10” (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 30 (5)). Maintaining GDPR-related documentation can be especially challenging for personal data intensive organizations that employ working principles with little documentation, such as agile and lean (Tikkinen-Piri, Rohunen and Markkula, 2017).

2.1.5 Data Breaches

In the event of data breach, relevant authorities and, in case of high risk, data subjects have to be notified without undue delay (Gilbert, 2016). In order to be compliant, organizations must establish processes that ensure quick reaction in case of personal data breaches (Tikkinen-Piri, Rohunen and Markkula, 2017). Furthermore, organizations must be prepared to be able to quickly contact the authorities, and, what can be especially challenging, data subjects
The requirement to notify data subjects will not be effective if the data is sufficiently protected, hence it is important for the organizations to consider data security methods, such as encryption (Tikkinen-Piri, Rohunen and Markkula, 2017). Wipp Ekman and Billgren (2017) established that requirements connected with data breaches are seen as challenging by the industry practitioners and that organizations need to introduce changes in order to fulfill the requirement of reporting to both the customers and the authorities.

2.1.6 Privacy by Design and Default

The concept of privacy by default and design is one of the new principles introduced by the GDPR (Tikkinen-Piri, Rohunen and Markkula, 2017). Put into practice, this means “that data protection and privacy must be considered right from the beginning of the security planning process” (Tankard, 2016, p. 6). It is important that organizations review, assess and possibly implement new privacy protection measures to be compliant with this obligation (Tikkinen-Piri, Rohunen and Markkula, 2017). Meeting this requirement can be challenging for the organizations, for example, due to legacy processes (Wipp Ekman and Billgren, 2017).

2.1.7 Pseudonomisation and Encryption

Encryption, along with pseudonomisation, is seen as an appropriate measure for ensuring data security (Tankard, 2016). Organizations that encrypt data are not required to notify data subjects about data breaches (Tankard, 2016; Tikkinen-Piri, Rohunen and Markkula, 2017). These two measures can also be used for demonstrating compliance with the GDPR (Tikkinen-Piri, Rohunen and Markkula, 2017). Wipp Ekman and Billgren (2017) establish that encryption can be risky, as there is a danger of potential data loss.

2.1.8 Data Minimization Principle

Data minimization principle under the GDPR means that personal data collected by the organizations should be “limited to what is necessary in relation to the purposes for which they are processed” (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 5 (c)). This means that organizations need to specify what data they need and for what purposes, as collecting excessive data is not allowed; moreover, every purpose requires a separate consent from the data subject (Tikkinen-Piri, Rohunen and Markkula, 2017). Special attention must be drawn to collecting data about children, due to the requirement to verify the age of data subjects and getting the consent of parents or custodians if necessary (Tikkinen-Piri, Rohunen and Markkula, 2017). This GDPR aspect will heavily affect, among others, the organizations who profile customers for the purpose of marketing (Tikkinen-Piri, Rohunen and Markkula, 2017). Wipp Ekman and Billgren (2017) establish that data minimization principle can be difficult for organizations, as this is a new approach to data collection in comparison with the previous practices of collecting data at all times in case there is a need for it in the future.

2.1.9 Data Protection Officer

Organizations have to designate a Data Protection Officer (DPO) if they are public authorities or bodies (except for courts “acting in their judicial capacity”), if their core activities require “regular and systematic monitoring of data subjects on a large scale” or they process “special categories of data” or “personal data relating to criminal convictions and offences” on a large scale (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 37 (1)). A DPO can, in some cases, be shared among several organizations (Tankard, 2016). As the DPO will be responsible for data protection and coordination with supervisory authorities, it is important that this person has a good understanding of both the organization and the law.
Appointing a DPO can be challenging, as there might be a lack of expertise in organizations and lack of relevant qualifications on the market (Tikkinen-Piri, Rohunen and Markkula, 2017). Several industry practitioners mentioned that a DPO should have the knowledge both about the legal aspects and the processes (Wipp Ekman and Billgren, 2017).

### 2.1.10 Demonstrating GDPR Compliance

The concept of accountability, introduced by the GDPR, means that data controllers are responsible for demonstrating compliance with the GDPR principles of personal data processing (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. (5); Tikkinen-Piri, Rohunen and Markkula, 2017). Butin and Métayer (2015) state that effective implementation of accountability is not an easy task. It needs a systematic approach and affects IT systems.

In addition to that, the GDPR promotes codes of conducts and such voluntary means as data protection certification mechanisms, seals and marks (Tikkinen-Piri, Rohunen and Markkula, 2017).

### 2.1.11 Penalties

According to the GDPR, organizations can be penalized for breaches. This applies to both data processors and controllers (Tikkinen-Piri, Rohunen and Markkula, 2017). For example, organizations can receive an administrative fine of up to 20 000 000 euro or 4 % “of the total worldwide annual turnover of the preceding financial year, whichever is higher” as the largest penalty for non-compliance (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016, art. 83). Organizations have to review their policies and processes in order to be compliant and also keep these penalties in mind when developing new processes (Tikkinen-Piri, Rohunen and Markkula, 2017). Wipp Ekman and Billgren (2017) established that penalties could create dilemmas for organizations, for example, when creating contracts with customers, who started to transfer as much responsibility as possible to data processors.

### 2.1.12 Territorial Scope

The scope of data protection under the GDPR is expanded and any organization that has to collect or process data connected with the EU citizens, no matter where the organization or data is located, has to be compliant with it (Tankard, 2016). In addition to that, the GDPR introduces new requirements for transfers of personal data to third countries and international organizations (Tikkinen-Piri, Rohunen and Markkula, 2017). The conditions for such transfers, applicable for both data processors and controllers, include the adequacy decision, which was already included in DIR95, and appropriate safeguards, which are new (Tikkinen-Piri, Rohunen and Markkula, 2017). Hence, organizations need to review their international data transfers, make decisions about how and what data will be transferred and processed and evaluate whether additional safeguards are needed (Tikkinen-Piri, Rohunen and Markkula, 2017). The challenges can also arise if the cloud services or their backups are stored outside of the EU (Wipp Ekman and Billgren, 2017).

### 2.1.13 Reviewing Terms with Third Party Processors/systems

Organizations need to review their contracts with third-party processors to make sure they comply with the increased GDPR requirements (Cooper et al., 2017).
2.2 Challenges Identified in the Literature

According to Wipp Ekman and Billgren (2017), the compliance challenges can be categorized in the following way.

2.2.1 Interpretation of Regulation

The category of interpretation of regulation deals with how organizations can understand and interpret the given requirement and break it down into manageable and implementable work tasks or requirements.

2.2.2 Ad-hoc and Generic Solutions

These are the challenges that focus on the difficulty of taking decisions between redesigning the generic compliance solutions and implementing ad-hoc changes targeting specific data processes. Both of these two approaches have different costs of implementation (in terms of human effort, tools used, time to market etc.) and the delivered value.

2.2.3 Organizational Compliance

These are the challenges that arise in connection with the management of human resources and the way they deal with the data processes. One example of such challenge can be how the team members handle the test data provided by the end-customers.

2.2.3.1 Continuous Compliance

This is sub-category of organization compliance. While the parent category deals with becoming compliant one time, this sub-category focuses on being continuously compliant.

2.2.4 Resource Allocation

Resource allocation challenges are related to the distribution of resources that are needed to make an information system compliant with the regulation.

2.2.5 Documentation and Monitoring

The challenges related to the understanding of the organization’s systems and providing documentation of various processes, that are involved in making the system GDPR compliant, to the relevant authorities.

2.2.6 Legacy Systems

Legacy systems are any systems that were developed by the members of an organization, yet over time, the techniques used to develop it have became outdated or the team members who developed it have either left their positions or the organization. (Bennett, 1995). The system may continue to be useful and working but modifying it can be big task (Bennett, 1995). These challenges arise due to the difficulties connected with modification of legacy systems.

2.2.7 Competing Compliance Measures

These challenges are related to the difficulty of making a system compliant while continuing to be compliant with any other regulations that the system adheres to. It can happen that two or more regulations may contradict each other.

2.3 Relevance of Findings from Literature for This Study

As stated in section 1.5, the Legal Technology organizations are an emerging industry domain. Being a technology and data processing domain, it is highly likely that the Legal Technology industry faces similar challenges as stated in the literature. Already, as shown from the literature review conducted in this study, various challenges are being faced by the industry in
its effort to become GDPR compliant. Hence, the findings from the literature review provide building blocks for this study.

Different aspects of the GDPR and challenges of the GDPR compliance from the literature review helped in creating the GDPR specific interview questions for this study. Further details related to interview design are stated in the next section.

The findings from the literature review also helped in identifying challenges, which are specific to small sized, Legal Technology organizations.
3 Research Methodology

3.1 Methodological Tradition

Both qualitative and quantitative research are based on the set of assumptions about what constitutes acceptable research and which research methods should be employed (Myers, 1997, Orlikowski and Baroudi, 1991).

Orlikowski and Baroudi (1991) and Myers (1997) distinguish between three philosophical traditions for studying the information systems: positivist, interpretive and critical research.

Positivist studies aim to increase predictive understanding of a phenomenon by testing theory (Orlikowski and Baroudi, 1991). The reality is seen as something which is a given and can be described by measurable properties independent of researchers and their tools (Myers, 1997).

Interpretive studies try to understand a phenomenon by accessing the meaning that is assigned to it by participants (Orlikowski and Baroudi, 1991). Interpretivist researchers assume that access to reality is possible through various social constructions, for example, consciousness, language and shared meanings (Myers, 1997).

The aim of critical research is to critique the social status quo and transform restrictive social conditions (Orlikowski and Baroudi, 1991, Myers, 1997). Critical researchers believe that social reality is established historically and that people produce and reproduce it (Myers, 1997).

The purpose of the current research was to investigate the challenges of the GDPR implementation in the IS of a particular organization from the perspective of its employees. For this reason, interpretive paradigm was employed for the current study, as it has the aim of understanding phenomena through meanings assigned to them by individuals (Orlikowski and Baroudi, 1991) and employs the assumption that the reality can be accessed through social constructions (Myers, 1997). The participants’ opinions and beliefs about the challenges of the GDPR implementation were analyzed through interpretive paradigm.

3.2 Methodological Approach

Myers (1997) states that the most common distinction done in the research methodology is between quantitative and qualitative research. Quantitative research methods were originally developed in order to study natural phenomena in the natural sciences (Myers, 1997). Such methods are suitable for testing theories by analyzing the relationship between variables, that are measured in order to produce numbered data (Creswell, 2008). Using quantifiable variables and hypothesis testing is generally applicable for the positivist paradigm (Orlikowski and Baroudi, 1991).

Qualitative methods were originally created in the social sciences. They allow researchers to explore cultural and social phenomena (Myers, 1997). Such research methods allow to study and understand the meaning given to a problem by individuals or groups (Creswell, 2008). Researcher in this case interprets the meaning of the data and the data collection usually takes place in the participants’ setting (Creswell, 2008).

The purpose of the current thesis was to interpret the challenges of the GDPR implementation from the perspective of individuals, who work in a particular organization, and understand the meaning given to this issue by the participants. The collection of the data for the research took place in the participants’ setting. Therefore, qualitative research methods were chosen as the most suitable for the current research.
3.3 Research Strategy

For the purpose of the current thesis, a case study was conducted, which helped in acquiring the industry practitioners’ perceptions. With regards to the current research, a case study can be described as a research strategy, where a researcher conducts an in-depth analysis of a process or activity (Creswell, 2008).

According to Yin (2014), a case study should be preferred when 1) dealing with “how” and “why” research questions; 2) researcher has no or little control over the events that are being investigated; 3) the research is focused on a contemporary phenomenon.

Current research was dedicated to the challenges of the GDPR implementation, which is a contemporary phenomenon. The researcher in this case had no control over the implementation and was interested in the perceptions of the organization’s employees. Hence, a case study was deemed a suitable research strategy for the current thesis.

Klein and Myers (1999) write that similarly to the classification of the three research paradigms, case studies can be divided into positivist, interpretivist and critical. Interpretive case studies attempt “to understand phenomena through the participants’ interpretation of their context” (Runeson and Höst, 2008, p. 135). The purpose of the interpretive case study employed in the current research was to understand the challenges of the GDPR adoption through the interpretations given by the employees of the Legal Technology organization.

According to Baxter and Jack (2008), the choice of the case study type should be motivated by the purpose of the study. Current case study can be classified as exploratory, according to Yin (2014), since its purpose was to explore a situation of the GDPR implementation in a Legal Technology organization. In addition to that, Baxter and Jack (2008, p. 549) state that single case study can be considered when looking at a phenomenon “in one environment because it is a unique or extreme situation”. This research can be considered a single case study, as the GDPR implementation challenges were being looked at in one environment and it was a unique situation attributable to a particular Legal Technology sector organization.

3.4 Research Setting

The case study was conducted in the organization Assently AB (referred to as Assently further in this study) that is situated in Stockholm, Sweden. The organization belongs to the Legal Technology industry. Below is the information about Assently and the solutions and services it offers.

Assently’s services are used by different organizations, which are referred to as "Customers". The customers of these organizations are referred to as "End-customers".

Assently has 17 employees and has roles in such areas as management, sales, support, software development and marketing. The main office is situated in Stockholm, Sweden. Additionally, a partner office that has three employees is located in Finland.

The organization maintains stringent security mechanisms for user data protection and utilizes state-of-the-art tools for its Information System (IS) security and error monitoring.

The organization offers the following solutions:

**Assently E-Sign** is a solution for signing documents and forms. The idea behind E-Sign was to find a way to digitize e-signature flow. In the past, only the beginning of the process (drafting of the document) was digital, however, later it had to be printed and signed and possibly scanned and archived again. With the E-Sign solution, the organization aimed to bridge that
gap and create the process that was digital end-to-end. E-Sign is a flexible product that provides both turnkey solutions and integrations: customers can either use turnkey solutions by signing up and using Web Office to build documents, set up document flows and manage e-signatures or build the solution into their systems. Additionally, this solution offers a validation mechanism.

Assently E-sign solution includes archiving of documents. The information is stored on Assently’s own servers.

Assently E-Sign offers various forms of digital signature methods. These signature methods may differ among different countries. For example, touch and SMS-based signatures are offered by Assently E-Sign worldwide, whereas electronic ID-based signatures are offered for the four Nordic countries.

**Point of Sale** and **LiveID** are two products under E-Sign. The former allows the customers to sign documents directly in store on a touch screen device and the latter allows the identification of a user with BankID during a phone call.

**Assently CoreID** is a way for organizations to integrate electronic ID into their own products or websites and identify a user. In this case, only identity proof is created and sent to customers, Assently does not store any personal information. The customers can decide if they should store the information in their systems or not.

Assently provides B2B solutions to various organizations within Nordic countries and the European Union. It is, however, possible that these Customers have End-customers outside of the EU. For its Customers, Assently acts as data processor. It has processing agreements with all its Customers. End-customers, who want to have their data deleted, have to contact Customers for this purpose. In order to handle personal data, Assently has a personal data inventory, which is currently being updated.

The E-Signed document also contains an embedded audit log. In addition to that, for debugging purposes and troubleshooting, technical logs are saved for a limited period. Personal data related to customers is contained only in the audit logs.

On the other hand, CoreID solution does not employ any tracking of customer actions. However, only for billing purposes limited logging is maintained. No personal data is logged in CoreID solution.

### 3.4.1 Software Development Life Cycle (SDLC) of IS at Assently

Business requirements can come either from within the organization or from the Customers. New requirements undergo a triage process, where prioritization of requirements is performed. The requirements are later groomed, documented in organization’s own systems. The documented tasks are added to the external task management system. The information stored in this system can only be seen by the employees of Assently. No customer data is saved there.

In the task management system, requirements are placed in a digital Kanban priority board where they are assigned to developers. Usually, product manager, developers, personnel working with sales and possibly management are included at this point. Personal data is not used at this stage. Requirements stage is followed by design, development and testing stages, where developers and project and product manager are included.

For internal testing, mock data is used. Apart from the production environment, Customers are also allowed to access and perform their testing in Assently’s staging environment. The name of the organization and username, name and e-mail of Customers are saved in this case. The
Customers are requested to avoid using data containing sensitive information for this purpose. However, sometimes Customers add sensitive data in staging environment.

According to information security policy of Assently, test data is not allowed to be saved on the personal computers of company employees. However, during testing, test data (mostly mock data) can be saved on the employees’ personal computers for a short time, but Assently has processes for the secure deletion of this data.

After the deployment of the product, automatic integration and manual tests are performed. In the former case, no personal data is used. In case of manual testing, only Assently employees’ data is saved.

Employees in the leading roles, developer team and support team can have access to customer data (for example, if a customer would like them to look at the specific document in their account as part of customer support). Customer support is provided via e-mail and phone. An external ticketing tool is used by the organization for this purpose. A support team works with the support tickets; however, if the issue needs technical assistance, the first line support transfers it to the development team. Support ticket information, including customer data, can only be accessed by the employees of Assently and the Customers who report these issues.

3.5 Data Collection

For the purpose of the case study, an introduction interview was conducted in order to understand the organization, its products and process flow. The interview was complemented with the information available from the Assently’s public website, https://assently.com/, and the documents that were demonstrated to the researcher after the initial interview. Firstly, a personal data inventory was shown to the researcher. Additionally, documents summarizing data flows within two main products of the organization – E-Sign and CoreID – were demonstrated. These documents were helpful for the understanding of the products and the ways of working within the organization.

As a next step, semi-structured interviews were conducted. Face-to-face conversations were held with interviewees and, with their permission, recorded on a mobile device. The employees, who work with the GDPR implementation and occupy such roles as product manager and developers, were chosen for the interviews.

According to Walsham (2006), one of the ways to analyze qualitative data is by using theory. Furthermore, Qu and Dumay (2011) state that in order to ask relevant questions during interviews and in turn collect the valuable information, researchers need to get as much knowledge about the research topic as possible. For this reason, the GDPR-related challenges and implications, as identified in the literature, were thoroughly investigated. In order to get a better understanding of the information system used by the organization and to formulate the interview design accordingly, the product manager was requested to describe the business and the information system in detail during the first meeting. After that, the subsequent interviews were conducted. The researcher was acting as a “neutral” observer, meaning that industry practitioners did not see the researcher as having strong prior opinions due to previous work in the organization (Walsham, 2006, p. 321).

Semi-structured interviews were chosen because, according to Qu and Dumay (2011, p. 216), they are “flexible, accessible and intelligible and, more important, capable of disclosing important and often hidden facets of human and organizational behavior”. Semi-structured interviews allowed the interviewees to answer questions by employing their way of thinking and their language use (Qu and Dumay, 2011).
The interview guides are included as Appendices A1 and A2. The introduction meeting guide contains general questions on the organization, the services it offers and its software development life cycle (SDLC). The questions in the second interview guide were designed based on the findings from the literature. They contain both general questions on the GDPR challenges and questions that are more detailed. Some of the questions follow the interview guide in (Wipp Ekman and Billgren, 2017).

Table 1 contains the characteristics of the interviewees, as well as the date and duration of the interviews. The interviewees were assigned codes IN1-IN4. As previously mentioned, the roles were selected, as they were involved in the development, management and maintenance of IS. The role of support team could not be used due to time and availability issues.

<table>
<thead>
<tr>
<th>Role in the organization</th>
<th>Interview date</th>
<th>Type of the interview</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product manager</td>
<td>04 April 2018</td>
<td>Introduction</td>
<td>IN1</td>
</tr>
<tr>
<td>Product manager</td>
<td>26 April 2018</td>
<td>Implementation challenges</td>
<td>IN1</td>
</tr>
<tr>
<td>Software engineer</td>
<td>11 April 2018</td>
<td>Implementation challenges</td>
<td>IN2</td>
</tr>
<tr>
<td>Software engineer</td>
<td>15 April 2018</td>
<td>Implementation challenges</td>
<td>IN3</td>
</tr>
<tr>
<td>Development team lead</td>
<td>16 April 2018</td>
<td>Implementation challenges</td>
<td>IN4</td>
</tr>
</tbody>
</table>

3.6 Data Analysis

Conducting data analysis is about following a certain process and making interpretations based on it (Lichtman, 2010). For the purpose of the current thesis, the raw data was transformed into information useful for the research by applying the three Cs approach suggested by Lichtman (2010, p. 251): coding, categorizing, concepts. In order to analyze the data derived from the interviews, the six steps stated by Lichtman (2010) were used. This iterative process is applicable for qualitative data analysis “by coding and looking for central concepts or themes”:

1) initial coding – interview transcripts were read carefully and codes (words or phrases) were assigned;

2) revisiting initial coding – assigned codes were reviewed, terms clarified, possible synonyms renamed;

3) developing an initial list of categories – codes were grouped into categories, which were later organized under a main topic;

4) modifying initial list based on initial rereading – the list of categories was revisited and categories were combined if necessary;

5) revisiting categories and subcategories – the categories were critically reviewed to ensure that they are important for the research;

6) moving from categories to concepts – the key concepts were identified and organized in a logical way (Lichtman, 2010, pp. 252-256).
3.7 Summary of Data Collection and Data Analysis

Figure 1 shows the summary of the data collection and data analysis process that was conducted in this study. A summary of data collection process is stated briefly in this section.

Firstly, the literature review was conducted where different aspects and challenges of implementation of the GDPR were identified. Some findings of such challenges and aspects were used to design introduction interview that was conducted with the product manager of Assently. During the introduction interview, the product manager also showed some data flow documents and personal data inventory that were helpful in understanding the products, complete data process and data flow in the IS and the ways of working within the organization. The data was also complemented with the public data that is available on Assently’s public website.

The findings from the literature review coupled with the findings from the introduction interview, documents and public data from Assently also helped in designing GDPR-specific interview. After the design of the GDPR-specific interview, interviews were conducted with employees of Assently that were available and had worked with GDPR related requirements in IS. After the GDPR-specific interviews, data analysis was performed by using Lichtman’s (2010) approach on interview data.
3.8 Reliability and Validity of the Study

In order to ensure the trustworthiness of the study, the constructs stated in (Shenton, 2004, p. 64) were addressed:

1) Credibility
2) Transferability
3) Dependability
4) Confirmability
Credibility means that researchers ensure the correct recording of the phenomenon (Shenton, 2004). For this purpose, the researcher made herself familiar with the culture of the organization that was investigated, at the same making sure that her judgments were not affected. The participants were given full rights of refusal to participate or withdrawal from the project at any point. The researcher introduced herself and the project to all the participants. Previous findings about the implications and challenges of the GDPS adoption found in the literature were analyzed.

According to Stake (2005), case studies gain credibility by continuous and thorough triangulation. In order to achieve this goal, information from the company’s public website and documents provided after the first interview were studied. Furthermore, interview participants were asked to assess empirical findings.

To address the issue of transferability, Shenton (2004) suggests describing background data and providing ample thick description of the phenomenon, so that the readers can understand it properly and compare the description in the report with their own settings. At the same time, the author questions “whether the notion of producing truly transferable results from a single study is a realistic aim or whether it disregards the importance of context which forms such a key factor in qualitative research” (Shenton, 2004, p. 71). For the purpose of the current thesis, the description of the phenomenon under investigation was provided, the research setting and the characteristics of the interviewees were described.

Dependability refers to the ability of the future researcher to repeat the same work (Shenton, 2004). Thorough reporting of the research activities gives the reader an overview of the employed methods and how effective they were (Shenton, 2004). For the purpose of the current report, all the processes within the research project were documented in detail.

In order to ensure confirmability, the results of the research must be based on the interviewees’ ideas and perceptions and not on the researcher’s preferences (Shenton, 2004). The findings of the current thesis were based on the perceptions of the industry practitioners and the author of the research remained as unbiased as possible. In addition to this, initial interview questions were motivated and based on the literature review. The process of data analysis and moving from raw interview data to categories and later to concepts was thoroughly documented.

3.9 Ethical Considerations
Ethical issues must be taken into consideration for all methods (qualitative, quantitative, mixed) and stages of research (Creswell, 2008).

According to Creswell (2008, p. 208), “first and foremost, the researcher has an obligation to respect the rights, needs, values, and desires of the informant(s)”. Keeping this in mind, the researcher made sure that all the interviewees understood their rights and role in the research. All the informants took part in the case study voluntarily and were able to withdraw from the research activities at any time. The participants were notified about devices and activities used for data collection (Creswell, 2008).

Informed consent forms were handed out to the interviewees and signed by both the researcher and the informants. The form contains elements mentioned in (Creswell, 2008) and (Sarantakos, 2005) and can be found in Appendix B.

The employees of the organization were aware of the identity of the researcher and the purpose of the research. Also, the interviewees were encouraged to contact the researcher in case of any questions or concerns. Prior to the publication of the thesis, all the information related to the participating organization was made available to the interviewees. The informants were
ensured that all the information deemed confidential by them, including their personal data, would be hidden from the thesis on their request. The results of the research activities were used only for the purposes stated in the current paper.
4 Empirical Findings

In this section, the findings from the interviews are described.

4.1 Empirical Findings from the Interviews

After the initial interview and analysis of documents, GDPR specific interviews were conducted where challenges related to the GDPR were discussed in detail. In order to keep track of the context of discussed topics, all interviews were recorded.

The interview data was analyzed using the guidelines presented in Lichtman (2010). The analysis started with the assignment of codes, followed by the assignment of categories and concepts.

As a result of this analysis, five main themes were identified.

Theme 1) Understanding regulation in order to implement it into information system
Theme 2) Creating new tools and processes
Theme 3) Reviewing existing tools and processes
Theme 4) Human resource availability for the support, management and development of information system
Theme 5) Facing possible Customer-related issues

These themes are discussed in detail in the following sections.

4.1.1 Theme 1: Understanding Regulation in Order to Implement it into Information System

This section describes the issues that are connected with the understanding of the GDPR.

All interviewees were asked to describe how the GDPR affected their way of working in the organization or the organization itself.

IN1 replied: “I would say, it impacts us on all levels, all teams, everyone is involved in it in one way or another. It’s either training or it’s a new way of working and new processes”.

Additionally, IN1 thought that the interpretation of the GDPR has not been much of a hindrance, at the same mentioning that it is a new regulation with no legal precedent or court cases to use as a reference: “...it’s new and there are no court cases to look at, so of course there are some things, but I wouldn’t say that it has hindered us so much (in our work for GDPR compliance)”

IN2 replied that the employees of Assently are now more concerned about such aspects as logging, testing, encryption. “I feel that we are even more concerned about what (type of) logging data we are putting in and also what (user specific) data we are putting in when we are trying to test the system, also (what) things should be encrypted. Data that we are processing, it should be encrypted if it’s already not encrypted”.

IN3 said: “It makes us more vigilant, we think more about data, we think more about things we do when we develop new features, how we handle the data and what data is sensitive and what we need to capture, what is required. That’s the bare minimum, basically.”

IN4 said: “...we have to be more careful about everything we do, from a developers’ perspective at least. And it does not only involve the data that we get through the code, but also
from a sales perspective, (for example) where sales teams collect information about companies or people that they (sales team) have to contact. So, obviously, previously we were not that actively thinking about it, but now, once GDPR has become a thing, we are more actively thinking about it and thinking about the things like minimization of information or even removing information when it is not relevant anymore. So from that perspective, it is a major impact. Because from a point where you do not think about it to a point that you are, completely actively, thinking about it, it’s a major shift.”

Regarding the training offered by the organization to its employees, IN1 replied:

“We’ve had some general trainings and biweekly company meetings, but I think we will have to do even more training down the line, because it’s not a one-time thing”.

IN2 also said that he had been offered training by the organization: “Yes, we have been given training”.

IN4 stated: “we have been building our own knowledge over time, also through the kind of things we do (for example) group sessions and team meetings, etc.”. He later added: “I think we have a really good general understanding”.

Several respondents also mentioned the guidance that the team gets from legal advisor:

IN4: “and we are also relying on the knowledge of our legal party, legal people in the company. They have knowledge and they also have knowledge of the product, so we are hoping that will guide us in the right direction”. He added: “I think, from a person who is leading development and also (as a person) figuring out the tasks that we have to do, I try to be as aware about it as possible, and I’m spending a lot of time with our legal person. (For example) when we are making all the different tasks and features, etc., we try to ensure that we take care of the GDPR perspective as best as possible from the onset.”

IN4 also stated that since the same person has both the legal and the product management knowledge, it allows the employees to consider GDPR aspects from the early stages of development cycle: “when we are creating user stories and tasks, the legal person is there because he is also a product manager in our case. So we are always discussing things from a GDPR perspective“.

IN3 also said that he gets advice from the company’s legal advisor in case of old logs: “Usually what I do is I ask our legal guy“.

At some point, external resources were involved in the GDPR work. IN4 said that the organization had had discussions with the consultant company to make sure they have the full understanding about the documentation they have to maintain:

“We hired a consultant company that helped us get on the way, their main reason of existence in our company was ISO 27101, but we also had some sessions with them on GDPR, and we tried to nail down all the different kind of documentation that we need”.

Understanding the requirements regarding the appointment of a DPO created some challenges:

IN4 thinks that understanding GDPR requirements related to the need to appoint a DPO was a challenge. He said Assently was considering having discussions with an external consultant company: “They (Assently) will talk to an external consultant company”.

IN1: “We talked about an external one (DPO), but we haven’t made a decision yet. Right now our assessment is that we are not obligated to have a DPO.”
IN1 also mentioned that understanding certain new GDPR requirements could require additional effort. When asked if the organization had to change processes to accommodate the concept of privacy by design and default, he replied:

“Yes. Maybe a year ago we started thinking about it actively and now we also have it documented. So it’s part of the process when we release new features.”

“We will probably have to get some more education on those (privacy by design and default) and get some training in what it actually is. Since it is a new requirement, privacy by design and by default, then there are not that many trainings available; you cannot go to that many conferences that only have this. But, we will have to make sure that we are actually doing the right thing”.

GDPR-related training is not something that will end with GDPR adoption. The organization sees it as a continuous process, especially as new employees might join the company. Hence, this is a challenge the organization will face in the future.

When asked if the organization was planning any recurrent training in the future or introduction plan for the new employees, IN1 replied: “Actually, both of them. And it touched our information security work as well, because in our ISO certification we’re also required to have information security awareness trainings, so we will do both at the same time. They are not the same question, information security and data protection, but the tools are the same. So we can have those two things together”. “It is part of our employee on boarding; it’s a checklist that we have for each employee that starts”.

IN2 also realizes the necessity of recurrent GDPR-related trainings in the future: “Maybe some kind of training might be a good idea to have. I mean, after every six months”.

IN1 mentioned that it was hard for the organization to estimate how much time and effort GDPR preparations will require “Maybe we started too late, I think, that’s a common theme with many companies, and we didn’t really realize how much work it would take. So now, we are spending a lot of time in our last month...It’s not going to stop on the 25th, it’s going to be an ongoing project, but we started a little bit too late.”

When asked how the organization is going to ensure that employees delete the data also from their personal computers, IN4 answered: “I guess the answer is training. We will have to train them and I guess this will be a part of some SOP, Standard Operating Procedure. So we write that when a company is removed, we make sure that we remove everything even from a personal computer perspective”.

Conclusion: Overall, the respondents do not perceive the interpretation of the GDPR as much of a hindrance, however, some requirements proved to be more complicated than other requirements. Therefore, additional effort to interpret them was required. Moreover, the organization has to ensure that its employees are aware of the coming regulation and its implications, hence different trainings and discussions were conducted. In addition to that, the necessity of further trainings was acknowledged.

4.1.2 Theme 2: Creating New Tools and Processes

The organization had to develop new processes and features, in order to be compliant with the GDPR. The challenges that the organization experienced are described in this section.

For its Customers, Assently acts as data processor. The aim of the organization is to provide the tools for the Customers that will allow them to handle the data, and in turn, minimize the
need for manual effort by the organization’s employees to perform the same tasks. For example, Assently is working on creating tools that will allow Customers to delete the data.

According to IN4, End-customers, who will want to exercise these rights, will be referred to Customers, who act as data controllers: “Most of the time, we act as a data processor, so we are just doing the things that the data controller is asking us to do. So if somebody asks us that we should delete the data, we are going to refer him to the data controller. For most part, the data belongs to the controller, so we don’t do anything with it, we just provide them the tools”. He added: “this functionality of deletion is not something that was there in the past, but we’re actively building it, so that the controllers can do it themselves, but for the part where they cannot, we will obviously help them. We are actively trying to build tools that allow the controllers to do these themselves”.

IN1 said: “We are preparing to help our Customers, who are the data controllers, so if they get a request like that (to delete End-customers’ data), we will have to tell them how to do. But we do not see that it will be so much burden on us, it will be more on our Customers. So we are building our tools so that Customers can actually find all the information (by themselves) so they do not have to contact us. Actually they can do it in the tool”.

He clarified that the main target is to make it as automatic as possible: “…that’s actually a challenge, because we don’t know, we can’t really know if there will be one person contacting us or a hundred thousand. But if there’s a lot of people, then automatic will be the best way forward, so we are trying to build it as automatic as possible, because it would take too much time if someone would have to do it manually”.

IN1 also added: “…in our Data Processing Agreement that we have with our direct Customers, it’s always specified that if we get a request that is meant for our Customer, we just forward the request to them. And we have to do it within a very short amount of time, because the clock starts ticking, once a person has sent the request”.

IN2 stated that he is working on the feature for data deletion: “I am the one who is implementing this feature. When the End-customer is going to ask the Customer to delete certain data, that Customer is going to use our feature and delete the specific case when they want. They can also set this feature (so that) that there can be automatic deletion as well”. He added: “the only challenge that I see right now is this that it’s quite hectic for us to implement these features”.

IN3: “I think the biggest challenge was that we had to develop new things with customers and we had to handle customer data and that made us aware of how to deal with that (data) and that was, I think, a challenge on how to keep the data safe basically, and remove the data after implementing, (and) after testing as well”. He added that deletion of certain data would be performed “through user interface”.

Documentation requirements stipulated by GDPR can be challenging for organizations, especially the small ones.

According to IN4, one of the challenges related to the GDPR documentation requirements was the absence of a template for the DPIA (Data Protection Impact Assessment) documentation.

IN4: “I think the first challenge is to get the right templates for those kind of things and that’s a challenge because there’s no one template to do that, there is no one DPIA template. I think different organizations have made different templates and I think the good thing with our company was that they took some of the famous ones and they kind of merged them together in order to, for example, cater for the majority of the risks that could happen. And then we started
to make the documentation for that, and it is still in progress, it is still on the way. But yeah it was a challenge, because, for instance, we wouldn’t even know about it to begin with.”

IN4 (when discussing accountability principle of the GDPR) stated: “Documentation is a challenge in itself ... Documenting everything, knowing what to document, knowing what it should look like, that all the information is there, that we are transparent. I think it’s a challenge in its own right”.

When talking about documentation and transparency requirements of the GDPR, IN1 said: “one of the challenges is that there is a lot of work to be done and we’re a small organization, so maybe that’s the biggest challenge. But the actual work just has to be done”.

Concerning demonstration of the GDPR compliance, IN1 added: “There is a lot of documentation to be done and that’s a challenge in itself. It’s a challenge when you’re a small organization, to have a lot of documentation and keeping it up-to-date”.

He added: “But we try to be transparent and we try to publish as much as possible on our website. So, before today, we did not have a list of our sub-processors on our website, but now we have it publically available for our customers. So that’s for transparency and just to make it easier, because if we have to send that list to all of our customers, that’s a lot of work, so it’s easier to put it online. And it’s a requirement that we need to show that we have agreements in place with these sub-contractors.”

Having GDPR-compliant documentation is not just a one-time effort for the organization, rather something that will have to be maintained in the future. When asked how the organization is going to comply with the accountability principle, IN4 replied: “it will be by way of documentation, we will have a lot of documentation on how our processes work”.

IN1 mentioned that when possible, he tries to make sure that no personal data is involved:

“I try to scope out as much as possible and whenever we buy in a new system or want to do something new, we try to make sure that we don’t process personal data, because if we do, then we will have to protect it accordingly”.

Conclusion: To sum up, additional tools and processes had to be introduced to secure GDPR-compliance. The respondents mentioned documentation as a challenging task, especially for small organizations. Moreover, documentation should not only be created, but also maintained in the future.

4.1.3 Theme 3: Reviewing Existing Tools and Processes

Another group of challenges is related to reviewing processes and tools that already exist in the organization.

According to IN2, trying to understand old software code can be challenging, especially for the employees, who are new in the company. Additionally, implementing new features got more complicated due to legacy software code: “the organization is new, still in the startup mode, it has some old code and we are still trying to understand that code, so making changes in that code takes time. So the biggest challenge is basically to find time to implement all these things.”

Moreover, due to the GDPR adoption, the organization had to revisit logs related to legacy systems.

IN3 mentioned that the organization had to revisit old logs to make sure they did not contain any personal data, which was challenging as some of them were related to legacy systems: “We
still see logs from the past we always stumble across new things, which are quite old, but for us new”.

IN4 stated regarding privacy by design: “We are also more careful about, for instance, data that we collected. So those kind of considerations are common for privacy by design. Now we do think about them anymore”. He added that “you are doing other things, but this becomes the most important thing because (of the) GDPR and the challenge is to find that time to do it. And also especially when it’s a system that you have not developed yourself”.

Reviewing logs is the issue that got special attention due to the GDPR preparations. Assently is making sure that logs and do not contain any personal or unrelated information.

According to IN1, “ensuring data minimization is a lot of work” and it is “mostly related to log files. We have to make sure that we have both, data retention on the logs, retention period, so that we don’t keep it longer than we need and also that the actual log files don’t contain more than we need”. He added: “We’re trying to ensure that we don’t log personal data, just log actual (software code) commands instead”.

IN2: “Now we cannot add anything in logging that can help us identify a user”.

IN3 said: “We do have log data and we try to not log sensitive information”. He added: “it’s a challenge for us as developers, to figure out what exactly we can log and what not”.

IN4: “Previously we were not that concerned about, for instance, logs, but we have changed the rules now, we only collect for a certain amount of time”.

Also, IN4 mentioned that the organization is considering what data should be collected from the initial stages of development: “We were always careful, but now are more careful. All decisions, even the features that we make, we actually actively write what needs to be logged and what should not be logged, so everyone is more informed now. We have done an assessment and we will do a further assessment into what the logs look like. So from a log’s perspective, that is work to do”.

Assently also had to look into terms of the third party tools.

IN4 said: “we are actively looking into their solutions with respect to GDPR”. He also added that the organization had to “at least read their Terms and Conditions properly. And also understand where, where their operations exist”. “There is a thing, if you have a company in USA, I think you have this thing called the Privacy Shield agreement and then it’s kind of ok. So you have to do this assessment and have a record of all these assessments, so you have to have the documentation that you did this assessment and you also have to have the documentation where you said that how is customer data processed in our systems and yes, we have also done it”.

IN1 said: “we have one or two sub-processors that are outside of the EU, and those are both very big companies that have certifications and they also have the … EU-US Privacy Shield, so we just had to update that documentation and make sure that it was OK in all our data processing agreements and that was not a big problem.”

IN2 said: “I haven’t done that, but I know that some people (at Assently) do that”.

He also confirmed that the organization had to review the terms of third-party processors or vendors: “Yes, everyone”, and that it was a challenge in itself.
Assently had been encrypting data even before the preparations for the adoption of the GDPR started. However, the focus on encryption has increased significantly, according to IN1, IN2 and IN4.

IN1: “We are improving our encryption, really working on that”

IN2: “We keep on improving this thing and we keep on improving and building encryption as well as adding more security”.

IN4 said: “we were using it (encryption) before as well but it was never the focus, because there’s so many other things to do.” He also stated: “we spent considerable amount of effort in making sure that files are encrypted ... That wouldn’t have been out primary concern maybe in the past, but because (of the GDPR) we did have to ... shift focus”.

While describing the way encryption is performed, IN4 said: “we have a new system that we use just for certificate management, secrets management, so we are completely revamping our system” and added that the technology is “truly cutting edge”. He added that it was a challenge: “It was challenging, for sure. It has taken quite many months to try to get this whole thing in place it is extremely exciting and very nice to have. But the amount of time and the resources and the understanding you need about the system it was challenging, for sure, because we did not build the system”.

IN3 mentioned that the aim of the organization is that enhanced encryption should not affect user experience: “our target is that it shouldn’t affect the customer at all, that it should be seamless as it was before, so the customer doesn’t notice any difference. That is what we strive for.” He confirmed that the organization updated infrastructure for this purpose.

All of the respondents stated that the organization has increased security measures due to the GDPR. IN1 added, that the preparation for the GDPR adoption is progressing in parallel with the preparation for the ISO certification.

IN1: “Since we’re doing both the information security certification and GDPR readiness at the same time, I would say yes, but it is for both of those projects. So we’re not treating GDPR as just one thing, (but in) combination with ISO 27000, so for both of them, yes, we are spending more time and resources on privacy and security”.

He also stated: “We’re getting a certificate in information security, and that requires a lot of documentation, a lot of new processes, and also some audits and preparing for that, and when we are doing it, we are also doing GDPR preparations. We’re spending a lot of time on both privacy and information security”.

IN2: “Yes, because organization is increasing (security), for example, more and more data is getting encrypted”.

IN3: “Definitely we are doing encryption of our data this is I think one of the biggest security improvements we had”.

IN4 provided several examples on how the focus on security had increased: “it was always secure, the systems, but we are looking to take this one step further with encryption and making sure that people have as little access as possible. For instance, there were people who would leave the organization, but their accounts in certain cases were not removed. Even though their access was limited but now we are much more careful about it, we remove as much as we know about the person. So that they do not have access nor the information, because we do not need their information anymore. This is one thing, the other is encrypting stuff, making sure there is no default passwords in the system, and all passwords are reasonably complicated. For our
systems, we want that people use two-factor authentication, though it is optional, but it is there. For ourselves as well, for instance, our accounts, the services that we use, we want to internally enforce that there is at least two factors of authentication. We were doing it in the past as well, but now we’re actively trying to do it more, which is a good thing”.

According to IN1 and IN2, due to the existence of penalties in the GDPR, required some additional communication with the Customers:

IN1: “it got attention both internally and externally, so customers started asking questions. If there were no penalties at all, then I do not think that we would have done so much. So yes, both external and internal attention due to penalties. That’s a good thing”.

IN2: “They are more concerned about how their data is being processed”.

One challenge mentioned by IN1 in relation with breach notification, is additional negotiations with organization’s Customers:

IN1: “one challenge is that some of our customers require us to notify them in a shorter amount of time than the GDPR stipulates. It says 72 hours, but some of the customers want us to do it within 24 hours in our Data Processing Agreement, so we are in negotiation with some customers now to try to keep it to 72, so everyone gets 72. Because if we promise just one customer that we will have to do it in a shorter amount of time, then we will have to do it to everyone. So that’s one of the challenges, but the way we are solving it is trying to negotiate and then see that we have the same time period to everyone”.

He added that the organization is improving security in order to minimize impact in case of data breaches:

“...and if it will happen, a data breach within us or one of our sub-processors, then we will probably post it on our website and also send it to Datainspektionen, the supervisory board. We are trying to implement as many security measures as possible so we (will not) have to contact the individual persons”.

This was confirmed by IN4: “... with GDPR and also the benefits you get sometimes because of encryption, you don’t have to tell the customer when there is a data breach. It made sense and this became a focus. So we did shift focus, we were already being careful, but we started to be even more careful, we started to actively look into things. So from that perspective we improved on it. But it was already relatively secure; the basics were already in place”. He also said that in case data breach happens, “we have to make a general statement as well; you can put it on your website, for instance”.

The organization also had to spend some effort on assessing their procedures related to backups, mainly in relation to data deletion requirement of the GDPR:

IN1: “We only keep backups for a limited amount of time, so if someone deletes it in the main branch, then it will still be retained in the backup, but only for a couple of days, and then the backup is overwritten. Because we have such a short amount of time span, and also because of the way we do backups, the technology is called “snapshots”, so you basically take a photo of the entire dataset. Then you cannot just delete one little thing inside of that. So due to technical limitations, we cannot. And there is actually that exception in the GDPR, that if you cannot do that with reasonable means, then it is ok. So our assessment is: because of short amount of time and also because it is technically not do-able, then we are going to keep it in the backups for that time until it gets deleted.”
IN4: “removing things from the backup, that is usually a rolling mechanism. So the Customer, if they deleted some account, it will be eventually removed from the backups as well and will cease to exist. And it’s difficult to do it any other way, because you can’t just go in a backup and remove an account”.

Some respondents thought that enhanced encryption might potentially increase the possibility of encryption-related challenges for the organization:

IN1: “There could be performance issues actually, so we will have to ensure that we will not run into any performance issues, something we will have to assess. We will have to ensure that it’s platform-independent. Another thing is in case the encryption key gets compromised, then we will have to re-encrypt everything. That will be also associated with downtime, when our services are not available so that will affect all our Customers. There are many challenges related to encryption, it’s not just pushing one button and being done with it”.

IN2 thought that enhanced encryption might complicate things in some ways:

“It can reduce the performance of the system, because every time you have to read some data and show it to the user, it has to be decrypted, and then show it to the user and then, when the user saves it again, it has to be encrypted again and placed to the file”. He also added: “Fixing of the bugs can also be slowed down, we haven’t encountered that, but that can happen. It can happen that when you are trying to fix a defect and some data is already encrypted, you have to go a little bit outside of the way to decrypt that information and then do it, whatever you want to work on. So it will slightly increase the effort. With effort I mean time and cost of hours spent on work”.

IN3: “This is something where I say it really depends on our architecture and our infrastructure”, adding that according to the organization’s target, customers should not notice any difference.

IN4 said: ”Today’s encryption standards are pretty good”, adding that: “The performance is quite good, but I think the problem could happen for instance if you are providing searching facilities. For instance, if you want to search cases, but your database and the fields that you have to search are encrypted. Then you can’t search anymore”.

Conclusion: Reviewing existing tools and processes was something that the organization employees had to do in their GDPR preparation work. The respondents noted dealing with legacy codes, making sure that old logs and backups were GDPR-compliant as a challenging task, especially since former employees might have developed these things. Despite already having very secure systems, the organization put in a lot of effort to improve security even more. Several respondents mentioned enhancing encryption as a major task that can create additional challenges in the future as well.

4.1.4 Theme 4: Human Resource Availability for the Support, Management and Development of Information System

In this section, issues related to human resources that arose due to the GDPR preparation are discussed.

Several respondents agreed that combining GDPR-related work with other business requirements creates a hectic schedule for the employees.

IN2: “right now we have these GDPR things that need to be implemented and also other business requirements as well that need to be implemented, so it’s quite hectic schedule, so I would say that it takes a lot of resources.”
He also added that the organization is using new technology and tools, hence does not need many employees to handle it under normal circumstances:

“And all of the tools we are using they are really state-of-the art systems. All the third-party tools that we are using in the code or the frameworks that we are using, they are state-of-the-art right now and that’s why we have not employed that many people, because it requires just few people to handle the whole system. But when it comes to changes, these changes are quite small but some of them (have) to be done in parallel by multiple people, and in that case we do not have that many resources, I feel”.

IN4 also stated that human availability and combining GDPR and other work could be a challenge: “if we are doing GDPR, we can’t do anything else, it’s a lot of work actually”. At the same time, he added that resources availability is often the case for startups: “Resources for a startup are scarce anyway, there’s always more stuff to do than you have people”.

IN1 also agreed that human resource availability could be a challenge.

In addition to that, as discussed in previous subchapters, external resources were involved or considered at some point. Possible obligation to hire a DPO was mentioned by both IN1 and IN4. Furthermore, according to IN4, external consultant organization was involved in the discussions about the documentation the organization has to maintain.

The possible challenges that can arise due to the appointment of a DPO are the following, according to IN4: “there will be a person who has to be paid, probably (with) access to the system, maybe developer time or some other person’s time (might be required), who is answering his questions”.

**Conclusion:** GDPR adoption was challenging also from the perspective of human resources. The organization is quite small and the number of developers is limited. Working with both the GDPR and other requirements, such as support calls, is challenging. Moreover, things like possible sickness and parental leaves and vacations should be taken into consideration.

4.1.5 **Theme 5: Facing Possible Customer-Related Issues**

In this section, possible challenges that are related to or might require additional communication with Customers are described.

Possibility of negative publicity by consequence was brought up by IN2 and later confirmed with IN1 and IN4.

IN2: “One challenge can be like this that if our Customers breach some GDPR law, we might get incorporated into the same breach as well. Even though we can fight a legal battle, but for some time, it might give us a bad publicity or reputational risk because of our Customers and that is a bit of a problem for B2B cases. In this case I feel that organization should not just review the contracts and check the GDPR-related terms and conditions with third party vendors, but with their customers as well, especially in B2B case”.

IN1 said that there is a possibility such thing could happen: “Both badwill and it could actually be that we would be liable financially somehow”. He pointed out a clause in GDPR: “I was actually this morning reading on Article 82 in the GDPR about the liabilities and it clearly states that the data subject can go to both the processor and the controller and because they have some kind of joint responsibility when it comes to. So one of our customers, if they go out of business, that person can turn to us instead and try to get money from us for damages, even though we did not do anything wrong. And again, interpretation of this, it is not super clear, so there is some kind of general worry, but I don’t think it’s going to happen”.

30
When asked, IN4 also said that such event could happen: “Maybe it’s just negative publicity by consequence, something happening even though we might not be responsible at all”.

Possible need to clarify the need for retention period, logs and backups was mentioned by IN4: “I think what’s important is that the customers know what that retention period is and why we have logs and backups”.

Some respondents thought that reduced logging could cause certain issues for the organization.

IN1 agreed that it could create challenges in bug fixing.

IN2: “Previously we were saving what user actions are being performed because it really helps us in trying to identify what defects our system has or what the user actions were (when the defect took place). But now it will be quite difficult because we will not be able to identify which user it was”.

IN4: “For testing scenarios, it might be that it becomes a little bit of a challenge.” He also gave an example: “for instance, if you’re checking some sort of a third-party signing mechanism, but you can’t log the data that is coming in from the signature”.

IN4 added that this could create some additional communication with the Customers: “Might be more dialogues with them, but I think the Customers will be more understanding at the same time”.

One hypothetical situation was raised, where a customer deletes data and the organization suffers database damage. In such case when the organization restores the backup, deleted data from the Customer will start appearing in the system again. This can be solved by asking a customer to delete the data again, according to IN1.

IN1: “We will have to contact the Customer and say that all of the actions that you did during this period of time, which is less than a day, you will have to do those actions again.”

**Conclusion:** Some issues might potentially occur due to the nature of the organization’s business, B2B. Moreover, being GDPR-compliant might create certain limitations in such areas, as customer support and bug fixing. However, it is expected that Customers will be understanding of the these changes, as they actually mean that the organization is following the rules and taking good care of the customer data.

4.2 Overview of Empirical Findings

Table 2 below contains five themes identified during the interviews. Furthermore, it contains the overview of findings belonging to each theme.
Table 2. Themes and main findings identified from the implementation related interviews.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding regulation in order to implement it into information systems</td>
<td>Getting knowledge about the GDPR</td>
</tr>
<tr>
<td></td>
<td>Providing guidance to the employees</td>
</tr>
<tr>
<td></td>
<td>*Introducing GDPR-related processes and rules to new employees</td>
</tr>
<tr>
<td></td>
<td>Understanding documentation requirements</td>
</tr>
<tr>
<td></td>
<td>Assessing what data necessary for the different information system products should be collected</td>
</tr>
<tr>
<td></td>
<td>Discussing documentation needs with consultants</td>
</tr>
<tr>
<td></td>
<td>Understanding DPO requirement</td>
</tr>
<tr>
<td></td>
<td>Understanding privacy by design and default</td>
</tr>
<tr>
<td></td>
<td>Understanding the magnitude of changes</td>
</tr>
<tr>
<td>Creating new tools and processes</td>
<td>Creating tools for data deletion</td>
</tr>
<tr>
<td></td>
<td>Creating documentation template</td>
</tr>
<tr>
<td></td>
<td>Introducing new documentation</td>
</tr>
<tr>
<td></td>
<td>*Establishing the process for maintaining documentation</td>
</tr>
<tr>
<td></td>
<td>Considering data collection in logs from the start</td>
</tr>
<tr>
<td></td>
<td>Considering the GDPR when buying in new systems</td>
</tr>
<tr>
<td>Reviewing existing tools and processes</td>
<td>Dealing with legacy code when implementing new features</td>
</tr>
<tr>
<td></td>
<td>Dealing with legacy code when reviewing existing features (enhancing encryption)</td>
</tr>
<tr>
<td></td>
<td>Revisiting legacy system logs</td>
</tr>
<tr>
<td></td>
<td>Reviewing terms of third-party tools</td>
</tr>
<tr>
<td></td>
<td>Improving infrastructure to handle enhanced encryption</td>
</tr>
<tr>
<td></td>
<td>Improving infrastructure to handle enhanced encryption</td>
</tr>
<tr>
<td></td>
<td>Improving encryption</td>
</tr>
<tr>
<td></td>
<td>*Handling potential threats due to enhanced encryption</td>
</tr>
<tr>
<td></td>
<td>*It will not be possible to provide search function due to encryption</td>
</tr>
<tr>
<td></td>
<td>Improving processes related to former employees</td>
</tr>
<tr>
<td></td>
<td>Strengthening passwords</td>
</tr>
<tr>
<td></td>
<td>Increased focus on security improvements</td>
</tr>
<tr>
<td></td>
<td>Assessing what data necessary for the different information system products should be collected</td>
</tr>
<tr>
<td></td>
<td>Reviewing logging</td>
</tr>
<tr>
<td></td>
<td>Assessing backups</td>
</tr>
<tr>
<td></td>
<td>Negotiating with the Customers regarding breach notification</td>
</tr>
<tr>
<td></td>
<td>Considering Customers’ concerns</td>
</tr>
<tr>
<td>Human resource availability for the support, management and development of information systems</td>
<td>Discussing documentation needs with consultants</td>
</tr>
<tr>
<td></td>
<td>Combining GDPR work with other business requirements</td>
</tr>
<tr>
<td></td>
<td>Internal resource availability</td>
</tr>
<tr>
<td></td>
<td>Considering the need to hire a DPO</td>
</tr>
<tr>
<td></td>
<td>*Possible appointment of an external consultant as a DPO</td>
</tr>
<tr>
<td></td>
<td>*Possibility of negative publicity by consequence</td>
</tr>
<tr>
<td>Theme</td>
<td>Findings</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Facing possible Customer-related issues</td>
<td>*Possible complications in bug fixing due to reduced logging</td>
</tr>
<tr>
<td></td>
<td>*Educating Customers about logs, backups, retention period</td>
</tr>
<tr>
<td></td>
<td>*Possible additional dialogues with the Customers (regarding customer support)</td>
</tr>
<tr>
<td></td>
<td>*Possibly having to ask Customers to repeatedly delete data in case of backup restoration</td>
</tr>
</tbody>
</table>

*Challenges, that have not been experienced by the organization yet, but are expected or might happen in the future, are marked with an asterisk.

Alternate rows are colored for the sake of readability.

The table containing assigned codes, categories and concepts can be found in Appendix C.
5 Discussion

In Chapter 2.2, various challenges that were found via literature review were presented. However, after conducting the interviews and applying Lichtman’s approach of data analysis, it was found that there were some challenges that were absent from the literature yet they were encountered in Assently. Also, there were some challenges that were found both in the literature and in Assently. Likewise, there were challenges, which were found via literature review but were not found in Assently.

Due to different environment setting and context (for example, work process, number of employees, technology stack etc.), the categorization of challenges in this study is slightly different from the one available in the literature. The summary of challenges is found in section 4.2.

In this chapter, the challenges that were found in Assently, are discussed.

5.1 Discussion of the Identified Themes

5.1.1 Theme 1: Understanding Regulation in Order to Implement it into Information System

During the interviews, it was identified that respondents consider proper training an important part of successful GDPR implementation and understand their role in ensuring continuous compliance. This agrees with Bulgurcu, Cavusoglu and Benbasat (2010, p.523), who state that employees within the organization can not only be seen as “weakest link in information security”, but they are also considered to be great assets for reducing information security-related risk. Hence, it is important that relevant rules and processes be communicated, in a timely manner, to team members, including new employees. A good way for making sure that the knowledge remains relevant and up-to-date can be to conduct recurring trainings, for example, twice a year. Furthermore, the importance of training was pointed out by several authors, such as Wipp Ekman and Billgren (2017), Cooper et al. (2017); Tikkinen-Piri, Rohunen and Markkula (2017).

One additional finding is that respondents were happy about the availability of a legal advisor in the team, stating that he was someone they could contact in case they needed guidance. Additionally, having legal knowledge in the team allows the development team to consider GDPR compliance already in the product planning stage. The absence of legal knowledge in the team can pose a challenge for small organizations and startups, which do not have many employees.

Understanding the GDPR posed a certain challenge for the organization as some requirements were more difficult to interpret than others. Additionally, there were challenges also from the perspective of employees’ time and effort in making the information system GDPR compliant. Organizations should consider the possibility of hiring additional resources (for example, external consultants) in case relevant knowledge is missing in the team.

Interpreting a new regulation can be a challenge, different interpretations of GDPR requirements might exist. As stated by IN4: “I think GDPR is quite strict and maybe over time we will realize that some of the things (in GDPR) are not supposed to be like that and there will be amendments, etc. I guess that’s the interpretation issue and needs to be cleared”. Therefore, it is important for the organizations to have a contingency plan for possible changes in the future.

It should also be noted that all businesses contribute to a country’s economy. Hence, it would be beneficial for the countries to request the EU to bring such regulations in iterations. In the
absence of clear definitions or interpretations of the GDPR, there is a risk of small organizations going out of business due to non-compliance. Results from the interviews show that while the organization is trying its best to be GDPR compliant, there are fears that some requirements could be interpreted in wrong ways. As the EU comprises of different countries, it is beneficial for the whole EU that such regulations are brought into effect in small parts. Moreover, it should be researched how the fines for non-compliance with the GDPR can be made in incremental mode. This can prevent small businesses from declaring bankruptcy due to incorrect interpretation of the regulation.

5.1.2 Theme 2: Creating New Tools and Processes

Due to the increased territorial scope, privacy requirements and data subjects’ rights, it is possible that GDPR implementation will require development of new tools and introduction of new processes. In order to comply with the requirements related to the increased data subjects’ rights, Assently implemented new tools that can be used by its Customers. Additional efforts had to be put in due to the GDPR provisions related to logging and documentation. All of this required time and effort, as well as balancing this work with other business requirements.

Several respondents mentioned documentation as a challenging task. Documentation and transparency was also one of the challenges pointed out by Wipp Ekman and Billgren (2017). Tikkinen-Piri, Rohunen and Markkula (2017), also state that documentation requirements posed by the GDPR can be challenging; furthermore, they emphasize the importance of paying attention to the company- and business sector-specific risks when conducting a DPIA.

Assently is employing a proactive approach to transparency, publishing as much information on their public website as possible, which not only helps to increase customer trust, but also simplifies some aspects of accountability for the organization. Moreover, as mentioned in the previous section, respondents said that they pay attention to GDPR aspects already from the early stages of the development cycle. This can be seen as a good approach to ensure accountability. According to (Butin and Métayer (2015, p.24), organizations often see accountability as a burden, and one way of handling it in a more efficient way would be “including provisions for accountability right from the start, in particular for information systems handling personal data (extending the “privacy by design” principle to “accountability by design”)”.

5.1.3 Theme 3: Reviewing Existing Tools and Processes

Assently placed a lot of effort to make its systems and processes more secure over time for the GDPR implementation. Some of the software codes and features were created by people who had left the organization, hence understanding and improving legacy systems required a lot of time and effort.

Legacy systems were also mentioned as a compliance challenge by Wipp Ekman and Billgren (2017), who pointed out that understanding location of the data, technology employed in the organization and ensuring compliance of data processes is not only complicated but also requires a lot of time. In addition to that, Bennett (1995, p. 19) wrote that update and migration of legacy systems “has technical and nontechnical challenges, ranging from justifying the expense to dealing with offshore contractors to using program-understanding and visualization techniques”.

Encryption has been mentioned both by the literature (such as Tankard (2016), Tikkinen-Piri, Rohunen and Markkula (2017)) and the industry practitioners. Even though improving encryption required a lot of effort from the participating organization, it also brought a lot of
benefits, such as enhanced security and minimized notification obligation in case of data breaches.

As stated by Cooper et al. (2017), existing terms with third-party processors should be reviewed by organizations during their preparations for the GDPR. Reviewing and understanding third-party tools was a crucial task that had to be performed by Assently in order to avoid the risk of non-compliance. As an example, it was important to understand if the tool was sending data outside of the European Union.

Wipp Ekman and Billgren (2017) identified that the existence of penalties got attention both from within the organization and the customers. Similarly, the industry practitioners, who participated in the current study, said that the existence of penalties got both external and internal attention and the Customers started asking questions. Furthermore, some additional negotiations were required due to the GDPR requirement of breach notification.

5.1.4 Theme 4: Human Resource Availability for the Support, Management and Development of Information System

Assently utilizes state-of-the-art tools for its information system development; it has been operating as a highly efficient organization. However, with GDPR compliance, additional work requires more heads as tasks are small but high in number. It posed challenges in relation to resource availability for system support, development and management.

The issue of resource availability was also mentioned in the literature. Wipp Ekman and Billgren (2017, p. 41) identify resource allocation as one of the compliance challenges, at the same time stating that it is “something that have been less problematic with the GDPR, as it has gotten attention from managerial levels”. Furthermore, according to Tikkinen-Piri, Rohunen and Markkula (2017), GDPR adoption requires significant resources, both human and financial. Hence, the finding agrees with the existing literature.

Bulgurcu, Cavusoglu and Benbasat (2010, p. 542) recommend the practitioners to allocate “a certain amount of employees’ time to be used to fulfill the requirements of the ISP (information security policy) so compliance efforts do not compete with daily job-related activities”. This can also be seen as a suggestion for organizations implementing data privacy-related measures.

5.1.5 Theme 5: Facing Possible Customer-Related Issues

One of the findings of the current study was that B2B organizations, who act as data processors, might be affected by the breach that was caused by data controllers. Assently can get bad publicity due to the breach caused by its Customers.

Additionally, processes and features that were changed or implemented due to the GDPR will have consequences that might have to be explained to the organization’s Customers.

Such challenges can lead not just to loss of revenue but also to increased costs for the organization.

According to Tikkinen-Piri, Rohunen and Markkula (2017), new GDPR requirements bring extensive changes to privacy policy implementation of the organizations. Consequently, it is possible that such major implementations will require certain changes in features and services offered to the customers. At the same time, the new regulation will both facilitate organizations’ work and improve privacy protection of data subjects (Tikkinen-Piri, Rohunen and Markkula, 2017). Furthermore, Tankard (2016, p. 8) states: “The time and effort required to achieve compliance will vary greatly from one organization to another, but it is well worth the effort”. This agrees with industry practitioners’ perception that the changes caused by the
GDPR implementation are beneficial for the customers, hence, the customers are expected to be understanding.

5.2 Significance of the Study

The outcome of the current thesis was a list of challenges faced by a Legal Technology organization when implementing GDPR-related changes into their information system. Both the challenges that the organization had already faced and the challenges that are expected or possible to happen in the future are captured in the study.

The findings of the study will be beneficial for the industry practitioners who plan similar major implementations in the future. The findings can also be relevant for small-sized organizations belonging to industry other than Legal Technology. Furthermore, these findings can also be used for the emerging Legal Technology organizations, who have to be compliant with the GDPR, hence, design their information systems accordingly.

The study contributes to the GDPR-related research. Tikkinen-Piri, Rohunen and Markkula (2017) wrote that empirical studies on how organizations are implementing the requirements of the new legislation should be conducted. Furthermore, Wipp Ekman and Billgren (2017) stated that research in specific domains would be beneficial. The current study is addressing these areas. Moreover, the study contributes to the literature dedicated to the relatively new and rapidly developing Legal Technology sector.
6 Conclusion

6.1 Conclusions

The aim of this qualitative interpretivist study was to investigate how a Legal Technology organization is affected by the challenges of the GDPR implementation in its information systems. Since not all of the challenges were experienced during the implementation of the regulation, the purpose of this thesis was also to gather expected challenges of the GDPR adoption as perceived by the employees of the organization. Due to the complexity of modern software and the magnitude of changes required for the successful adoption of the GDPR, such challenges can be significant. Furthermore, as Legal Technology sector is relatively new, it was not covered by any GDPR-related research.

In order to address the purpose of the study, the following research question was posed:

RQ: How is a Legal Technology organization affected by the challenges of the GDPR implementation in its information systems?

To answer the research question, a literature review was conducted, followed by a case study in Assently AB, the small-sized organization belonging to the Legal Technology industry. First, an introduction interview was conducted with the purpose of acquiring information about the organization, its products and processes. After that, semi-structured interviews dedicated to the GDPR implementation challenges were conducted. Four employees, who are working with the information systems and are aware of the GDPR-related preparations, were chosen for the interviews. In addition to that, the information from the organization’s public website was studied and documents were demonstrated to the researcher during the first interview. This allowed the researcher get a better understanding of the organization and its processes.

While analyzing the challenges identified during the interviews, five themes were identified:

1) Understanding the regulation in order to implement it into information system.
   This theme contains the challenges connected with both interpreting and learning the GDPR.

2) Creating new tools and processes.
   This theme comprises of challenges related to the implementation of new processes and tools.

3) Reviewing existing tools and processes.
   The theme contains the challenges the company faced when reviewing the processes and tools that already exist in the organization.

4) Human resource availability for the support, management and development of information system.
   The theme where the challenges related to the availability of both internal and external resources are described.

5) Facing possible Customer-related issues.
   This theme contains possible challenges that are related to or might require additional communication with the Customers.

Among many challenges, the study found that it was beneficial for an organization to have a legal advisor whose input could be used while designing the requirements. Having such a
person meant that GDPR related requirements could be enforced from the early implementation stage of any requirement. For the challenge of stale knowledge regarding the GDPR, recurring trainings for the employees were suggested to renew their knowledge. Due to the impact of massive fines as penalties for non-compliance with the GDPR, it is suggested that such requirements should be introduced in iterative form, so that small iterations are enforced in smaller periods. This will motivate the organizations to start working on the requirements earlier in time. Fines should also be researched so that approaches could be found to enforce fines in incremental ways. Otherwise, there is a risk of small organizations declaring bankruptcy due to massive fines.

It was found that as part of its compliance with the GDPR, the organization had to develop new tools and processes. Such tasks take time and effort and take away the focus from other general business requirements. Having a proactive approach to transparency and making as much information publicly available as possible, helped not just in increasing customer trust but also simplified some aspects of accountability for the organization.

Apart from designing new tools and processes, existing processes and legacy code needed to be reviewed as well. This included enhancing encryption techniques and methods as well as making changes to legacy code whose original developers had left the organization. It increased human effort and time needed for completion significantly. The challenge of reviewing the third-party vendor tools was also identified in the study.

While Assently had been using state-of-the-art tools, it also meant that small amount of people was employed by the organization. Hence, the resource availability became an issue when additional work required more heads.

It was found that some issues might potentially occur due to the nature of the organization’s business, B2B. Furthermore, being GDPR-compliant might create certain limitations in different areas, such as customer support and bug fixing. However, customers are expected to be understanding of these changes, as this actually means that the organization is following the rules and taking good care of the customer data.

To sum up, the findings from the interviews revealed that the industry practitioners experienced certain challenges in their effort to implement the GDPR. In addition to that, the respondents stated that ensuring GDPR compliance is a continuous process. Educating employees, maintaining documentation and considering GDPR requirements when developing new features are some of the activities that will continue after the implementation date of the regulation. Moreover, the respondents mentioned some of the GDPR aspects that might affect the organization in the future.

6.2 Contribution of the Study

The thesis resulted in a study on the challenges of the GDPR implementation faced or expected by the organization in the Legal Technology industry.

This study contributes to the literature dedicated to the GDPR-related research and Legal Technology organizations. Even though some literature on the GDPR is already present, the Legal Technology industry has not been the focus of GDPR research.

Additionally, the findings from this thesis will be useful for organizations and industry practitioners to conduct better risk analysis for the upcoming similar implementations. It is also possible that challenges similar to the ones identified in this study will be faced by the small-sized organizations in other industry domains.
Furthermore, emerging Legal Technology organizations can also benefit from this study, as these organizations will have to design their information systems in compliance with the GDPR.

6.3 Reflections

This research was dedicated to the challenges faced during the implementation of the GDPR-related changes in the IS of a Legal Technology company. Conducting this research gave the author an opportunity to see the work of an information technology organization from the inside. In addition to that, it helped the researcher to get a better understanding of a Legal Technology industry. Furthermore, it allowed the researcher to acquire knowledge about how the compliance of the information systems is ensured.

One challenge experienced by the researcher was that there was not much literature available on the Legal Technology industry. The challenge was solved by conducting an introduction interview with the product manager of the organization in order to understand the products and the ways of working of the organization.

Conducting interviews was a new experience for the researcher. The participants were willing to share information; hence, it was possible to collect all the necessary data through the interviews. Analyzing raw data from the interviews proved to be a challenging task for the author, however, careful revisions of initial codes and categories allowed the researcher to arrive at the logical concepts.

6.4 Suggestions for Future Research

The focus of this study was on the challenges faced by a small-sized legal technology organization in implementing GDPR requirements in its IS. In future, challenges faced by organizations of a different size or belonging to a different industry may be explored.

Moreover, once the GDPR comes into force, a study that evaluates the cost of such implementation will be beneficial. Additionally, a study of how to reduce such costs by employing various processes can be conducted.

One suggestion presented in this study is to introduce major regulation in iterative mode by the EU authorities. The EU authorities or different countries can research the possibility and aspects of such implementation in future. Furthermore, a more efficient way to penalize organizations for non-compliance can be studied. For example, the fines can be incremental, meaning that the fine for the first breach, which may have resulted from a wrong interpretation, can be smaller. Subsequent fines can be increased with the degree of non-compliance.
References


Bitar, H. and Jakobsson, B. (2017) GDPR: Securing Personal Data in Compliance with new EU-Regulations. Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering.


Appendix A1: Interview Guide for the Introduction Meeting

**Interview Guide for the Introduction Meeting**

The purpose of the meeting is to get an overview about the organization and the services it offers. Moreover, the introduction meeting will help understand the various processes being followed in the organization, for example, resource availability process (support on-call process), number of employees etc.

The following questions have been designed in order to understand the different aspects of the organization and how they might be affected by the clauses stated in the GDPR. For example, questions related to customers’ demographics can highlight the challenges that might arise due to non-EU customers in foreign states governed by non-EU laws. Hence, it is important to understand the organization and its working in detail.

1. Can you please state your role and how long you have been working in the organization?
2. Can you please describe the services provided by the organization?
3. Can you describe the information system used by the organization?
4. What type of customer segments use the services provided by the organization?
5. Does the usage of the services offered by the organization differ among various segments? If yes, how?
6. Can you please describe a typical use-case?
7. How is the user data from a common use-case saved in the system?
8. How is the logging and tracking of user actions being performed in the system?
9. How many human resources does the organization employ?
10. What major roles exist in the organization (for example, developers, product manager, support staff, etc.)?
11. Can you describe the end-to-end cycle of feature delivery (SDLC)? (For example, can you describe how do you get the requirements for the product? How the requirements are defined and made available to the rest of the stakeholders? What happens after the requirements phase? How do the requirements get translated into technical requirements? Likewise, can you please describe the other phases in detail?)
12. How is test data produced for testing environments?
13. How is support/bug reporting from the customer perspective handled by the organization?
Appendix A2: Interview Guide (GDPR Challenges)

Interview Guide (GDPR Challenges)

Assently AB’s services are used by different organizations, which are referred to as "Customers". The customers of these organizations are referred to as "End customers". Each sent document ("case") can have one or multiple persons ("parties") who sign it. There can also be persons which are not involved in signing documents, however, they might still need to view or be informed of the signing process. They are referred to as "stakeholders".

1. General
   1.1 Please state your name, role and how long you have been working in the organization.

2. Staff training
   2.1 Are you aware of the GDPR?
   2.2 How does the GDPR affect your way of working in the organization, as well as the organization itself?
   2.3 Have you been given any trainings, seminars, etc. related to the GDPR by the organization?
   2.4 Are there any possible exemptions from using the GDPR for your organization (alternative regulations, standards)? If yes, please describe them.

3. Consent policy
   3.1 Please describe the challenges or difficulties you have faced in relation to the GDPR principle of consent (obtaining, recording, withdrawing, and consent of underage persons’ parents or custodians)?
   3.2 Does Assently AB have to take consent from all parties and stakeholders?
   3.3 Did you have to implement any specific consent management system or consent management process for your products? If yes, please describe.
   3.4 Do you apply ISO or any other standards when developing your consent form (for example, is it readable by vision-impaired users)? If yes, please describe.

4. Increased rights of data subjects (right of access, erasure or right to be forgotten, data portability, rectification, restriction, objection, automated individual decision making, information to be provided)
   4.1 Please describe the challenges you have faced in relation to the increased rights of data subjects under the GDPR (such as right of access, right to be forgotten, right to data portability).
   4.2 How will data subjects be granted access to their personal data?
   4.3 How will the data deletion be performed (right to be forgotten)?
   4.4 Have you considered different locations where users’, parties’, stakeholders’ data might be saved (tools, storage locations, e-mails, support systems, test data, developers’ machines, etc.)? How do you make sure that such data is removed in relation to the right to be forgotten?
   4.5 Do you have an alternative legal basis (alternative law) that prohibits you from securing the increased data subjects’ rights (for example, the right to be forgotten)? If yes, please describe.
4.6 Does the organization apply automated individual decision-making, including profiling? If yes, have you reviewed this process? Please describe the challenges you see in relation to this.

5. Documentation and transparency
5.1 Please describe the challenges you have faced in relation to the documentation requirements of the GDPR.
5.2 Do you have to keep both the record of personal data processing activities and a data protection impact assessment?
5.3 How will the documentation be handled?
5.4 If your organization employs Agile-working principles that normally require little documentation, do you think increased documentation needs under the GDPR will interfere with these principles? If yes, how?

6. Data breaches
6.1 In case of any data breach, Assently AB will need to notify the authorities or the data subjects, as part of its compliance with GDPR. How will such requirement be handled?
6.2 Please describe the challenges you see in relation to that (for example, locating data subjects within a designated timeframe).
6.3 Have you increased your organization’s security measures due to adoption of the GDPR? If yes, please describe the performed changes.

7. Privacy by design and default
7.1 Did you have to change your processes to accommodate privacy by design/default requirements? If yes, please describe the performed changes.
7.2 Please describe the difficulties you have faced or you think you will face in relation to this requirement?

8. Pseudonymisation and encryption
8.1 Will the organization use pseudonymisation of data to protect personal data?
8.2 How will the organization pseudonymise the data?
8.3 How will pseudonymisation of data affect data processes of the organization?
8.4 Will the organization use encryption of data to protect personal data?
8.5 How will the organization encrypt the data?
8.6 How will encryption of data affect data processes of the organization?
8.7 Is the test data encrypted / pseudonymised? Can it slow down the testing process?
8.8 Is pseudonymisation / encryption used for logging? Can pseudonymisation / encryption slow the process of solving customer support requests, debugging, and fixing errors (and as a result make system more vulnerable)?
8.9 Do you see any problems that can arise from encryption/pseudonymisation of data? If yes, please describe.
8.10 Do you see any impact on user experience due to such implementation?

9. Data minimization principle
9.1 Please describe the challenges you have faced in relation to the GDPR data minimization principle?
9.2 Did you have to change the way you collect user data / delete any data? If yes, please describe how.

10. Data protection officer
10.1 Is your organization required by the GDPR to appoint a data protection officer? If not, are you planning to appoint one?
10.2 Are you planning to appoint someone from within or outside of your organization? Are you planning to share the data protection officer with other organizations?
10.3 In your opinion, what kind of knowledge should a data protection officer have?
10.4 Do you see any challenges in adapting to this article of the GDPR? If yes, which ones?

11. Demonstrating GDPR compliance
11.1 Do you see any challenges in demonstrating your organization’s compliance with the GDPR? If yes, please describe which ones.
11.2 How is the organization planning to demonstrate its compliance with the GDPR, if necessary?

12. Penalties
12.1 Does the existence of penalties affect your processes? If yes, please describe how.
12.2 Did the existence of penalties under the GDPR affect the way you conduct your business with your customers in any way? If yes, please describe how.
12.3 Did the existence of penalties under the GDPR pose any challenges for your organization? If yes, please describe them.

13. Territorial scope
13.1 Does the organization transfer data to countries outside of the EU or have data storage outside of the EU? If yes, did the organization have to implement any additional safeguards? Which ones?
13.2 Please describe the challenges you have faced due to increased territorial scope of the GDPR?

14. Reviewing terms with third party processors/systems
14.1 Did you have to review terms with any third party processors? If yes, please describe the challenges you have faced in relation to this.

15. Concluding question
15.1 Please describe any other challenges you have faced in relation to the GDPR implementation that have not been mentioned yet.

Miscellaneous questions:
16. Do you have any systems, code, application or module that was written in the past but its original authors have left the organization? For such legacy code, do you face any difficulties in implementing GDPR related requirements? If yes, please describe them.
17. Do you face any challenges or difficulties related to human resource availability planning in relation to GDPR? If yes, can you please describe?
18. Was the implementation of the GDPR a costlier requirement compared to general business or market requirements?
Appendix B: Informed Consent Form for Master Thesis

Informed Consent Form for Master Thesis

Research Topic (Slight Modifications Possible)
Challenges Involved in the Implementation of General Data Protection Regulation (GDPR)

Researcher
Kristiina Kutserenko, Master Program in Information Systems, Linnaeus University.
E-mail: kk222md@student.lnu.se

Purpose of the Study
The purpose of the study is to investigate the challenges that legal technology organizations are facing in their effort to implement GDPR-related changes in their information systems.

Benefits for Participating
After understanding the organization and its processes in detail, different challenges will be highlighted by the researcher, which may allow the organization to better prepare for the GDPR compliance. Furthermore, the conclusions from the thesis will be useful for organizations and industry practitioners to conduct better risk analysis for the upcoming similar implementations.

Participant Involvement
You will be asked to participate in semi-structured interviews, where the organization and your experiences with the GDPR adoption will be discussed. Your answers will help me understand the information system of the organization and the challenges that its employees are facing when trying to implement the GDPR requirements. In addition to this, observations might be conducted by the researcher, if permitted by the organization.

Risks to the Participants
Participation in the research is seen as free of risks for the interviewees. Your answers collected during the interviews will be used only for the purpose of this research.

Confidentiality
Prior to the publication of the thesis, all the information related to the participating organization will be made available to the interviewees. All the information that is deemed confidential by the participants will be hidden from the thesis on their request, this also includes personal data of the individuals.

Withdrawal
Participation in current research is strictly voluntary. The participants can withdraw from the research activities at any point. The interviewees can also refuse to answer any specific questions without justification.
Additional Questions

If you require additional information about this research, please contact Kristiina Kutserenko (kk222md@student.lnu.se).

Please sign this consent form acknowledging that you understand the purpose of the research, your rights and your role in the research.

Participant’s name:
Participant’s signature:
Date:

Researcher’s name: Kristiina Kutserenko
Researcher’s signature:
Date:
# Appendix C: Codes, Categories and Concepts Identified from the GDPR Implementation Interviews

<table>
<thead>
<tr>
<th>Code</th>
<th>Category</th>
<th>Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting knowledge about the GDPR</td>
<td>Learning new regulation</td>
<td>Understanding regulation in order to implement it into information system</td>
</tr>
<tr>
<td>Providing guidance to the employees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Introducing GDPR-related processes and rules to new employees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Understanding documentation requirements</td>
<td>Interpreting regulation</td>
<td></td>
</tr>
<tr>
<td>Assessing what data, necessary for the IS, should be collected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discussing documentation needs with consultants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Understanding DPO requirement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Understanding privacy by design and default</td>
<td>Understanding the magnitude of changes</td>
<td></td>
</tr>
<tr>
<td>Creating tools for data deletion</td>
<td>Developing new features</td>
<td>Creating new tools and processes</td>
</tr>
<tr>
<td>Creating documentation template</td>
<td>Creating new processes</td>
<td></td>
</tr>
<tr>
<td>Introducing new documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Establishing the process for maintaining documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Considering data collection in logs from the start</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Considering the GDPR when buying in new systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dealing with legacy code when implementing new features</td>
<td>Reviewing legacy codes/systems</td>
<td>Reviewing existing tools and processes</td>
</tr>
<tr>
<td>Dealing with legacy code when reviewing existing features (enhancing encryption)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revisiting legacy system logs</td>
<td>Reviewing existing tools</td>
<td></td>
</tr>
<tr>
<td>Reviewing terms of third-party tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improving infrastructure to handle enhanced encryption</td>
<td>Enhancing security</td>
<td></td>
</tr>
<tr>
<td>Improving encryption techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Handling potential threats due to enhanced encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Limitations of providing good user experience due to encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improving processes related to data left by former employees in IS</td>
<td>Reviewing existing processes</td>
<td></td>
</tr>
<tr>
<td>Strengthening security and IS access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessing what data, necessary for the different information system products, should be collected</td>
<td>Reviewing existing processes</td>
<td></td>
</tr>
<tr>
<td>Reviewing logging mechanisms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessing backups mechanisms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiating with the Customers regarding breach notification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Considering Customers’ concerns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discussing documentation needs with consultants</td>
<td>Human resource availability</td>
<td>Human resource availability for the support, management and development of information system</td>
</tr>
<tr>
<td>Combining GDPR work with other business requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal resource availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Considering the need to hire a DPO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Possible appointment of an external consultant as a DPO</td>
<td>Facing possible Customer-related issues</td>
<td>Facing possible Customer-related issues</td>
</tr>
<tr>
<td>*Possibility of negative publicity by consequence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Possible complications in bug fixing due to reduced logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Educating Customers about logs, backups, retention period</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Possible additional dialogues with the Customers (regarding customer support)</td>
<td>Possible additional communication with Customers</td>
<td></td>
</tr>
<tr>
<td>*Possibly having to ask Customers to repeatedly delete data in case of backup restoration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Challenges, that have not been experienced by the organization yet, but are expected or might happen in the future, are marked with an asterisk.

Alternate rows are colored for the sake of readability.
Linnaeus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0)772-28 80 00
teknik@lnu.se
Lnu.se/fakulteten-for-teknik