JÖNKÖPING UNIVERSITY
Jönköping International Business School

Compliance issues within Europe's General Data Protection Regulation in the context of information security and privacy governance in Swedish corporations

A mixed methods study of compliance practices towards GDPR readiness

MASTER THESIS

THESIS WITHIN:	*Informatics*
NUMBER OF CREDITS:	*30 ECTS*
PROGRAMME OF STUDY:	*IT, Management and Innovation*
AUTHOR:	*Sebastian Stauber*
JÖNKÖPING	*May 2018*

Master Thesis Project in Informatics

Title: Compliance issues within Europe's General Data Protection Regulation in the context of information security and privacy governance in Swedish corporations: *A mixed methods study of compliance practices towards GDPR readiness*

Authors: Sebastian Stauber

Tutor: Andrea Resmini

Date: 2018-05-21

Key terms: *GDPR, Privacy, Data Protection, Information Security, Privacy Governance, Information Governance, IS Governance, IT Governance, IT Compliance, GDPR Implementation, Privacy Regulation*

Abstract

The European Union has introduced a new General Data Protection Regulation that regulates all aspects of privacy and data protection for the data of European citizens. To transition to the new rules, companies and public institutions were given two years to adapt their systems and controls. Due to the large area of changes the GDPR requires, many companies are facing severe problems to adapt the rules to be ready for enforcement. This marks the purpose of this study which is to look into compliance practices in the implementation of GDPR requirements. This includes a prospect of compliance mechanisms that may remain insufficiently addressed when the regulation comes into force on May 25, 2018. The study is conducted in Sweden and aims to investigate the situation in corporations and not in public institutions.

Mixed methods have been applied by surveying and interviewing Swedish GDPR experts and consultants to gain an understanding of their view by using capability maturity scales to assess a variety of security processes and controls. The analysis shows a low implementation in GDPR requirements while having seen improvements over the past two years of transition. It points out that a holistic strategy towards compliance is mostly missing and many companies face obstacles that are difficult to overcome in a short period. This may result in non-compliance in many Swedish corporations after the regulation comes into force on May 25.

Acknowledgements

At the beginning, I would like to put some words of gratitude to the people who have been supporting me in the writing of this thesis and the conduction of the research.

First of all, to my supervisor Andrea Resmini for his guidance and feedback during the creation of my research project, and to Osama Mansour for his feedback during the seminars which helped to make this thesis better. I would also like to thank my program director Christina Keller for her continuous academic support during my Master studies at Jönköping International Business School.

Secondly, I would like to express my gratitude to my interview partners who have provided me with their insights and knowledge in the field of GDPR – Debbie Chong, Lars Magnusson and Alexander Hanff.

Finally, to all respondents to the survey who gave a bit of their time to share their thoughts about GDPR.

Thank all of you.

Sebastian Stauber

May 21th, 2018

Stockholm, Sweden

Table of Contents

Figures

Tables

Abbreviation List

AI	Artificial Intelligence
BCP	Business Continuity Assessment
BIA	Business Impact Assessment
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CMM	Capability Maturity Model
DLP	Data loss prevention
DPA	Data Protection Authority
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSM	Digital Single Market
GDPR	General Data Protection Regulation
GRC	Governance Risk and Compliance
IDS	Intrusion identification system
IPS	Intrusion prevention system
PCI	Payment Card Industry Regulation
PD	Personal data (according to GDPR definition)
PIA	Privacy Impact Assessment
PII	Personal identifiable information (former practitioner definition)
SEM	Single European Market
SME	Small and medium sized enterprises
SOX	Sarbanes-Oxley Act
TEU	Treaty on the European Union

1. Introduction

This chapter will introduce the research topic about data protection and give a broad overview of the concepts and problems in the area. It will outline the purpose of the study and delineate research questions that ought to be answered based on the delimitations which are presented here. It will close with key definitions and a disposition to transition to the theoretical background in the next chapter.

1.1 Background

The European Union was founded based on the pillars of unity and peace inside Europe by fostering a single European market with common rules and the same currency (TEU art. 3) (Bonde, 2009). These were ideas built upon the events of World War Two and have endured after the end of the cold war when a new European spirit was born to be utilised to strengthen and enlarge Europe in its values of unity and human rights (Marcut, 2017). These human rights ought to be protected whenever they are endangered which requires action taken by the European institutions. Privacy is a human concept that can be taken as a human necessity as a claim of an individual to decide which information about oneself is communicated to others (Westin, 1967, p. 166). The EU ought to protect this human right connected to this concept guaranteed by the "*European Declaration of Human Rights and Fundamental Freedoms*" (TEU art. 6 (3)) which the EU must respect based on TEU Article 2.

In the digitalised world, privacy is threatened by ever-increasing computer speeds and lowering costs of storage capacity which incentivises internet companies to store all information virtually forever in case the information could be useful for the future. This principle of data maximisation gets supported by the advent of artificial intelligence (AI) as the attempt to give computers a human-like brain. However, this software needs tremendous amounts of data from which algorithms can be used to make predictions. Rationalising human behaviour is of particular interest to businesses as it allows for more specific advertisement and better predictions of human actions. Inspired by enormous advantages for humanity, AI gets developed at rapid speed while concerns about the risks to privacy are rising (Sadeghi, 2017). Apart from the question of AI development, it raises the question of ethics of the gathering of vast amounts of data concerning privacy.

In the year 1995, the European Union (EU) voted for the Data Privacy Directive 95/46/EC (DPD) which defined the rights of European citizens regarding privacy, a concept which was for the first time defined in a legal sense on the European level (Osterman Research, Inc., 2017). Nonetheless, this directive was merely a directive which meant that even though member states were obligated to incorporate it into their own laws, they retained a certain amount of freedom in the phrasing. It must also be stated that this directive came with the arrival of the internet in the middle of the 1990s and disregards most of the specifics of privacy concerns nowadays. The directive marked the first step in the divergence from the Single European Market (SEM) for physical goods, services, labour and capital, which was promoted and realised by the Delors Commission in 1993 with the Maastricht treaty, into an inconsistently regulated market in the developing digital space (Marcut, 2017). This inconsistency is a major concern of the current Commission under Jean Claude Juncker which has taken the creation of a Digital Single Market (DSM) into their strategy to achieve in consecutive steps.

As Europe's objective principle of a single market has been violated, the directive from 1995 caused severe problems due to the nature of inconsistency of different privacy laws in member states (Osterman Research, Inc., 2017). Building an internet company across Europe is by far more challenging than in a large population country with consistent laws like the United States. To end this condition and restore the principles of an SEM, the European Parliament adopted

on April 14, 2016, the General Data Protection Regulation (GDPR) to repeal the directive of 1995 and enhance privacy rights with a legally binding regulation that comes into force on May 25, 2018 (Regulation (EU) 2016/679, 2016). The advantage of a regulation over a directive is that it does not have to be implemented by each member into national law and is valid in its approved form except some parts which leave minor decisions by the member states explicitly. For this reason, Europe incorporates a single data privacy regulation which is valid in all member states and even applies to foreign companies which use personal data from European citizens despite having no office located in Europe. In this way, the new regulation gains a global perspective as a multitude of U.S. based companies must comply with it (Osterman Research, Inc., 2017).

1.2 Problem definition

The General Data Protection Regulation will be in effect from May 25, 2018, after a two-year-long adaption period for EU companies and public institutions. Several implementation guides and frameworks were proposed to assist in its implementation during this time from which companies had a considerable choice what to pick from the collection. Due to the nature of changes that corporations are subjected to, the EU admitted that organisations would face challenges in its rapid implementation and stated an extended transition period. Non-compliance is highly consequential as compared to the current data protection directive. Consequences are high fines up to 20 million € or 4% of net income which would cause serious harm to existence for many companies (Metric Stream, 2017).

The changes affect the fields of IT governance and information security as well as privacy governance. Compliance with the regulation must be demonstrative at all time which means processes need to be formalised which have been merely ad-hoc so far. This includes risk assessment and decision-making regarding personal data processing or security implementation (Stibbe, 2017). The requirements are very process-driven and need to be addressed with new procedures and policies, as well as architecture concerns to build "privacy by design" into new products or services. The GDPR requires new organisational structures that support its obligations towards documentation of measures in security and privacy (Roessing & ISACA GDPR Working Group, 2018). A data privacy officer (DPO) must be introduced as a new role to meet these obligations (Regulation (EU) 2016/679, 2016). Breach notifications have to be done without "*undue delay*" (Stibbe, 2017) which requires fast detection mechanism and PR capabilities to communicate data breaches to the customers. All these requirements and more affect organisational as well as technical areas of an organisation (Karczewska, 2017). Hence, it increases the level of changes that are necessary to make an organisation with ad-hoc processes to a truly GDPR compliant and efficient corporation until May 25, 2018, with clearly defined policies and processes that enable it. For companies that have already well-defined IT governance structure in place, the GDPR requirements are easier to implement, but for those who are still working in an ad-hoc based condition, it is an opportunity to build one (Thomas, 2017). In principle, after the financial crisis in 2008, the trust of the people in corporations has decreased which affected legislation by introducing new regulations. Hence, this new regulation can be used for senior management to review their GRC processes to transform them into a business advantage, rather than seeing them as disadvantageous (Vicente & da Silva, 2011). As the GDPR requirements do not only need to be implemented, they also need to be documented to be able to demonstrate compliance with the regulation; processes need to be in place that makes this happen.

The supervisory authorities have a clear intention to support businesses in achieving compliance and helping in a variety of ways, but there is no research conducted in Sweden, in

which security processes and controls are at the centre of consideration in its attempt to analyse their effectiveness in compliance.

By the time of writing in January 2018, there are still five months left on the road towards compliance. As of now, significant changes have already been undertaken in corporate structures and control systems which may have caused obstacles during the project time. Therefore, we are presented with the opportunity to research in the last months of the transition period several key aspects of the current state of requirements implementation, their complications and which areas may be left insufficiently addressed after the regulation will start to be enforced.

1.3 Purpose

Based on the described research problem, the purpose of this study shall be to look into key aspects in the implementation of GDPR requirements in Swedish corporations on how these are applied to comply with the new regulation. This includes a prospect of compliance mechanisms that may remain insufficiently addressed when the regulation comes into force on May 25, 2018.

Compliance is a part of risk management in corporations which implies that requirements need to be fulfilled in a risk-minimising way but at the lowest costs. Hence, several aspects of compliance are more critical than others and need special attention. In a prior study, Billgren and Ekman (2017) outlined a very general picture of GDPR compliance challenges which they compiled in a mere qualitative study at the beginning of the GDPR transition period when many companies have not even started working on the regulation. They state in the limitations of their research that a more specific picture is needed and has relevance to the public. This study can close that research gap by using the potential of a mixed method approach with an in-depth survey and interviews which enables the creation of results that gain a deeper and more precise understanding of the variety of compliance obstacles and challenges in GDPR that limit compliance capabilities.

Critically assessed, this research purpose has the potential to produce a study with valuable and relevant output for practitioners as well as for researchers as it gains comprehension of information and privacy governance that could guide to new research in the field of IT governance holistically. On the other side, it cannot draw a representative picture of Sweden's current state in GDPR compliance, but as outlined in the delimitations of the research, this is not the intention of the study.

1.4 Research questions

Based on the described problem statement and research purpose, the following two research questions were chosen:

RQ1: *How well are key aspects of GDPR implementation in Swedish corporations applied and how have they evolved since January 2016?*

Based on a variety of key aspects that are related to GDPR and information security/governance, this question requires seeking for corporations' compliance activities and mechanisms. As the GDPR has a transition period of two years, the question intends to investigate which processes and controls have been seen by companies as the most important to tackle to become compliant.

RQ2: *What are the compliance obstacles and challenges that may remain insufficiently addressed by adequate processes and controls by May 25?*

Among all regarded GDPR aspects, the question arises what major obstacles exist that reduce the capabilities to comply. These obstacles may be of technical or organisational form or a combination of both. The interest lies in processes and controls that are applied to tackle those but cause severe challenges that might end up immature to comply with GDPR.

1.5 Delimitations

The thesis shall focus on Sweden and merely on corporations. The reason for this delimitation is to achieve a narrow focus for the study on particular organisations. As the GDPR has implications towards organisational and technical levels, it is more appropriate to study structurally similar organisations. Corporations and public organisations like governmental agencies have very different structures and need to fulfil different requirements for their data collection. Corporations gather data to fulfil business promises to their customers, whereas governmental agencies are gathering data to execute the duties of the state. Hence, the amount and sensitivity may vary considerably why it makes sense to focus on one type of organisation. For this thesis, the focus lies solely on business corporations in Sweden.

Additionally, this study intends to focus on key aspects related to GDPR compliance in terms of organisational and technical requirements. It does not aim to build a representative-probabilistic picture of Sweden's GDPR compliance in corporations; it merely makes statements about selected aspects that were chosen based on available literature and the interest of the author. A holistic approach would exceed the feasibility of the research project. Hence, a focus on selected aspects was drawn.

1.6 Definitions

In order to understand some essential concepts in the course of this thesis, several terms are defined and explained to equip the reader with the necessary knowledge for further reading.

1. Data controller and data processor

The data controller/processor can be any legal or natural person that is collecting and processing personal data. The decisive difference between these two actors is the question of who is determining the *"purpose and means of processing"* (GDPR art. 4). While the data controller is setting it, he/she is also accountable for the compliance with GDPR principles. The data processor is merely *"processing personal data on the behalf of the data controller"* (GDPR Article 4). Still, the processor is accountable for the adequate protection of the data and fulfilment of protection requirements in the contract the processor has with the controller (Metric Stream, 2017).

2. Personal data and data subject

Personal data is in the centre of the GDPR's attention which requires a detailed definition by law. A definition which was too vague in the directive of 1995 (DPD). As new data types were starting to be processed (ex. geo-location which was not prevalent in 1995), national courts had decided what falls into the categories of the directive which were implemented inconsistently among all member states (Hert, Papakonstantinou, Wright, & Gutwirth, 2013). The accurate definition of personal data and their owners, the data subjects, was formulated in the following way: *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,*

physiological, genetic, mental, economic, cultural or social identity of that natural person." (GDPR art. 4(1)). The term of Personally Identifiable Information (PII) is, therefore, broader than this new and very narrow term of Personal Data (PD) in the GDPR. In many old laws in different territorial jurisdictions, the term PII is used. Hence, it made sense to replace the term with a more explicitly defined notion which can achieve to be a new global standard (Roessing & ISACA GDPR Working Group, 2018).

3. Special categories of personal data

Like the definition of personal data, the regulation defines special categories which are merely allowed to process under special conditions. Violations in this field are suspect to the highest category of fines. Special categories of personal data are *"racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"* (GDPR art. 9(1)).

4. Data Protection Directive (DPD)

The Data Protection Directive 95/46/EC is the currently applicable directive from the European Union which was put into national law of all member states until 1998. It is going to be repealed on May 25, 2018, when the GDPR comes into force (Regulation (EU) 2016/679, 2016).

1.7 Disposition

The thesis is structured in a way to introduce the reader to the topic and methodology used in the research. Afterwards, the results will be analysed, and conclusions will be drawn that get discussed at the end.

The theoretical background will bring the new regulation in perspective and outline its principles and main requirements. The theory in this chapter will be used to build the research design of the study.

The methodology chapter will present how the mixed method study is conducted and outlines the reason for the chosen methods to find adequate answers to the research questions. It concludes with a discussion about the research quality of the study.

In chapter four, the results of the study will be presented and analysed by taking into consideration the theory from chapter two.

After that, conclusions will be drawn to satisfy the purpose of the study and adequate answers to the research questions will be formulated.

The thesis will end with a discussion about the study, implications for research and practice as well as limitations and strengths of the conducted study. It will also analyse its research contribution and which future research could be conducted.

2. Theoretical framework

This chapter will provide the theoretical background in which the research is conducted. It will put the new regulation in context, state its guiding principles and in which main requirements they are translated. After that, starting with an explanation of information security and its role in personal data protection which is supported by the theory of IT compliance in current research. At the end, this will be linked to implementation guidelines and governance frameworks that are in use to lead to a successful and well-monitored requirements fulfilment.

2.1 GDPR in context

2.1.1 Legislature history

Since the beginning of the age of computers, data processing had begun in the 1970s with larger data sets, increased with stronger computers and ultimately with the connection of those to regional networks which ended in the global internet as we know it today. This development caused a new problem in the society as the question arose in which extent do these new technologies intervene with our privacy (Regulation (EU) 2016/679, 2016; Hert & Papakonstantinou, 2016).

As one of the pioneers, the German district Hessen had implemented in 1970 the first data protection law (Wilhelm, 2016). This law was merely limited to that district, but set a precedent for future laws and decision, in particular in Germany where the highest court proclaimed the "*right of informational self-determination*" in 1983 (Wilhelm, 2016). In 1981, the first European data protection treaty entered in effect, called the Council of European Convention 108. During this time, there was no legal possibility to declare law in all European member states, hence, a treaty needed to be signed which was also signed by non-EU member states, in total 47 (except Turkey) (Wilhelm, 2016). Figure 2-1 shows the way of privacy legislation throughout the years.

After the Maastricht treaty in 1992, the European Parliament gained the power as a co-legislator and gave it more control over the executive, in particular, the right to issue directives which commands the legislatures of member states to implement their content into national law (The European Parliament, 2018). In 1995, the first directive concerning data protection was put into effect by the parliament. Called Directive 95/46/EC, it had to be implemented by all member states until 1998 (Wilhelm, 2016). Nonetheless, it must be stated that this new directive was produced at the beginning of the information age when processing and data storage costs were still high which discouraged high amounts of random data storing (Hert et al., 2013; Hert & Papakonstantinou, 2016; Osterman Research, Inc., 2017). This has changed and a new regulation needed to be found, especially after severe revelations about global surveillance programs in the 2010s and the rising pervasiveness of information technology in our lives (Wilhelm, 2016). Another essential driver for change were the inconsistent privacy laws in the Union which discouraged companies to build information systems across Europe due to high compliance costs (Hert et al., 2013; Osterman Research, Inc., 2017). This inconsistency could appear as European member states can implement a directive in different ways in each member state. A directive sets the common goal but leaves out how the member states implement it. With the new treaty of Lisbon in 2007, the European Parliament gained power by replacing the co-decision procedure of the Maastricht Treaty with the new ordinary legislative procedure

which covers more policy grounds including privacy and security (The European Parliament, 2018). This change enabled the passing of a European regulation by Parliament and Council which requires no implementation into national law (Osterman Research, Inc., 2017). This way of implementation was also preferred by the European Council (Hert et al., 2013). The new General Data Protection Regulation was adopted April 14, 2016, by the European Parliament, Council of the European Union and the European Commission and will enter in effect on May 25, 2018 (Regulation (EU) 2016/679, 2016).

2.1.2 Privacy by design and default

The term "Privacy by design" is rather new and was coined first on the conference "Computers, Freedom & Privacy" in the year 2000, but had no immediate consequences in the time afterwards (Hutchison et al., 2014). Hence, one can say that this concept was first made popular during the development process of the GDPR as its clarification was given in a footnote of one of the proposal papers (Hutchison et al., 2014). The footnote read the following: *"The principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal."* (COM 2012, 11 final) (European Commission, 2012). At this time, it defined a concept which was undefined before, even though it was considered an important prerequisite for every information technology project. Usually, in particular, at the beginning

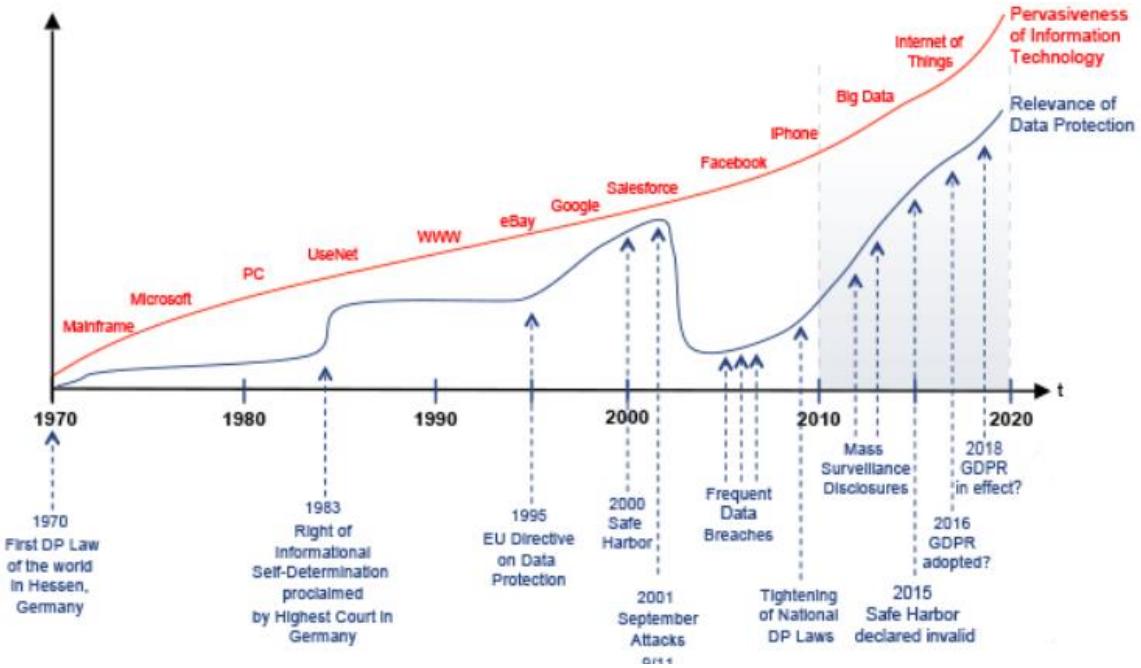

Figure 2-1 History of data protection (Wilhelm, 2016)

of the time of computer engineering, security was seen as a requirement which can be addressed later when the product is in its final stages of development. Due to this, many software applications and internet protocols have attached-security, rather than inherent-security (e.g. SSL on IPv4). Building security into a system from the beginning makes the product inherently more secure as the solution ships with fewer vulnerabilities in design (Brotby, 2010). In principle, the concept can be regarded as a *"technical approach to a social problem"* (ENISA, 2014, p. 48). The GDPR takes this concept into legal action and requires conducting data protection impact assessments (DPIA) if the processing of data poses a privacy risk to data subjects that cannot sufficiently be addressed by the data controller (GDPR pretext (84)). This activity will be part of a company's due diligence and would have legal consequences if it is

not or not accurately enough conducted. It is in particular mandatory if special categories of personal data are going to be collected (Roessing & ISACA GDPR Working Group, 2018).

The concept "privacy by default" is considered rather as an add-on to "privacy by design" as it links this concept to the accountability of an organisation towards taking the privacy of their clients seriously (Cavoukian, Taylor, & Abrams, 2010). This requires rules and governance to commit to privacy policies and the rights of their clients. Hence, it requires implementing "privacy by design" in all their products and solutions (Cavoukian et al., 2010; Hert et al., 2013).

There was broad criticism about the concept of "by design" in a draft document (European Commission, 2012) of the regulation that was published in 2012. Koops and Leenes (2014) point out in their article that "hardcoding" privacy requirements in technological terms would complicate the matter and reduce its feasibility. They state that it would be wise to interpret "by design" rather as an organisational matter which can lead to a more general understanding and support the implementation of highly technical standards like NIST SP 800-53. Technology best practices are already available and can be used to achieve "privacy by design" whereas GDPR can support in a communicational perspective by changing the mindset of IT project managers to regard privacy and security in the design stage of the project (Koops & Leenes, 2014).

All in all, it can be concluded that despite criticism and wide-spread confusion about the exact definition of "privacy by design and default", the European Parliament seems to have responded to this discussion which it fostered by releasing early drafts of the regulation early in 2012. The final text in article 23 states the concept from an organisational perspective rather than a technical one. Specific engineering requirements are not given, the regulation refers by implication towards standards, frameworks and best practices which are already existing and maintained by practitioners in the field.

2.1.3 Supervisory authorities

Enforcement of the new regulation is a major concern of the European Union. Hence, a good network of enforcement agencies is required.

Even though the regulation is European, it is enforced on a national level at first and on European level only for special issues. This means that each member state must have a Data Protection Authority (DPA) in place which will transition from enforcing the DPD to the GDPR. As DPAs are already in place, most member states naturally move the competence of their authority to the new law (Team ITGP Privacy, 2016). In Sweden, this competence falls under the responsibility of "Datainspektionen" which is a governmental administrative authority under the justice department (Förordning (2007:975) med instruktion för Datainspektionen, 2017).

Raab and Szekely (2017) have conducted a survey study among DPAs to research about the state of expertise in a DPA which is needed to do its duty adequately. They concluded that high-level experts are needed to *"monitor relevant developments"* (GDPR art. 57(1i)) to fulfil their role in the GDPR next to their primary tasks as regulation enforcement authority. The DPAs are focusing on developing such expertise in-house rather than getting the experts from consulting firms to keep their independence and save costs (Raab & Szekely, 2017). As data protection is by nature a "*moving target*", the DPAs must keep track of technological advancements to remain a functioning executive body in the enforcement of European law (Raab & Szekely, 2017, p. 15)

2.2 GDPR principles and main requirements

2.2.1 Principles

The primary purpose of the GDPR is it to give back control to European citizens about their data and therefore strengthen privacy as a human right. To achieve that, the regulation is driven by principles from which individual requirements are drawn that have to be implemented in organisations that process personal data from European citizens. These principles were created first and foremost before the regulation was written (Hert & Papakonstantinou, 2016). They ought to be used for the interpretation of the law for courts and hence had to fulfil certain conditions. According to Hert et al. (2013, p. 134) *"all-encompassing, abstract and omnipresent"* is the main condition to fulfil. This abstraction is notably important to keep the regulation contemporary in the time of rapidly evolving information technology. However, these principles can also help to guide companies towards compliance with their systems (Team ITGP Privacy, 2016). Some of these principles remain the same as with the directive of 1995, but a change in their definition. In total, six privacy principles were developed which can be found in article 5 of GDPR:

1. *Lawfulness, fairness and transparency*

This principle is comprised of three parts from which the most important consideration is lawfulness which requires that the processing is under the disposition of article 5 in the regulation which states that consent must be given, and the processing is necessary for the fulfilment of the contract apart from others. The data controller has to describe the processing activity which has to match with what is really undertaken (e.g. "transparency") and is not allowed to go out of the scope of the primary consent (e.g. "fairness"). If further processing is required, additional consent has to be collected first (Team ITGP Privacy, 2016).

2. *Purpose Limitation*

Once the purpose of the data collecting activity has to be stated to the data subject via privacy notice, this purpose cannot be widened without consent. According to article 5, data gathering is only allowed for "*specified, explicit and legitimate purposes*". This means in practice that the selling or transferring of personal data sets to third parties is not allowed if their use of the data is beyond the scope of the original privacy notice (Team ITGP Privacy, 2016).

3. *Data Minimisation*

For every data collection, it is obligatory only to collect the data types which are actually required for the fulfilment of the contract. Article 5 states that the personal data collected should be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". The use of excess data is prohibited. As the main reason for this obligation is the objective to reduce the amount of data that could be stolen or become outdated as it does not have any necessity to be kept up-to-date (Team ITGP Privacy, 2016).

4. *Accuracy*

This principle aims to protect data subjects from wrong decisions made based on profiling and has the potential to reduce the risk of identity theft which usually happens with outdated data. It requires that data must be *"accurate and, where necessary, kept up to date"* (GDPR art.5) (Team ITGP Privacy, 2016).

5. Storage Limitation

Once the purpose of the data collection is fulfilled or not valid any longer, the data has to be removed from the servers. This requirement does not apply to all subjects which are obliged to apply with GDPR. Several exceptions are given which can be summarised for archival purposes, for example in healthcare records and similar. In principle, the new regulation tries to minimise the amount of data stored from their citizen to reduce the extent of possible data breaches (Team ITGP Privacy, 2016).

6. Integrity and confidentiality

The last principle is directly connected to the overall information security of an organisation, both in technical as well as in organisational matters. While GDPR, in general, is more about privacy and not about cybersecurity, this principle links privacy to cybersecurity by stating that it is imperative to address the security of personal data *"in a manner of appropriate security"* (GDPR art. 5(1-f)) by implementing *"appropriate technical and organizational measures"* (GDPR foreword (78)). This abstract wording intends to refer to best practices, standards and frameworks that guide information security practitioners to implement adequate safeguards in company networks to protect from data breaches and malicious intrusions (Brotby, 2010; Team ITGP Privacy, 2016).

2.2.2 Data subject rights

In the following, I will analyse the rights that were given to data subjects by the regulation to bring them into context with the principles of GDPR and how they connect with requirements. The primary focus of every GDPR-regulated organisation should be to enable the rights of European citizens.

First and foremost, it is of importance that the data subject has the right to be informed about the way, their data is processed and by whom. This transparency connects directly to the **right to access** their data by requesting a copy. Under the GDPR, this right is even broadened by receiving further information about the time period; their data is processed. Also, the **right to rectification** ensures that the possibility must be given to correct data, either by themselves or automatically based on the criticality of the information. This regular updating is extraordinarily important when the data is used for profiling purposes which helps in automatic decision making. At this moment, the rights of a citizen might be violated if a decision is made by an algorithm based on inaccurate information. The **right to appropriate decision making** gives the individual the right to request human intervention to protect from automatic decision making that has legal effects (e.g. creditworthiness) (Team ITGP Privacy, 2016).

As one of the most controversial rights under the GDPR is the **right to be forgotten** or how article 17 GDPR calls it officially, the **right to erasure**. Primarily, it simply states that data has to be deleted as soon as the purpose of the data collection is not valid any longer or the data subject withdraws consent by utilising their **right to object.** In 2014, the European Court of Justice demanded that Google must apply the right to be forgotten on the internet by deleting links to sites with personal information. This right was derived from the Data Protection Directive from 1995 and thereby created a precedent (Lee, Yun, Yoon, & Lee, 2015). As it is merely impossible to delete all information on the internet once it was published, the legislators decided to put a reasonable claim into the regulation by stating in article 17, clause 2 that this should be done by *"taking account of available technology and the cost of implementation, shall take reasonable steps to inform controllers which are processing the personal data".* Of

course, this right has limitations as for the archiving, defence purpose, public interest or to protect the right of others which falls under freedom of expression (Team ITGP Privacy, 2016).

A right in the middle ground is the **right to restrict processing** which gives the individual the right to restrict the processing of certain information. Its major purpose is to protect citizens from storing excess information even when particular services are unused. If the data controller himself is altering or removing the data, it is in their duty to inform the data subjects, known as the **right to notification** (Team ITGP Privacy, 2016).

The last right that must be considered is **the right to data portability** which enables data subjects not only to access a copy but also request the data in a portable form or to move it to another data controller. This transfer could be done automatically or via a machine-readable format like CSV (Team ITGP Privacy, 2016). One can say that this novelty is the major noticeable change for data subjects as it makes it easier to switch from one digital provider to another. This right creates an overlap with the right to access which can be considered as a *"right of knowledge"* whereas portability is a *"right of controllership"* (Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez, 2017, p. 9). Nonetheless, this right remains unclear in its extent as it is unclear which type of data must be made available for transfer. Hert et al. (2017) describe two cases concerning the degree of information transfer. Either, the regulation limits it to data that was provided by the data subject *(*e.g.*"adieu scenario"*) or widens its definition by including the produced data by the data controller (e.g. virtual properties like Facebook posts, collected fitness data, etc.) in a so-called *"fusing scenario"* (Hert et al., 2017, pp. 9–11). The latter would introduce a *"user-centric platform of interrelated services"* (Hert et al., 2017, p. 11) on the internet and foster competition among service providers. The actual text leaves this open to interpretation which might engage the courts in the future to set precedents for this user right.

2.2.3 Data protection impact assessment

Data privacy requires data protection which is mostly a technical concern. A conventional method in information security is the risk assessment which aims to identify and analyse the risk and to obtain risk prioritisation for which mitigation steps can be implemented to reduce the risk (ISO/IEC 27005). In business terms, a business impact analysis (BIA) is conducted to get a list of processes sorted by priority based on criticality. This way, it helps to construct a well-designed business continuity plan (BCP) which enables recovering the main processes in an efficient and fast way, but also to implement controls to respond to the risk of process failures (Brotby, 2010). Similar to a BIA, the GDPR requires undertaking a data protection impact assessment (DPIA) to assess the risks of processing certain personal data in new environments. Basically, for all new services and processes that require the use of personal data, it is advisable to conduct a DPIA and document its steps to demonstrate compliance. Even though the assessment is facultative, it is obligatory if data from special categories (GDPR art. 9) are planned to be processed. The main goal of a DPIA is to gain knowledge if data processing results in high risk of the *"violation of the rights and freedoms of data subjects"* (Roessing & ISACA GDPR Working Group, 2018, p. 31). Hence, it considers the impact on data subjects and not like the BIA, the financial impacts on the corporation. Still, these two assessments are intertwined in their result as data protection implies information security in the network of an organisation together with failsafe software applications that do not disclose any information once they fail/crash (Brotby, 2010).

Regarding GDPR, it is crucial to put a formalised DPIA process into the organisation or to outsource the process to external consultants. These obligations may look at the first view as an inconvenience, but also offer advantages as it reduces unnecessary costs for projects whose

privacy impacts are not tolerable regardless. Those projects can be cancelled at the beginning of the project lifecycle before they cost too much money. If privacy concerns are manageable, the assessment helps to identify them that safeguards can be built in from the design stage (e.g. "privacy by design"). Overall, this assessment shows that a DPIA can be more considered as an instrument of self-regulation and transparency that reflects an organisation's commitment to privacy (Wright, 2013).

Several guidelines were produced to conduct Privacy Impact Assessments (PIA) as it was first called in the early years (the regulation itself names it data protection impact assessment). One of the first ones was the PIA Framework (PIAF) which was finished in 2012 and proposes a six-step process (Wright, 2013). Numerous other ones exist for different purposes and environments and were all produced from the start of the discussion about a new European data protection regulation (Roessing & ISACA GDPR Working Group, 2018).

2.2.4 Non-compliance consequences

The penalty for non-compliance with the new regulation views the commitment of the European Union to enforce the privacy protection of their citizens. In contrast to the European directive from 1995, the fines are very high and encourage corporations to adopt privacy governance to comply with the regulation. The fines are of monetary nature and comprised of two brackets based on the gravity of the violation. The lower bracket imposes fines of 10 million € or 2% of the annual turnover of the preceding year, whereas the upper bracket imposes 20 million or 4% of the annual turnover, whichever is higher. The upper bracket is mainly used for violations that involve special categories of personal data like race, sexual orientation, etc. (Team ITGP Privacy, 2016).

2.3 Privacy and information security

The regulation itself outlines no specific technological requirements nor suggests any standards to comply in terms of security (Koops & Leenes, 2014). In general, the regulation focuses on privacy and demands that "*appropriate technical and organisational measures*" are taken to comply (GDPR art. 24(1)). Hence, the connection between privacy and information security in the regulation is implicit. Still, it mentions that security measures shall be taken based on a risk approach (GDPR art. 32). Security controls can be taken from existing frameworks and based on best practices in the field. Article 32 mentions this by stating the goals of each Information Security Management System (ISMS) based on the international standard ISO/IEC 27000 in clause 1(b)(c)(d). These implications are about the so-called CIA-triad which combines the major goals of information security regarding *confidentiality*, *integrity* and *availability*.

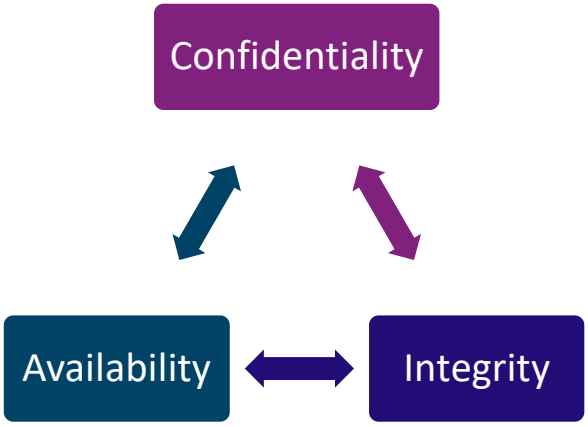

Figure 2-2 CIA Triad of Information Security (adapted from (Brotby, 2010))

Based on the global standard of the international standards organisation (ISO), **confidentiality** defines the protection of data from unauthorised disclosure which would include breaches of unencrypted data sets. **Integrity** describes the conservation of data in its form without malicious or unintentional alteration or deletion (ISO/IEC 27000). **Availability** is regarded as the possibility to access the data when needed implying the "*resilience of processing systems*" as demanded by GDPR art. 32(1b) (ISO/IEC 27000).

By this, one can see that the legislators followed global standards in information security to stringently indicate the application of best practices in the implementation of safeguards and controls. **The primary purpose of this chapter is to link the regulation towards security controls which shall enable the compliance with GDPR requirements.** Even though the regulation demands appropriate measures which seem to reflect merely technical controls, organisational controls are also necessary to consider. For the conduction of the study in this thesis, a framework that both defines the technical, as well as organisational concepts, must be developed to find valid answers to the research questions. Hence, possible evaluation frames will be outlined here to guide towards the methodology used in the study which is later discussed. This will provide a theoretical framework which the study can adapt to produce the results to answer the research questions.

Every corporation that is aspiring compliance needs to follow in their GDPR implementation project several workstreams as seen in figure Figure 2-3.

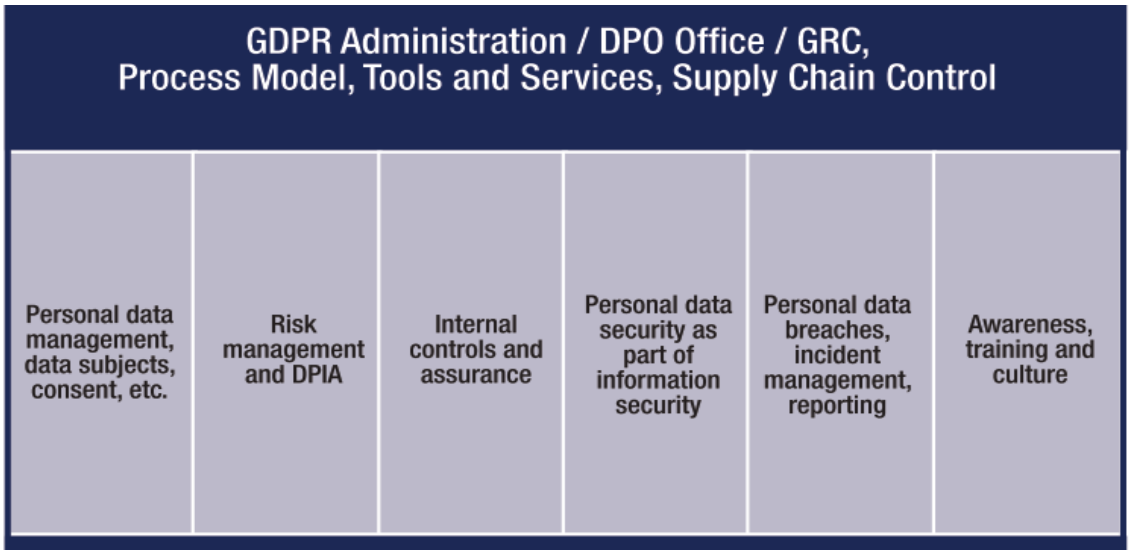

Figure 2-3 Generic GDPR Workstreams – taken from Roessing and ISACA GDPR Working Group (2018, p. 23)

It outlines the security-related subjects related to privacy protection of citizens. In establishing a personal data management, ISACA, the global organisation involved in the development of IT governance and IS audits, suggests data governance with a clear intent of senior management to set the context in which personal data management ought to happen (Roessing & ISACA GDPR Working Group, 2018).

As directed by the regulation, data protection has to follow the risk approach which enables the corporation to focus on high-risk processes and usage of resources in the best possible way. This links to the deployment of internal controls for which particular frameworks can be utilised. There are several control frameworks available which differentiate in purpose, specificity and environment. Among those are COSO as an integrated controls framework with SOX compliance purpose (COSO, 2018), COBIT 5 as a holistic framework which focuses on control objectives in information systems (ISACA, 2012) and NIST SP 800-53 which is a mere technical framework with a compilation of controls and their implementation requirements

(NIST SP 800-53, 2013). Comparable to NIST, the CIS control framework is also focused on technical control, yet, it is simpler and by far shorter which simplifies its application in the study of this thesis (Center for Internet Security, 2016). Table 2-1 gives an overview of the control areas of the framework. Each area has several controls listed which shall be implemented on a risk basis.

Table 2-1 The CIS Critical Security Controls for Effective Cyber Defence Version 6.1 (adapted from Center for Internet Security (2016))

1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defences
9	Limitation and Control of Network Ports
10	Data Recovery Capability
11	Secure Configurations for Network Devices
12	Boundary Defence
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

The GDPR encourages organisations to review their personal data protection measures to either integrate it into their information security management system or build one from scratch. This phenomenon is what Zerlang (2017, p. 8) calls a *"milestone in convergence for cybersecurity and compliance"* which are often regarded as divergent by senior management. Next to

controls which can proactively mitigate risks, GDPR article 1(b) requests resilience that as described above connects to the CIA security goal of *availability*. Total availability can never be achieved with technical systems, but with rising technological maturity, the availability levels could be increased tremendously, and service level agreements with data processors often state a level of 99.999% (Stewart, Chapple, & Gibson, 2015). Hence, valuable incident response procedures must become prevalent in organisations to comply. Even though the regulation does not state any level of availability, it should be considered that industry expectations should be seen as a threshold.

Last but not least, a well-understood security awareness among employees must be in the corporation to facilitate the policies which come from senior management to operational personnel in a top-down approach. As the European Union has made clear that data protection is deeply rooted in the protection of individual rights, employees should be made aware of the setup that they are a part of success in achieving privacy protection for EU citizens (Roessing & ISACA GDPR Working Group, 2018). However, this has not only constitutional reasoning but also a practical one since it is easier to control data governance and security in an organisation when employees are participating and not sabotaging, intentionally or not, the systems in place. Between security and convenience is often a trade-off which can cause unexpected actions by employees that lean towards convenience by neglecting security measures (Stewart et al., 2015).

2.4 IT governance and security towards GDPR

Grounded by academic research and experiences from practice, practitioners from all over the world gather in various institutions to build practice-oriented frameworks. Institutions like ISACA (-> COBIT), Axelos (-> ITIL), the IT Governance Institute (ITGI) or government agencies like US-based NIST propose a variety of tools and frameworks to engage in better IT governance and security to enhance value creation in organisations. Due to this vast knowledge creation, many frameworks overlap which incentivises researchers to work out their effectiveness and application areas.

An overarching framework which shall help to provide guidance in the use of other frameworks is COBIT with its latest update in 2012 to version 5 (ISACA, 2012). Hence, compliance theory must be viewed from two angles: research and practice. This is also true in GDPR implementation projects for which practitioner institutions produced several guidelines and research was performed from a more scientific approach. The goal remains the same, and throughout the two-year transition period, new guidelines were published for which subsequent feedback was provided. One of the most impactful organisations, ISACA, published a new guide to GDPR in January 2018, (Roessing & ISACA GDPR Working Group, 2018) only five months before the regulation comes into force. This shows the continuity, in which these organisations approach GDPR support. In the following, I will provide an overview of frameworks/standards/guidelines in regard to GDPR implementation from a practical view (Table 2-2). This shall support the theoretical framework in which this study is conducted. As the study intends to select the most relevant GDPR aspects, it is helpful to understand which support material is out that has guided companies in their implementation efforts. Based on this information, the most relevant aspects can be chosen which shall be regarded in this research project.

Table 2-2 GDPR implementation guidelines

COBIT 5 and ISACA implementation guide	Holistic framework to combine Cobit with GDPR requirements. It gives control objectives and implementation timelines for organisational and technical changes.
NIST SP 800-30/37/53	American guide to risk assessment and application for information systems. SP-53 provides a list of technical controls that could provide the level of data protection needed to comply with GDPR.
ISO 27000 Information Security Management System (ISMS)	The global standard for ISMS including IT risk assessment. Each practitioner framework derives its fundamental risk approach on this standard. GDPR itself derives its risk definition from this standard.
ENISA Guidelines	The European Union Agency for Network and Information Security published a guideline in late 2014 to fill the gap between the legal frame of the regulation and potential technical solutions to fill it (ENISA, 2014).
ISO 27018 PII in the cloud	The global standard for data processors to comply with GDPR requirements. ISO certification can enhance their competitiveness as data controllers can be assured that their processors are meeting GDPR compliance.
ISO 29100 Controls to process PII	Next to NIST SP-53, this global standard gives another compilation of controls to process and protect PII.
Guidelines from regional supervisory authorities	Each national supervisory authority (see chapter 2.1.3) has published guidelines in their local languages to guide through differences in GDPR and their former data privacy laws.
Article 29 Data Protection Working Group	An independent European advisory body based on article 29 of DPD to provide guidelines on data privacy on a European level. Their guidelines are very specific but yet not industry specific. (European Union Article 29 Data Protection Working Party, 2016)

The importance of these guidelines constitutes in their broad applicability in different industries and branches. They principally tackle the same topic or are generic enough to tackle GDPR even though they were not built for this specific regulation. Of course, they display overlaps and redundant duplications and therefore also inconsistencies, but predominantly all of them are usable next to each other to find the best for one's specific business.

This chapter shall provide a context for GDPR support from several angles. It is widely known that GDPR implementation is viewed as challenging due to the short timeframe (Roessing & ISACA GDPR Working Group, 2018) despite the vast support available. Hence, it supports the motivation for this study to look into processes and controls as compliance mechanisms in Sweden as its purpose described.

2.5 GDPR compliance timeline

As the thesis research is conducted within the last five months of the GDPR transition period, it is crucial to understand the approximate state of requirements implementation. Many companies were incorporating proposed timelines, and it is likely to say that it is reasonable that most companies are in the third part of the implementation. This would mean that major requirements like DPIA, PD registers and risk analysis are already in place and governance processes and internal controls are in their last phases of development. The timeline from ISACA (Roessing & ISACA GDPR Working Group, 2018) shall give a broad overview of the

context of this study. However, it is evident that timelines differ from various companies in their goal to align it with their business.

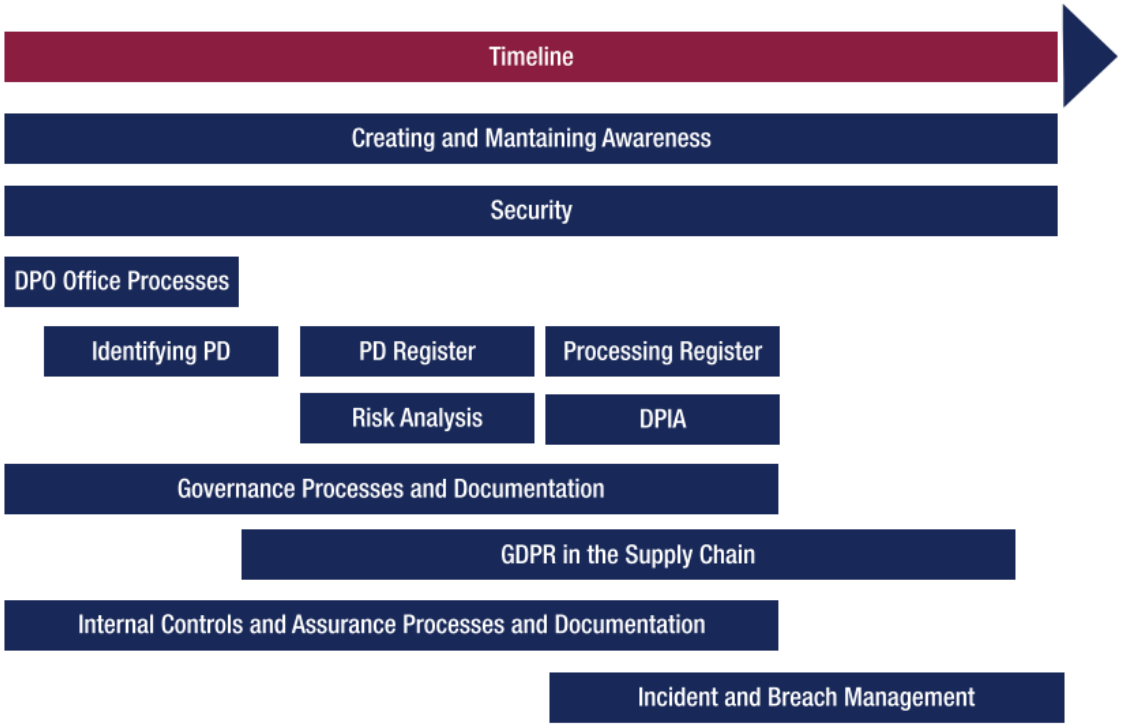

Figure 2-4 Proposed GDPR Implementation Timeline by ISACA (Roessing & ISACA GDPR Working Group, 2018, p. 24)

Next to awareness creation and security control implementation, it can be particularly stated that incident and breach management will be addressed at the end of the project when most controls are in place, and business impact analyses are performed. As one of the most impactful requirements, a company must be able to notify data subjects about a breach of data in their system "*without undue delay*" but not later than 72 hours (GDPR art. 33(1)). This requires technical measures to identify breaches early and communication methods to process a notification which fulfils the regulation both to data subjects as well as to the supervisory authority (Heimes, 2016).

The current state of implementation is essential to consider for the data analysis part of this study to keep holding perspective in the interpretation of the results and in selecting the aspects which shall be regarded for the study.

2.6 Common implementation issues with GDPR

The purpose of this research is to look into compliance mechanisms concerning GDPR key aspects and to compile areas that may be insufficiently addressed. Building on prior research, one needs to see which areas were identified at the beginning of the transition period. Billgren and Ekman (2017) conducted a qualitative study about compliance issues with the GDPR in the middle of the transition period by interviewing six persons involved in the implementation inside companies. In their findings, they present that obstacles are primarily not of technical,

Compliance Challenge	Sub-Challenge	Description
Interpretation of Regulations		How to interpret the regulatory document into implementable requirements.
Ad-hoc and Generic Solutions		The decision of redesigning generic compliance solutions or implementing ad-hoc changes to specific data processes.
Organizational Compliance		Managing the human side of data processes.
	Continuous Compliance	To continuously stay compliant after the law comes into force.
Resource Allocation		Allocating the resources needed to make an information system compliant.
Documentation and Monitoring		Understanding your systems and proving compliance to authorities.
Legacy systems		Understanding the technological landscape of the organisation, learn where data resides and make the data processes compliant.
Competing Compliance Measures		Considering former security measures, other regulatory documents and interdependencies between systems.

Figure 2-5 Findings of GDPR Compliance challenges by Billgren and Ekman (2017)

instead of organisational nature. It starts with the mere understanding of requirement needs to managing employees' behaviour to align with the rules. Senior management must be behind the efforts to allocate sufficient resources, documentation processes need to be defined, and former ad-hoc processes need changing. Figure 2-5 is presenting their findings from the thesis. The only technical obstacle the authors could find is the prevalence of legacy systems that might not have the capability to be updated. All in all, Billgren and Ekman (2017) state that current technical measures seem to be available to build a compliant organisation with GDPR, the primary concern lies in organisation and process management. Their research presents the opportunity to be developed further to analyse security processes and controls instead of merely making general statements about GDPR compliance issues. Since their study was conducted in an exploratory manner which aimed to gain a general understanding about the topic, a narrower approach is desirable in which key aspects are selected based on their research and other

theoretical frames which were outlined in this chapter. Hence, the underlying research will use the findings of Billgren and Ekman (2017) as part of the theoretical framework in which controls and processes are evaluated in their current implementation status. In particular, this study will take a deeper look into the compliance challenges of ad-hoc/generic solutions and organisational compliance in which extent they have progressed since the beginning of the transition period.

The methodology of the study will be based on current literature as the theoretical framework to develop the current scientific knowledge further by widening the spectrum and utilising a different method as previously. Different to Billgren and Ekman's study who made their qualitative research exploratory, this research will be a descriptive/explanatory mixed methods study by asking GDPR experts in a very systematic and structured way with an in-depth survey and more specific interviews than in Billgren and Ekman. This approach will produce different results to answer more specific questions as to that former research project. The next chapter will lay out the method to achieve that.

3. Research Methodology

The chapter's purpose is to lay out the methodology which was deemed adequate to achieve the goals of the research and its applied ethical rules. It gives clear motivation for why certain methods were chosen and discusses the research quality in terms of transferability, dependability, confirmability and credibility.

3.1 Research Method

Various research methods can be adapted to conduct investigations and experimentations. Those methods are either qualitative, quantitative or a combination of these (Saunders, Lewis, & Thornhill, 2016). This study follows the **interpretivist** research paradigm in an **abductive** approach and **applies quantitatively-driven mixed methods** to make statements to describe the current state of the observed phenomenon and draw conclusions about future compliance capabilities.

The large field of compliance is difficult to impossible to measure due to its complexity and interconnectedness. In order to conduct a study in this field, one must accept this complexity and find a practical way in which good research can be produced in which rigour and relevance can be attained in a balanced way. Hence, **mixed methods** have been seen as the way to go in order to achieve a well-structured and relevant research that inheres the capability to grasp the field of compliance in all nuances. In particular, this study utilises quantitative methods with a **survey** questionnaire as the primary source of data collection. This is combined with qualitative data from **expert interviews** to corroborate the results as the secondary source of data. The questions aim to answer the two research questions by assigning numerical values (e.g. Likert scales) to the qualities of key aspects of GDPR compliance (e.g. quantitative data). The respondents of the survey will be experts in the field of GDPR in Sweden that have gained vast experience in the implementation of this new regulation in various Swedish companies as consultants. Their profile will be described further in a later part of this chapter. These experts will be asked for their holistic view of the current state and compliance efficiency of numerous companies they have worked with. From this standpoint, conclusions will be drawn to gain a broad view towards Swedish corporations. These conclusions will be validated and corroborated by interviews (e.g. qualitative data) to provide context and support in interpretation.

The **interpretivist** research paradigm of this study underlines the experience of a person and contextualises the interpretation of situations (Henning, van Rensburg, & Smit, 2004). In the way that this research project is conducted, the opinions of several experts are gathered and analysed. Hence, based on the underlying paradigm, it is recognised that the reality is subjective and gets influenced by the participants' perception of a regarded phenomenon (Ponterotto, 2005). In congruence with this subjectivity, the study asks for the perception of participants towards key aspects of GDPR compliance in Sweden. This will be conducted in a structured way, grounded by theory, to increase the credibility of the research. The quality of this approach and its limitations are discussed in chapter 3.5.

3.2 Research approach

The research goal of this study is **not** to replicate previous studies and assess their results in regard to compliance challenges. This research ought to be more specific than that. Currently, compliance towards this new regulation is managed as a project with a clear end-goal: *compliance*. This means that organisational processes need to be monitored and evaluated in order to improve its compliance-seeking activities. It is, in particular, the challenge of continuous compliance which Billgren and Ekman (2017) found in their study as an obstacle

to compliance as a sub-challenge of organisational compliance, as I have described in chapter 2.6. Compliance itself is not enough; its efficiency, expressed by its process maturity, is key to sustainable maintainability of the attained status. This is connected to financial issues in which compliance is considered a business risk that ought to be mitigated to achieve a residual risk below the risk appetite threshold (Brotby, 2010).

There are two main research approaches that can be viewed as capable of acquiring new knowledge in a particular field – **inductive** and **deductive** (Lee & Lings, 2008). From these, the deductive approach builds upon a theory from which hypotheses can be formulated that need to be tested in the research, whereas induction utilises the opposite approach and starts with general observations about the world which terminates in the generation of a new theory (Lee & Lings, 2008). Another way is a combination of both, as Morgan (2007) writes, **abductive** reasoning can be used as a less rigid way of doing research which is in particular useful in mixed methods research. Abduction is a is a logical reasoning to a possible explanation without guaranteeing the conclusion which leaves several explanations open for consideration (Feilzer, 2009). This differs from deduction in a way that the conclusion is not consequential since the underlying assumptions are not solid, but merely gives us orientation. Sober (2013, p. 28) defines abduction as "inference to the best explanation".

The decision to conduct **abductive** research is grounded on the fact that this thesis builds on the identified research gap of Billgren and Ekman (2017) who have conducted their research **only inductively** with qualitative methods. Abduction is a reasoning process in research which alternates between the inductive and deductive research approach (Morgan, 2007). To construct a more specific picture of compliance mechanisms, abduction was chosen as the way to analyse the data by moving between the different data sets that contain a variation of knowledge which must be brought together to interpret it multidimensionally (Feilzer, 2009). This enhances the explanations found in this mixed methods approach by a wider range of data. Hence, this study intends to make statements based on qualitative and quantitative data about selected key aspects in terms of GDPR compliance and draws conclusions about the development of those with regards to future compliance capabilities.

Every study has a research purpose that determines the method and approach the study must be conducted. As Saunders et al. (2016) describe, there are three main categories of purposes – exploratory, explanatory and descriptive. Exploratory studies are mainly conducted to examine a problem by observing its current reality without specific hypothesis (Porta, Greenland, & Last, 2008). Explanatory studies try to explain a certain phenomenon and may primarily ask for 'why' and 'how' and are hence building upon the knowledge generated from exploratory research which produces general knowledge about a topic (Porta et al., 2008). This may increase relevance and utility of the research for society to seek for practical answers to real-world problems and may include analysis of the causal mechanisms of a phenomenon (Recker, 2013). In descriptive studies, the mere status is interesting to the researcher without taking into account any causal relationships due to which the status is as it is (Porta et al., 2008). Those studies mainly describe the current state and construct a baseline from which further research can be conducted. Since the aim of this research is to investigate compliance mechanisms and how well they are applied to achieve GDPR compliance, this study is a combination of **descriptive and explanatory research** as it intends to describe and explain the situation about key aspects in GDPR compliance in Swedish corporations by underlying their governance maturity of information security. Thus, due to a vast amount of literature, the research approach was not chosen to be exploratory as knowledge in this regard is already prevalent. To increase the relevance of the study and utilise the point in time this study is conducted, the descriptive/explanatory approach seemed most reasonable to produce relevant research. By utilising the descriptive power of a survey and the explanatory power of

interviews, the mixed methods approach has the potential to satisfy the descriptive and explanatory purpose of this study. This is in alignment with the research approach of the study which is adopting the **abductive** approach by combining **deduction** and **induction** (Figure 3-1 Research approach). It utilises the theory gained from the theoretical framework to conduct the survey which approaches the **descriptive** research purpose from a **deductive** standpoint by using **quantitative** methods. The **inductive** part is elicited from the semi-structured interviews which tries to enhance theory in the **explanatory** purpose of the study. Hence, it must be stated that this study is not trying to generate a new theory, rather to enhance the theory by utilising methods related to its **abductive** approach.

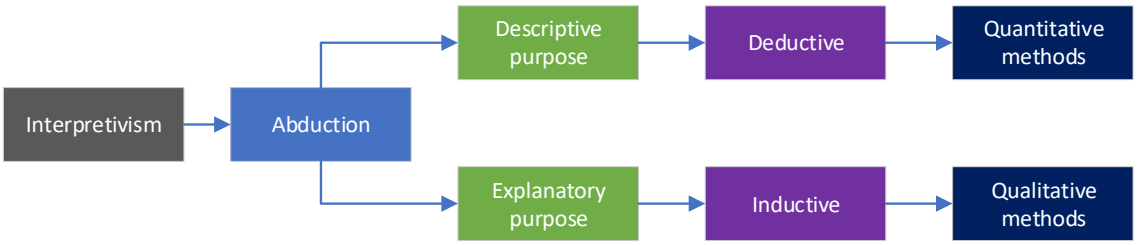

Figure 3-1 Research approach

3.3 Research design

Throughout the history of scientific research, a variety of research strategies was developed which could be utilised to bring the theory of research into action (Saunders et al., 2016). To bring the method into practical realisation, **sequentially applied mixed methods** were chosen to serve as the methodology of this study.

Figure 3-2 visualises the research flow in its entirety. From the initial problem statement, a literature review was conducted to frame based on the purpose of the study the research questions that ought to be answered. The detailed literature review of the topic gives insights into the current knowledge and research which is already done in this field. Based on the research purpose, GDPR key aspects were selected which were allocated in the structure of the

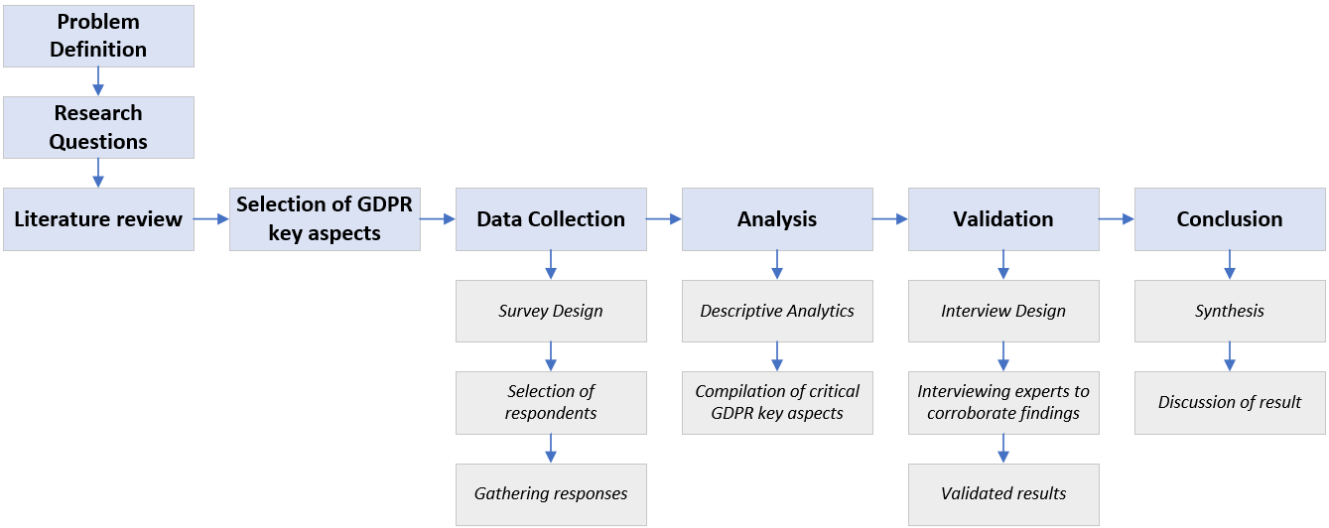

Figure 3-2 Research Flow Overview

survey as the primary tool of data collection. The analysis happens by **descriptive analytics** which concludes with **preliminary results** that will be validated and corroborated with expert interviews for which a semi-structured interview questionnaire is designed. The final result

gets discussed together with the applied research method and its limitations at the end of this thesis.

3.3.1 Literature review

A literature review was conducted as the first step in the thesis to identify research gaps and potential research opportunities in the field of GDPR compliance. As Easterby-Smith, Thorpe, and Jackson (2015) mention, a review which is based on the researchers opinion of the relevance of found literature is called a **traditional literature review**. The review enabled a placement in literature of GDPR compliance practices, mechanisms and potential issues which usually arise. The goal was to identify key areas which are supposed to be crucial for being compliant with a data privacy regulation, in particular GDPR. The knowledge gained was used in the creation of the survey and the subsequent interview guide. In order to find a good base of articles and other literature, I used databases which are accessible via JIBS, like DIVA, Scopus, Google Scholar and Primo, but also EUR-Lex as the database of the European Union. The main keywords to search were: *data protection, privacy, IT compliance, organisational compliance, GDPR, privacy regulations, information security, IT security*. These keywords were partly also combined with Boolean operators to widen the spectrum of findable articles. The aim was to find a large base of peer-reviewed articles, but also institutional documents about the regulation like EC-proposals and research papers from the European Commission and Parliament. Since the topic of GDPR is very new and the regulation being adopted since January 2016, the articles in this thesis are also very new and barely older than 5 years. The GDPR had a long preparation phase and a lot of literature was produced in this timeframe to improve the EC-proposals for the regulation. In addition, published material from ISACA and other organisations was used to complement academic articles to also gain a practical view on compliance and GDPR.

As a result, the conducted literature review enabled the formulation of a well-defined research problem, guidance towards applicable theory for the study and a reasonable selection of GDPR key aspects which are regarded in this research.

3.3.2 Survey design

In alignment with the deductive research approach of the quantitative method, a theoretical model guides the creation of the survey questionnaire which is designed based on the theory described in the theoretical background. It is not intended to form a valid construct, instead assess specific aspects of GDPR compliance in Sweden which were chosen based on current literature and the interest of the author. These aspects will be assessed in a well-defined structure and are put into **five** sections to easier visualise their place in GDPR compliance activities and mechanisms. **Later, these sections will be filled with parts of theoretical models in which specific controls and processes are**. In the following, I will explain each section and its theoretical foundation:

First and foremost, the requirements of a new regulation must be discovered and assessed to what extent it is applicable towards the organisation. Afterwards, each safeguard must be evaluated based on risk to which extent it needs implementation (Pereira & da Silva, 2013; Roessing & ISACA GDPR Working Group, 2018). The first section is named '**discover**' as it targets the discovery of personal data inside an organisation and to what extent its security is already regarded in the current strategy. The section aims to investigate all major GDPR requirements that tackle the eight rights of the data subject supported by the undertaken risk assessments to reduce duplication of work and unnecessary costs.

Figure 3-3 Sections of the survey (own development based on the knowledge gathered in the literature review – each section has a theoretical grounding explained in the chapter)

Billgren and Ekman (2017) state that continuous compliance with the regulation is a considerable challenge. This implies issues in monitoring like a widespread lack of internal controls and internal audit. Management and IT governance are major factors that determine the success of compliance efforts as Vicente and da Silva (2011) state in their GRC model. Governance evaluates, directs and monitors the activities towards a particular goal. Thus, the section '**manage**' was chosen to represent it.

The appropriate response to the risks related to personal data is to '**protect**' them in the most appropriate way. This protection is part of the GDPR requirements even when the regulation is not technical; it requests "*appropriate protection*" (GDPR foreword 72) which implies a risk approach. Protection must happen on the one hand proactively with safeguards (e.g. proactive controls), but on the other hand reactively to have processes in place to react to incidents such as data breaches. As for that, two sections ought to produce results to make statements about certain compliance aspects: '**protect'** and '**react'**.

The last section entails the level of education and awareness of employees. As Vicente and da Silva (2011) state, communication is a crucial component of policy enforcement. Communication creates awareness which supports compliance activities in this regard. Hence, the level of awareness and communicated knowledge among employees was chosen as the fifth section: '**educate**'.

Allocation of a theoretical model into the survey structure

After the sections of the survey were decided, a theoretical model is put into this frame under which the survey questions will be designed. Since GDPR implementation projects usually work in different workstreams to organise the project next to the general timeline in which it operates (Roessing & ISACA GDPR Working Group, 2018, p. 22), a more complete picture can be drawn from this standpoint. These different workstreams can be drawn implicitly from the regulation itself by categorising all major articles in the regulation which require implementation of individual strategies, controls, monitoring, capabilities and awareness. I have allocated these workstreams which were developed by Roessing and ISACA GDPR Working Group (2018) under the sections that I have chosen to structure the survey to visualise the connection between the sections and the way companies try to achieve GDPR compliance.

Allocation of specific controls and processes into each GDPR workstream

In each section of the survey, I regard several aspects of GDPR compliance in relation to cyber and information security. This must be done systematically. Therefore, the *CIS Critical Security Controls for Effective Cyber Defence* (Center for Internet Security, 2016) are used as

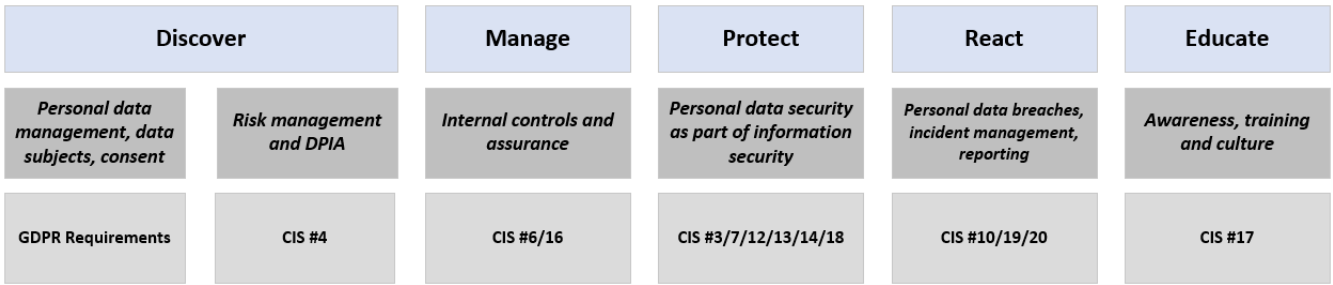

Figure 3-4 Structure of the survey and representation of the selected controls relevant for this research

a structure to build several questions which shall give answers for the compliance aspects that I am looking at for this study. Figure 3-4 represents the overall structure of the survey and mentions the controls which were selected. As described in chapter 2.3, Table 2-1 shows the 20 control categories in which information security can be framed. Each of these categories entails a number of controls that ensure well-defined information and cyber security inside an organisation. These control categories are more focused on technical network security, rather than personal data protection. **Hence, not all controls are interesting for this study. Only controls that are useful to give conclusions for the purpose of this study were chosen in this context**. The selected control categories were associated with each workstream to obtain a better structure for the survey.

Table 3-1 and Table 3-2 show the entire structure of the survey in table format in which all chosen controls are listed. The way of data collection happens in survey format which gets discussed in the next chapter.[1]

Table 3-1 Survey content structure (part 1)

Section	Code	Workstream and CIS Controls
Discover	A	*Personal data management, data subjects, consent*
	A1	Data inventory creation and tracing its location
	A2	Analysis if the reason and purpose of collecting specific data is legally valid
	A3	Implementing data portability of user data in common format (preferred automized)
	A4	Privacy policy enforcement (data protection according to its sensitivity and usage as intended)
	A5	Implementing a procedure to enable users to give and establish consent
	A6	Implementing a procedure to enable users to withdraw consent
	A7	Data dispute handling (a user wants to change data)
	A8	Data completeness and accuracy (up-to-date)
	A9	Visually demonstrating compliance with GDPR to auditors
	B	*Risk management and DPIA*
	Critical Security Control #4: Continuous Vulnerability Assessment and Remediation	
	B1	Formalized process for Data Protection Impact Assessment
	B2	Formalized process for risk management in information security
	B3	Implemented Data Protection Officer with clear job description and education
	B4	Regular vulnerability scans run on the system and threat analysis
	B5	Patch management procedures incl. patch testing
Manage	C	*Internal controls and assurance*
	Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs	
	C1	Regular internal IT audits
	C2	Regular analysis of aggregated logs from multiple machines
	C3	Formalized change management procedures for information systems and their configurations
	Critical Security Control #16: Account Monitoring and Control	
	C4	Access control and authentication for employees
	C5	Regular account reviews (for employees and guests)
	C6	Multi-factor authentication for sensitive data and administrator accounts

[1] The survey can be also viewed under this link.

Table 3-2 Survey content structure (part 2)

Protect	D	***Personal data security as part of information security***
	Critical Security Control #3: Secure Configurations for Hardware and Software	
	D1	Process for secure hardware and software configuration management
	D2	System hardening processes
	D3	Security baselining process
	Critical Security Control #12: Boundary Defense	
	D4	Implementation of breach identification systems (e.g. IDS and others)
	D5	Firewall at perimeter
	D6	Demilitarized zone (DMZ)
	Critical Security Control #13: Data Protection	
	D7	Implementation of DLP (Data loss prevention system)
	D8	Encryption or pseudonymization of databases with highly sensitive data
	D9	Data classification schemes to determine the level of protection
	Critical Security Control #14: Controlled Access Based on the Need to Know	
	D10	Proper access control on a need-to-know basis among employees for data viewing
	D11	Proper access control on a least privilege basis among employees for executing programs
	D12	Highly sensitive data is encrpted and requires secondary authentication mechanism
	Critical Security Control #18: Application Software Security	
	D13	End-to-end encryption for customer servicing portals
	D14	Server-side input validation for databases like SQL
React	E	***Personal data breaches, incident management, reporting***
	Critical Security Control #10: Data Recovery Capability	
	E1	Weekly backups to an alternate site
	E2	Secure physical storage space for backups
	E3	Backup encryption at rest
	E4	Regular testing of data restoration process
	Critical Security Control #19: Incident Response and Management	
	E5	Incident response plan
	E6	Disaster recovery plan
	E7	Business continuity plan
	Critical Security Control #20: Penetration Tests and Red Team Exercises	
	E8	Regular external and internal penetration tests are conducted
	E9	Regular testing of incident response plan (red team exercise)
Educate	F	***Awareness, training and culture***
	Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps	
	F1	Level of education of your Data Privacy Officer (DPO)
	F2	Level of awareness and education about data PRIVACY among internal employees
	F3	Level of awareness and education about CYBER THREATS among internal employees

The controls and processes will be evaluated based on their maturity level. The evaluation happens through questions in the survey questionnaire in which respondents will be asked to evaluate the current implementation state based on different scales.

For **each** process and control, **two** questions are asked: one main question about current implementation state/maturity level and one follow up question about difficulty/complication or state/maturity before the GDPR implementation projects in Sweden have started (e.g.

January 2016). This information shall bring the current state into perspective and gives the opportunity to build a ranking of implementation challenges. The maturity level is classified by the Capability Maturity Model (CMM) in six states from 0-5. This model is well-known in the field of IT governance as it classifies the current state of key processes and key practices in its efficiency and maturity. It was first developed by Watts Humphrey in 1987 and has emerged in various integrations and varieties over time (Daintith & Wright, 2008). The levels of process maturity are the following:

- Level 0 – non-existent
- Level 1 – initial/ad hoc process, rather unpredictable and reactive
- Level 2 – managed process on the project level
- Level 3 – defined process, rather proactive than reactive
- Level 4 – quantitatively managed and controlled
- Level 5 – optimised process, rather stable and flexible

The survey questionnaire can be viewed in 0. In overview, Table 3-3 gives a picture of the question types and their measurement scales of **perception**. In summary, it can be said that the questions aim to ask for how the majority of Swedish corporations have implemented the requirement. This information is given subjectively by the GDPR expert which reflects his/her opinion and experience.

Code	Workstream and CIS Controls	Question type main	Question type follow up
A	***Personal data management, data subjects, consent***	Likert scale 1-10 (state of implementation)	Likert scale 1-5 (level of difficulty/complication)
B	***Risk management and DPIA***	in CMM	CMM before GDPR
C	***Internal controls and assurance***		
	Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs	in CMM	CMM before GDPR
	Critical Security Control #16: Account Monitoring and Control	Likert scale 1-5	state before GDPR
D	***Personal data security as part of information security***		
	Critical Security Control #3: Secure Configurations for Hardware and Software	in CMM	CMM before GDPR
	Critical Security Control #12: Boundary Defense	Likert scale 1-5	state before GDPR
	Critical Security Control #13: Data Protection	Likert scale 1-5	state before GDPR
	Critical Security Control #14: Controlled Access Based on the Need to Know	Likert scale 1-5	state before GDPR
	Critical Security Control #18: Application Software Security	Likert scale 1-5	state before GDPR
E	***Personal data breaches, incident management, reporting***		
	Critical Security Control #10: Data Recovery Capability	Likert scale 1-5	state before GDPR
	Critical Security Control #19: Incident Response and Management	in CMM	CMM before GDPR
	Critical Security Control #20: Penetration Tests and Red Team Exercises	in CMM	CMM before GDPR
F	***Awareness, training and culture***		
	Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps	Likert scale 1-5	state before GDPR

Table 3-3 Question types for survey in each workstream and control category

3.3.3 Interview design

In accordance with the sequential design of mixed method which is adopted in this study, interviews are conducted to collect qualitative data.

The data collection with the survey which is based primarily on Likert scales and CMM evaluations as primary data collection method and serves as the quantitative investigation, while interviews are conducted with experts to corroborate the preliminary findings of the survey analysis. The purpose of conducting interviews as the qualitative method in this mixed methods approach is to gain information about the context in which companies are operating in their attempt to achieve compliance. Since the methods are used **sequentially** (first survey, second interviews), the interview guide could be created **after** a preliminary analysis of the

survey data had been made. This strategy enables the creation of an interview guide that asks very **narrow questions** that are relevant in order to corroborate the preliminary findings and enrich them with context. Hence, open topics were chosen for the questions which were left insufficiently answered by the survey alone. It reflects the abductive approach of this study which aims to build a more specific picture of compliance activities and processes. Still, the interviews should not be too stiff to not as this would lead to responses that might focus too much on a certain aspect. Therefore, the decision was made to **semi-structure** the interviews in order to balance the level of guidance with the freedom of response in an undefined way which can enrich the response by using **open-ended questions**. This enables the interviewee to state theses and make argumentation that justifies his/her opinion. Both is valuable information for this research and can be captured in this way. The interviews had approximately 7-10 questions. Some questions were asked to all interviewees to enable a comparison of different answers. Other questions were chosen based on the specific profile of an interviewee to gain details which could not have been gotten with other interviewees. The questions were not too stiff and allowed the respondent to give some examples which could justify and enrich their answer.

The questionnaire can be found in *Appendix* 8.5. The way in which interviewees were chosen is subject of the next chapter. The interviews are transcribed partially and focus on the parts of the speaker that is of main interest for the underlying study. A verbatim transcription is therefore not necessary. Next to the transcript, a quick summary was written by the author. It can be viewed in *Appendix* 8.5.

3.4 Research Strategy

3.4.1 Sampling and collection

Quantitative method - the survey

To achieve high quality in this research, it is necessary that people are chosen based on their experience with GDPR in various companies and not just in one. The selection of relevant individuals is key to be able to transfer the results to different scenarios. For the survey, this eliminated all GDPR project managers that focus on one company only. Needed are consultants that have seen many different companies and supported them in their implementation efforts. This approach is a **qualitative sampling method** as it is based on **self-selection** of respondents and highly subjective. Therefore, this self-selection needed to happen based on a pre-defined purpose that a respondent has for the study. Hence, **purposive sampling** was utilised. The following profile was considered suitable for these people being regarded eligible for this survey:

- Working as a GDPR specialised consultant in Swedish corporations.
- Has worked in this position for most of the time since January 2016.
- Experience and education in information security
- Experience in information governance
- If possible, certified as GDPR or data privacy expert.
- If possible, certified as CISSP, CISM or similar.

As each expert, based on his/her profile, has a holistic view of Swedish corporations, a certain sample size does not need to be attained. As not the companies themselves are asked in the survey, there is no way to generalise over the entirety of Swedish companies in a traditional sense. **The goal is to achieve a robust and holistic view of the current state of Swedish companies in several compliance aspects based on the views of experts who are working in this field.** The number of experts that was tried to achieve was **10**. The final number of answers in the survey is **12**. Section 3.5 discusses the research quality of this approach and goes in-depth regarding its descriptive power.

Qualitative method – the interviews

The interviews were conducted **sequentially after** the survey was analysed. For those, a narrower view was taken as their intention lies in corroborating the results and enriching them with context. Hence, the required profile for interview partners was widened, and people outside of Sweden were approached additionally. However, the focus remained in Sweden and two out of three interview partners were from a Swedish consulting background. The following people were interviewed, and questions were tailored towards their area of experience:

Table 3-4 Interview Partners

Name	Background
Lars Magnusson	Information security, CISSP certified, GDPR consultancy, security architecture, cloud security
Debbie Chong	US Attorney, CEO of Lenos Software (San Francisco), Privacy Expert
Alexander Hanff	CEO of ThinkPrivacy, Computer Scientist, CIPP/E certified Privacy Expert

Qualitative method – interview questions in online discussion forums

Some of the questions in the interview guide were posted on social media groups where GDPR experts discuss specific issues within the regulation. These groups were used to gather additional data for questionnaire items. *Appendix* 8.4 shows the questions and answers which could be gathered from these groups as an additional data source for qualitative data. The respondents were not self-selected, the only selection undertaken by the author was the selection of the discussion forum in which a question was posted. The questions were answered by people who self-committed to participate in the study after having been made aware in the posting that their answer will be used in a research project.

The way of finding respondents and interviewees

To gather the needed data for the study, a list of potential respondents for survey and interviews needed to be created based on the decided profile of people. This was accomplished by using **LinkedIn** which provides the advantage that experts can easily be found and checked if their experience fulfils the criteria. It also enables an easy way of contact. The primary way of communication was still email, as many addresses were published online on their company websites. In total, **63** experts were contacted from which **12** replied to the **survey**. For the **interview**, **7** people were contacted from which **3** have agreed to an interview.

3.4.2 Research ethics

Ethical rules need to be kept in each type of research. Otherwise, harm could inflict the participants of the study, but also the society as a whole (Easterby-Smith et al., 2015). Most important in this conducted research in terms of ethical concerns was the making of contact with potential survey participants, whereby several considerations were made.

The contact made with these experts was via a message which explained the study, its goal and in which way the data would be gathered. In this context, consent from each respondent was obtained by stating that the survey respondents would be treated anonymously, and no name would be published without their consent. *Appendix* 8.1 contains the text of the mail in which transparency was the guiding principle. This ensures the confidentiality of the data and provides privacy to the participants.

For the interviews and general collection of open-ended questions, LinkedIn and Facebook was used as the primary source. On several GDPR related groups, postings were made about a research project in this field to gather qualitative responses. To adhere to ethical rules, it was made clear in each posting that the answers given in the comment section or via personal message will be used in the study. The answers were treated anonymously in the study; therefore, names are not mentioned. The questions and responses can be viewed in *Appendix*

8.4 in their original text form. Only the interview partners are mentioned in the study after having received their consent that their names can be published.

3.5 Research quality

In the two ways of undertaking research, quantitative and qualitative, there are different quality concerns to consider. While quantitative research tries to achieve generalisability over a population as external validity and reliability to satisfy replicability of the study, qualitative research tries to achieve trustworthiness by satisfying criteria as **dependability**, **credibility, transferability and confirmability** (Golafshani, 2003, p. 600) based on the construct of Guba (1981). This reflects the aim of validity and reliability in quantitative research with the aim of qualitative research to achieve *trustworthiness*, *rigour* and *quality* in research (Golafshani, 2003, p. 604). Since this study was conducted by mixed methods while probabilistic representativeness was not tried to achieve, the quality criteria for qualitative studies were considered to fit best for this approach.

3.5.1 Dependability

By the underlying theory of knowledge of social constructivism, the study respects the notion that the real world is under constant change. Hence, the study focussed on gaining an understanding of GDPR key aspects at the beginning of the transition period in January 2016 and of now. The results will change if the study is replicated since the environment has changed. Nevertheless, the replicability of the study has to be ensured to fulfil the requirement of **dependability** which means that the results have to be consistent (Easterby-Smith et al., 2015). The chapter about the methodology ensures this by outlining the entire process of data collection. The regarded aspects are listed, the measurement scales are described, and the profile of the respondents is clearly explained, this makes it possible to repeat the study at any given time to produce *consistent* results at a later point in time which can be compared with the results of this study. Dependability can be seen as the concept that frames the reliability of a result in a qualitative study (Lincoln & Guba, 1985). Since reliability is mainly a measurement of the quality of quantitative studies, it still needs to be somehow considered to evaluate the quality of qualitative research (Golafshani, 2003).

3.5.2 Credibility

In alignment with my interpretivist paradigm, I acknowledge that there is no single truth and all respondents in the survey and interview partners have a different view on reality. In accordance to Lincoln and Guba (1985), **credibility** can be used as a validity criterium in qualitative research which describes the neutrality of the author towards interpreting the results. To assure credibility of the research, it is necessary to stay as neutral as possible as the researcher to avoid any bias. All survey questions were formulated from a neutral stance not to influence the perception of the respondent. They were clearly outlined and sorted in a way that was understandable and consistent to make it easy for the respondent to comprehend the concept of the questionnaire. To test the credibility of the results, general questions were asked to see if their results correspond to the results of more specific questions. This has been the case as the analysis chapter outlines and underlined the credibility of the results. In addition to the survey, interviews with selected GDPR experts were conducted to corroborate the results of the survey. This supports the findings with additional data and enhances the insights of the results. By gathering data from multiple sources (survey, interviews), methodological triangulation could help to increase the credibility of the study. Even though it is subject to discussion, if methodological triangulation can achieve a higher value of validity (King & Horrocks, 2010), I argue that especially the conducted interviews due to its semi-structured

form reduced the authors bias as the interviewees could speak more freely. In this regard, I see triangulation as a potent tool to cross-verify data from several sources to corroborate findings. Since the conducted study follows a mixed methods approach, a better picture of obstacles and challenges of GDPR could be drawn and higher credibility of the results achieved.

3.5.3 Transferability

The goal of this research is to provide an aggregated holistic view about several aspects of GDPR implementation inside of Sweden by experts working in this field. In this regard, generalisability in the form of **transferability** of the result to a different context needs to be considered (Lincoln & Guba, 1985; Smith, 2017). Calder, Phillips, and Tybout (1982) state in their article about 'external validity', that generalisation is in general two-fold: on the one hand as "*effect generalisability*" and on the other hand as "*theory generalisability*". As for the first, this can be considered as the classical approach to this quality characteristic in quantitative research. It intends to find a suitable sample that allows for extrapolation to its population in a representative-probabilistic manner. For this, the sample needs to fulfil the criteria for representativeness with adequate sample size and well-done sampling to a certain extent. As for the second, a suitable sample is not necessary, since, in studies which focus on gaining a general comprehension of a topic, a small sample with relevant individuals is good enough to provide generalisability in this regard (Calder et al., 1982). As for the underlying study, the targeted definition is '*theory generalisability'* in the form of *transferability*. The sampling method is utilising *purposive sampling*. Hence, the study aims to gain a *general understanding* of a topic by analysing the views of people that have a holistic view of it. It averages the opinions of all respondents who provide their view of reality in the survey to capture the aggregated view of field-level experts in GDPR who are relevant individuals that can lay down their view. The question is if their view of reality which they have gained throughout numerous companies is transferable to other companies in Sweden. I argue that this is the case since the way of gathering the information from respondents was structured in a way to obtain their *subjective* opinion throughout a multitude of security controls and processes concerning their status by consistent Likert scales. Also, the results were validated by interviews with experts that support the results and provide additional insights. This is in accordance with the interpretivist research paradigm underlying this study in which it recognises the multitude of interpretations of the reality in different contexts. Hence, a probabilistic generalisability cannot be adopted by this research, but a *transferability* of their viewpoints towards the 46 security controls and processes in other company environments is applicable. As the assumption underlying this research is epistemologically seen constructivist, I argue that the reality in this field is constructed and subjective. Hence, to grasp multiple realities, averaging the values of subjective results is a justifiable way to gain transferability of these values to different settings.

3.5.4 Confirmability

In order to be confident that the findings of the study derived from the collected datasets, **confirmability**, as a quality criterium has to be considered to avoid any bias by the author (Easterby-Smith et al., 2015; Lincoln & Guba, 1985). Objectivity in science can best be achieved when the instruments that were used are independent of human perception (Patton, 1990). To achieve a highest possible confirmability, an approach called "*audit trail*" was applied in which the research was outlined in all individual steps to increase transparency (Shenton, 2004, p. 72). This is in particular critical in the creation of the questionnaire itself. As this tool was created by a human, it might be subject to bias. The survey results are not capable of bias as it provides numerical values, but the decision of what to put into the survey could reflect the author's predispositions. To avoid this bias, the entire flow of survey creation

and for the interview questionnaire was depicted to highlight an objective way of creation. Thus, confirmability could be achieved in the highest possible way and enables the reader to evaluate it based on the transparency of the chain of thought.

4. Results and analysis

The following chapter gives the results of the conducted survey and analyses them based on the purpose of the study. Several highlights are described in detail, while the rest is visualised for better understanding. It presents all major findings based on the gathered primary and secondary data of the survey.

The results were gathered by a survey and interviews and analysed based on the research questions asked in the beginning. The survey can be found in the *appendix* under 0. As described in the method chapter, the goal of the survey is to look at key aspects of GDPR requirements. Hence, the chapter about the result will present and analyse these aspects and bring them into perspective. The data was primarily scored using the Likert scale as a measure of perception by respondents with a relevant profile to answer the questions. The interviews validate and corroborate the results and enrich them with context and further information. The transcripts for the interviews with Lars Magnusson, Debbie Chong and Alexander Hanff can be found in *Appendix* 8.5., and for questions posted on social media groups in *Appendix* 8.4.

4.1 Current state and implementation issues in Sweden

4.1.1 Current state

Based on the selected aspects used for this study, one can get a holistic view of the current situation in Swedish corporations in this regard. The survey was divided into five key sections that included key controls and their implementation state at the moment and at the beginning of the transition period for GDPR implementation in January 2016. Based on the opinion of experts in the field, *Appendix* 8.3.1 shows the overall implementation status in percent of full implementation of controls and processes in each section.

One can see that the implementation state is relatively low in the last months before the

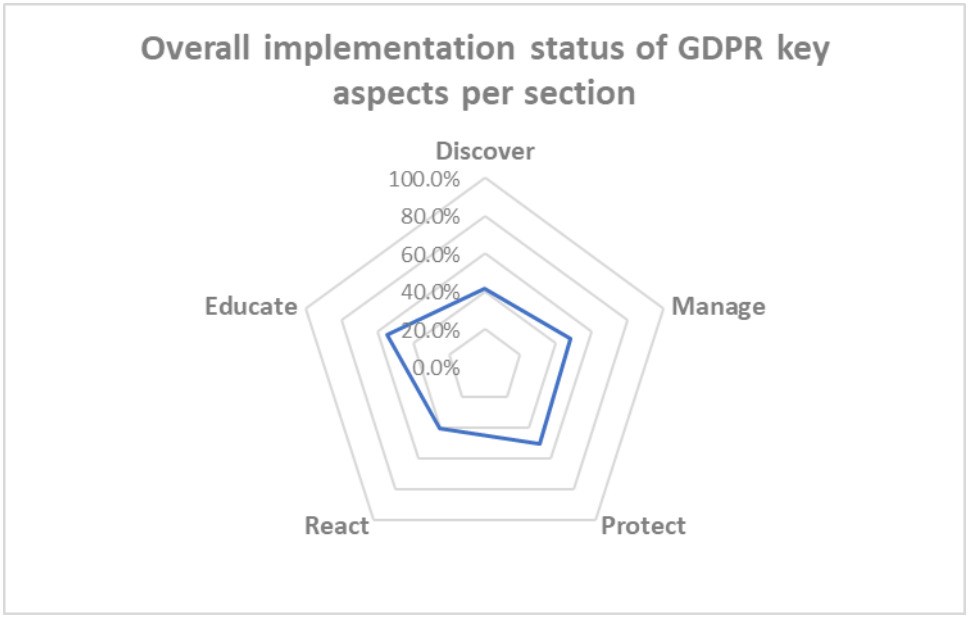

Figure 4-1 Overall result of implementation status in GDPR

regulation gets enforced. *Appendix* 8.3.1 shows the numerical results. Overall can be seen that the implementation of key aspects is rather low and varies around 50%, whereby incident management has the lowest rating with 40% and "Awareness, training and culture" have the highest with 55%. These ratings show low implementation progress across all sections. The

percentages are taken by the assumption that only the highest level of maturity is enough to comply with GDPR. This is not necessarily the case, even lower values can comply with GDPR but on a lower basis in terms of efficiency. It is difficult to set a level which is the minimum for compliance as it is profoundly subjective and does not live up to the reality. To avoid this bias, a percentage of the maximum was used to visualise the situation. However, an answer from a GDPR group on social media towards the question which maturity is high enough for efficient compliance, the member meant that '4' is enough (response 1a in chapter 8.4). Debbie (Paragraph 16) thinks that protection of data in terms of information security is a major concern, in particular of suppliers that could be more vulnerable than themselves. Even though, it can be stated that technical challenges in terms of security are not the main concern, Alexander (P. 8) states that due to a lack of due diligence more severe issues can arise for example if a service provider is chosen from an American company that is not listed in "Privacy Shield".

In general, the perception of respondents was rather negative towards a successful GDPR compliance as soon as the regulation gets enforced – average value of 2.25 on a scale from 1-10 was the result on the respective question. In their perception, the current implementation state is on average 4.58 (scale 1-10), whereas the corporations themselves see themselves a bit higher (-> 5.58). It appears to the respondents that the privacy governance is of low efficiency, a value of 2.50 (scale 1-10) was observed in this question. Lars (P. 2) corroborates this view by stating his estimation that 80% of companies will "*have not done particularly much in regards to GDPR*". Concluding can be stated that the perception of the chosen respondents towards the Swedish GDPR readiness is rather low which might predict a variety of incorrect data handling cases in the future.

4.1.2 GDPR compliance capabilities

The first section of the questionnaire focussed on personal data management which is among the major requirement areas of the GDPR.

The general levels of implementation are rather low and range between 3.00 – 5.17 out of 10.

Personal data management, data subjects, consent	Implementation level now 1-10	Difficulty 1-5 (easy-hard)
Data inventory creation and tracing its location	4.83	3.83
Analysis if the reason and purpose of collecting specific data is legally valid	5.00	3.42
Implementing data portability of user data in common format (preferred automized)	3.00	3.75
Privacy policy enforcement (data protection according to its sensitivity and usage as intended)	5.17	3.50
Implementing a procedure to enable users to give and establish consent	4.75	3.25
Implementing a procedure to enable users to withdraw consent	4.17	3.75
Data dispute handling (a user wants to change data)	4.08	4.17
Data completeness and accuracy (up-to-date)	4.08	3.67
Visually demonstrating compliance with GDPR to auditors	3.41	4.00

Table 4-1 Workstream Personal data management results in section "Discover"

This shows a somewhat problematic state where, in particular, these new requirements that come with the regulation are still in progress of improvement. The lowest value is on **data portability** of user data which was considered as a difficult requirement of the GDPR. The result strengthens this view with a difficulty rating of 3.75 and shows that major problems seem to arise in areas where the regulation changes the status quo significantly which requires not only organisational but also technical changes. This is the case in **data accuracy** and **dispute handling** where the difficulty levels are rather high and implementation low. Still, it is expected that data portability will not be the main right that will be used by the consumer (Debbie P. 14), the **right to be forgotten** will have a stronger attractiveness. Hence, only a few

people might actually use their portability right. It remains to be seen in which way the right will be enabled as standardised models are still missing (Alexander, P. 12).

The organisational requirement of "*visually demonstrating compliance*" is among the most problematic areas. It is a key requirement to document all precautions taken. Lars (P. 4) states that the "documentation is too brittle" which makes it hard to perform a proper data mapping. His view corresponds to Debbie (P. 16) that SOX is similar to GDPR and companies that have been already subject to SOX have better documentation available that is useful for GDPR compliance. It shows that regulations increase information governance in an organisation. Still, it is very connected to the corporate culture and its business connection to data privacy which "permeates through the entire company" (Debbie, P. 2).

The question arises if there is a correlation between the implementation level and the perceived difficulty. It could be expected that a high level of difficulty could lead to a low implementation state which can be visualised with the data from the survey. Figure 4-2 plots the data in a scatter chart where one can see a slight correlation which is not good enough to argue based on the R^2 of 0.31. Still, one can see a high level of perceived difficulty in all requirement areas concerning personal data management.

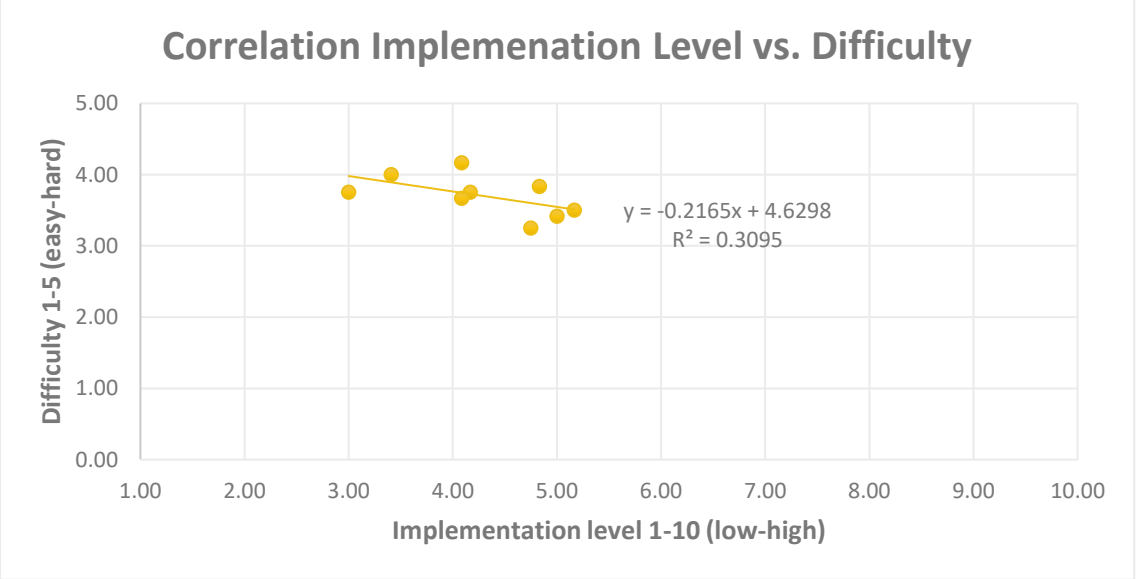

Figure 4-2 Correlation implementation level vs difficulty of personal data management requirements

This is in alignment as one respondent framed it in an open question of the survey that "*Sweden is far behind many other countries*" (paragraph 8.3.4). Even though other countries were not studied in this research, it can be stated that Sweden has rather low implementation levels in general and needs to improve its way of handling personal data. A possible explanation was given by Lars (P. 2) who sees the legal departments can be partly blamed as GDPR was treated as a new PUL law (e.g. the Swedish data privacy law before GDPR) which is mainly a legal issue without regulatory components as they exist in GDPR. Alexander (P. 10) also mentioned that particularly troublesome in Sweden is the availability of data about individuals which will not be compatible with GDPR and needs to change.

As expected, the **data portability requirement** (A3) has one of the lowest implementation rates which may be due to a lack of standardised models (Alexander, P. 12). This requirement is among the newest in the new regulation. Hence, it was expected that its implementation might lag behind. Whereas, the **analysis of reason and purpose of specific data collection** (A2) has a relatively high implementation state compared to other aspects. As this requirement was proposed by numerous GDPR guidelines to be the first step towards GDPR compliance, it

appears appalling that the level of implementation is not higher. The relatively low level of difficulty would assume a higher value would be easily achievable, but the most hindering problem is according to Lars (P. 4) the lack of documentation which makes a full analysis impossible in many corporations.

Overall, we can see a difficulty level of 3.7 out of 5 which points to the challenge the GDPR has posed since its inception. This results in low implementation rates by the end of the transition period.

4.1.3 Security processes and controls

The survey regarded controls and processes which were measured by similar but still different scales to respect the difference between a control and a process. Each process was put into a maturity level between 0-5 and each control into levels from 1-5. Hence, they are regarded separately in the result chapter to avoid any mathematical biases.

Starting with the regarded security processes, one can primarily see that most processes (Figure 8-3 in the *appendix*) range between maturity states of ad-hoc and managed. Among the best processes according to this study is **change management** with a CMM of 2.36 which indicates a managed process on the project level. This criterium has also seen a steady improvement since January 2016. Since regulations bring up new topics of concern, they pose a good exercise for change management (Lars, P. 18). Thus, the high improvement is not surprising, and it is likely that SOXed companies have seen a lower level of improvement than those that have been unregulated before.

The top 3 processes are connected to **incident response** (E5) and **regular log analysis** (C3). It is interesting to see that in CIS control #19, incident response was given the highest maturity, whereas the more complex processes for disaster recovery and business continuity were given a lower value. The latter received a value of 1.86 which is rather low and reflects Debbie's response (P. 12) that BCPs are usually too simple to function, whereas Alexander (P. 18) explained that most companies are utilising the cloud where providers take care of BCPs. Among the lowest maturities for processes can be seen in **penetration tests**, but this is mainly due to the nature of the process itself as it mainly gets outsourced to service providers. Problematic in the future could also be processes B1 and B3 concerning a formalised process for a **data protection impact assessment** and the clear implementation of a **data protection officer** which the GDPR both demands clearly. The maturity levels for these range at around 1.5. Still, it can be seen as a partial success as both levels were before under level 1 (at 0.83 and 0.92) which shows that it was at least tackled to a certain extent. As Debbie mentions in the interview (P. 10), **DPIAs** are actually not very difficult to conduct, since a variety of ready-to-use tools are available for free and do not require in-depth knowledge. Companies strive to seek the most cost-effective solution which might involve conducting DPIAs in-house, or if the complexity is higher, consulting firms may be engaged. This might explain the low level found in the survey as DPIAs had no real reason to be adopted as a defined process since they are sporadically conducted. This view corresponds with Alexander who mentioned that companies are striving for cost-efficiency and consultants who have done hundreds of analyses can provide a better result in less time (P. 16).

Among security controls, one can see that **perimeter firewalls** (D5) which protect internal networks through filtering malicious traffic are a well-established control in most businesses. This comes not surprisingly as it is rather easy to install the application and cheap in price. **Demilitarised zones** (D6) to protect the internal network from data streams of public-facing servers by filtering traffic through two firewalls (one at the perimeter and one at internal network perimeter) is also a common control and well implemented. Still, in CIS #12 where

these two controls are allocated, the implementation of **intrusion detection systems** (D4) lacks behind significantly which is worrisome in regard to GDPR which requires a fast identification of possible breaches. Information security is by all interviewees seen as a major concern which may be caused due to low funding as Lars states (P. 6) or simply by the prevalence of human error due to social engineering attacks (Alexander, P. 4). Only when companies start to realise that data loss costs money, the funding will eventually increase (Lars, P. 6). Alexander (P. 14) mentions that breach identification systems are generally high in costs, but most breaches actually happen by human error. So, for SMEs, a cheaper solution could be a clean-desk policy to reduce one of the major risks.

In the section "**protect**", the highest implementation value is in **application security** (CIS #18) where encryption and database protection play a crucial role. The lowest value is in CIS #3 about **secure configurations for hard- and software** where in particular the **baselining process** received a low level of maturity. This shows again that major concerns lie in documentation and organisational controls. Since the GDPR requires corporations to be able to "*demonstrate compliance*", this can be regarded as a weakness in Sweden. This view is backed up by Lars (P. 4) by stating that the level of documentation is not sufficient.

Among the strongest concerns are **the right to be forgotten** (officially the 'right to erasure') which may attract many people to request their right (Debbie, P. 14) really. The problem is rooted in technical issues of complete deletion by not affecting other data. Since overwriting does not guarantee a deletion, data media could need to be destroyed to comply (r. 3c in 9.4). Backups are also affected which are normally stored on older hard disks or even tapes that could cause trouble in deleting specific entries without affecting other data (r. 3ad in 9.4).

4.1.4 Implementation progress

Next to the mere levels of maturity in processes and controls, this study also gives an overview of the progress which was made since the inception of the regulation at the beginning of 2016. Figure 4-3 visualises the progression levels in processes and controls.

Overall can be stated that based on the survey result, all processes and controls which were

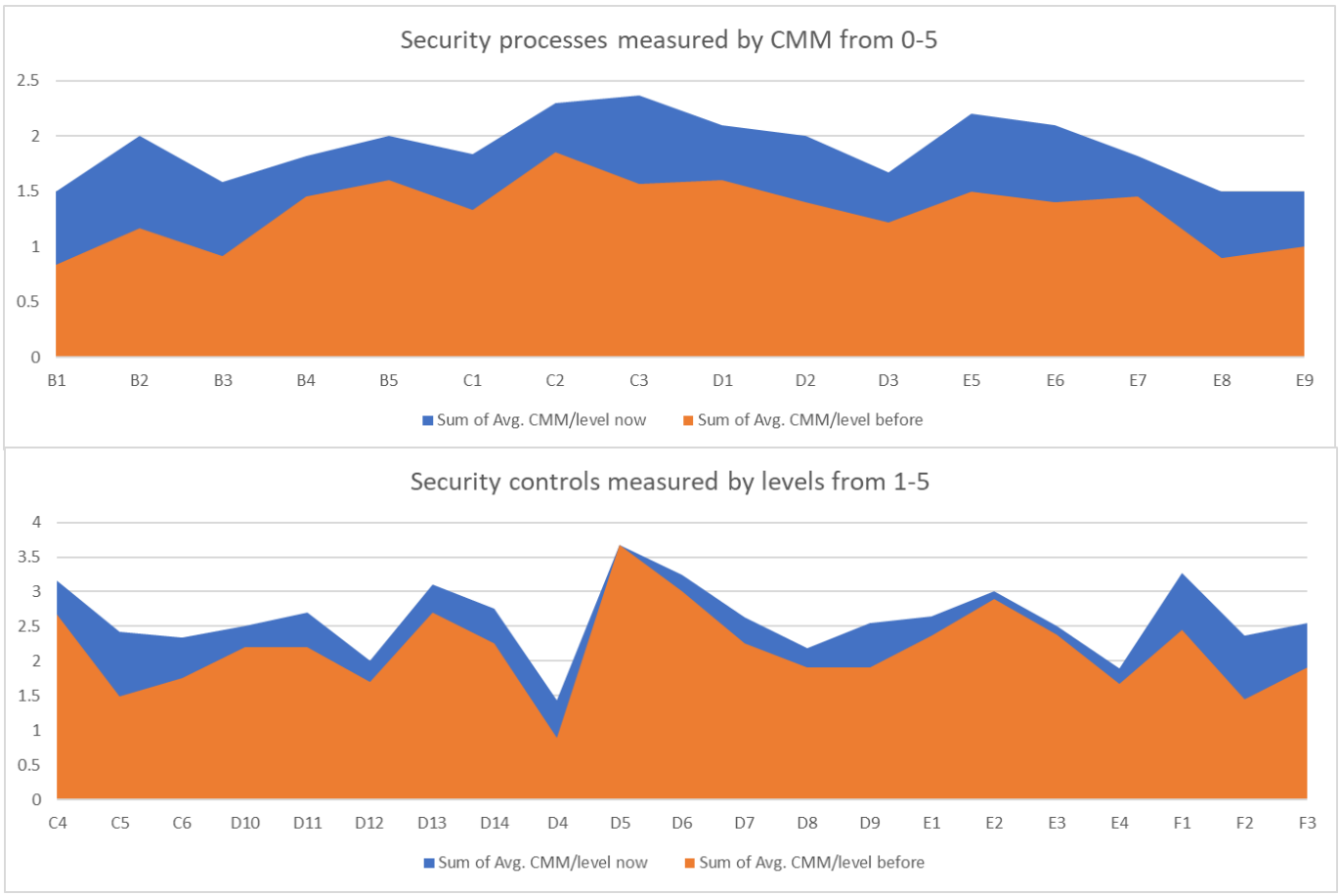

Figure 4-3 Progression of security controls and processes since January 2016

regarded in this research have improved at varying levels. Most of them which are affected by the GDPR in a greater extent, like **risk assessment** (B2), **regular account reviews** (C5), **data classification schemes** (D9) and **incident response** (E5) have progressed the most in maturity.

Process C3 about **change management** which is among the highest gainers of maturity among the aspects that were regarded for this research project is now one of the most efficient processes. This could indicate a general focus of companies towards formalised and well-documented processes as a result of compliance efforts for GDPR. This should not be confused with cause and effect but mentioned can be that the general security and privacy posture of Swedish corporations has improved over the last two years disregarded of what it may have caused, but the GDPR will have played a role in it with high likelihood. Alexander (P. 2) supports that view that changes in data governance had been made, but this does not mean that it is a direct effect from the regulation.

Risk assessments (B2) are a process which got elevated to a level of high importance by the GDPR due to its risk-based view. The regulation shows that its creators (e.g. EU Commission and Parliament) had a broad understanding of information security (Lars, P. 8) since the risk approach is the usual way. Nonetheless, Lars states that companies struggle with **efficient** and

continuous risk management (P. 10). The high improvement shows that companies have acknowledged their weaknesses and try to increase their level.

Controls for **identification of breaches** like IDS (D4) did not progress enough to live up the requirements of GDPR. Here a higher progression would have been expected, especially as data breaches regularly reach the public eye and result in a loss of reputation. Companies see that breaches happen which shifted the focus to incident response (Debbie, P. 12). Lars (P. 6) is fearing that if companies increase their level of proactive controls and encrypt data in storage and transfer, networking security could move in the background as a lack of competence and insufficient financial funding.

In CIS #17 concerning the skills and awareness of employees, we can also see a significant increase in particular about **data privacy** (F2), less about **cyber threats** (F3). The respondents also state that employees' knowledge is higher in cyber threats than in data privacy. This might seem odd at the first look but could be explained by the environment in which they work. For example, emails pose a considerable cyber threat in which most employees must engage every day, hence, their awareness of dangerous links and file attachments may explain this higher value.

4.1.5 Organisational vs technical changes

One of the major questions in terms of GDPR implementation is the differentiation between organisational and technical controls and how it affected their needed change towards compliance. One of the questions asked to rate the level of changes on a scale from 1-10 (technical – organisational), the result was a 6.67, indicating that change was more needed on an organisational level. This matches the observation of the level of changes of all controls/processes since January 2016 and interview answers.

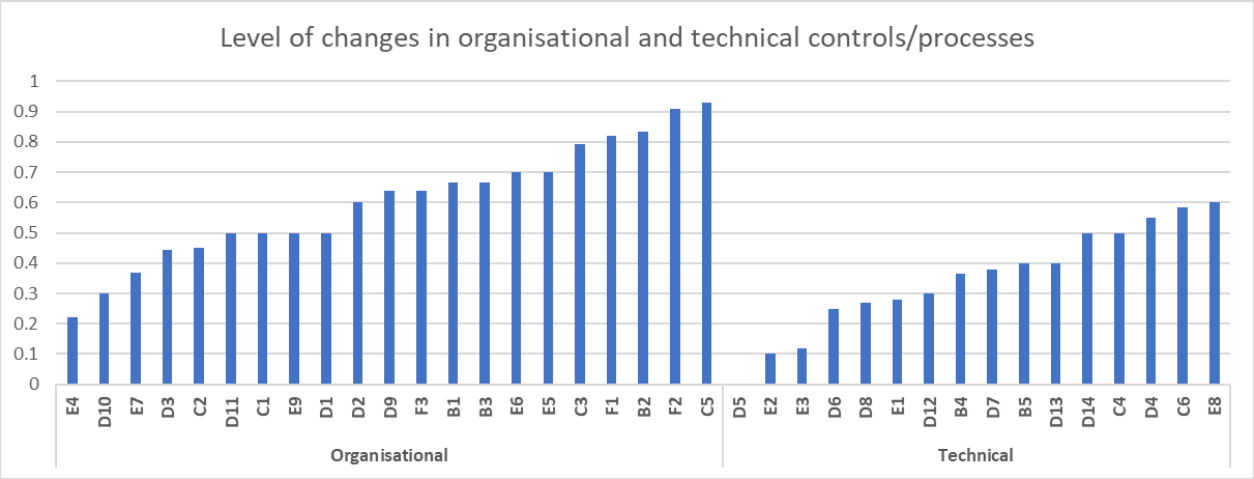

Figure 4-4 Change comparison of progression between organisational and technical controls

From all organisational controls, the average level of change is 0.6, whereas the average change of technical controls is merely 0.35. This matches the findings of Billgren & Ekman, 2017, p. 42, who found that most challenges in achieving GDPR compliance require organisational changes. Their study can now be appended by the results of the underlying study. The major changes in organisational controls were necessary for control C5 (e.g. **regular account reviews**) and the technical control E8 (e.g. **penetration tests**). Striking is as well the high level of change in control B2 (**risk assessment**) since this is a major requirement in GDPR which is a very prominent requirement. Also, as previously stated, control D4 (e.g. **breach identification**) has the third highest change by remaining at a low level of 1.44.

Concluding, the GDPR was intended to be a non-technical regulation that affects technical change. Its nature is organisational and leaves changes to be made on a risk basis. This points out that the effects were as intended by the EU, but it also shows that technical changes needed to be made as a consequence of organisational alterations. As Lars stated (P. 4), the regulatory components of the regulation affected companies' IT systems since GDPR is not like former data privacy laws (e.g. PUL in Sweden) but more analogous to SOX which affects business practices. Still, major mistakes are made since many do not look holistically at data privacy compliance (Alexander, P. 20). GDPR is not the only regulation to consider, many other laws and regulations (e.g. ePrivacy directive, national communication laws) are seen to be neglected.

4.2 Persistent compliance issues

Among the studied key aspects of GDPR compliance in this research, the following list gives an overview of processes and controls which need most attention by corporations to achieve compliance with the new regulation. Whereas chapter 4.1 provides a presentation of the result and analyses the responses in regards to privacy and security, chapter 4.2 presents the final analysis of the results.

Among the 46 security controls and processes which were regarded in this research, Table 4-2 shows the main obstacles and challenges that may remain insufficiently addressed in the future after the regulation is enforced. These issues are connected to several processes and controls that need to be in place and functioning efficiently to stay in compliance with the regulation, but also for future regulations that affect the business practices of corporations. The list selects the major concerns of GDPR compliance in most corporations in Sweden based on the analysis of the collected data. It shows the variety of issues the regulation causes, both in organisational as well as technical components. All of these issues have the possibility to persist for a longer time after GDPR gets enforced as it takes time to achieve a sufficient maturity in these aspects. As Lars (P. 14) stated, most organisations in Sweden have started working on GDPR too late and could now face problems in one or more of the highlighted findings in this study.

Table 4-2 Final findings in main obstacles and challenges

Issue	Reason
Breach identification	High level of improvement since January 2016, but still on a shallow level. In particular, SMEs face problems to identify breaches timely.
Security baselining	Low level of implementation and low progress made. A consistent security baseline enables continuous compliance and supports the level of documentation and demonstrating compliance. Since this process is of low maturity, continuous compliance may be endangered.
Information governance	Despite progress made, a more fluid translation from the top (corporate governance) to bottom is necessary. This includes a defined risk management strategy which, despite progress made, is still at level 2.
Lack of documentation	Hinders corporations to fully map their data collections and will persist for the long-term future. Old information is lost forever; now it is crucial to build a documentation structure that continues.
Network security	Low improvement of secure hard- and software configurations and boundary defence with stagnation at level 3. It may also lack focus due to a resource shift to superficial GDPR compliance activities like gathering consent. A threat lies in potential negligence.

Full data deletion capabilities	High level of difficulty and requires technical solutions to automate the process to be applied to all storage media while not affecting other data.
DPOs with clear job description	Both major requirements with low implementation values despite strong improvements since January 2016.

5. Conclusion

This chapter reflects the research purpose and concludes the results of the study with the most relevant findings by answering the research questions.

This study aimed to provide a more precise picture of compliance activities and mechanisms in Swedish corporations in order to close a gap in GDPR compliance research. Since this regulation is of high importance to companies that process data from EU citizens, this research proved to be relevant in this field. The purpose of the study was to look into key aspects of the implementation of GDPR requirements in Swedish corporations and how those are applied to comply with the new regulation. This includes a prospect of compliance mechanisms that may remain insufficiently addressed when the regulation comes into force on May 25, 2018. By adopting **mixed methods** with a **abductive approach**, the study has provided insights into the perceived implementation status of the GDPR in Swedish corporations by experts working in this field by utilising a **survey** and **semi-structured interviews**. It analyses key aspects of GDPR compliance for which security controls and processes were allocated to measure the perception of maturity and how they are applied. This was achieved by the usage of the CIS control framework (Center for Internet Security, 2016) and ISACA's GDPR workstreams (Roessing & ISACA GDPR Working Group, 2018) to structure the survey to gain insights in the selected key aspects. Those insights were utilised to design interview questions that analyse the findings more profoundly and corroborate the results.

Response to the research questions

The introduction of this thesis has outlined two research questions that ought to be answered by this study:

Response to RQ1: *How well are key aspects of GDPR implementation in Swedish corporations applied and how have they evolved since January 2016?*

Overall, a low level of maturity can be shown in most security processes and controls. Swedish corporations have treated the new regulation mostly in an inadequate way without seeing the bigger picture of GDPR and its full extent. Still, all regarded processes and controls have seen an improvement at a varying degree from which the most prominent ones have evolved the most. This shows a siloed approach in which separate systems are made compliant without a coherent, holistic strategy for the corporation.

Response to RQ2: *What are the compliance obstacles and challenges that may remain insufficiently addressed by adequate processes and controls by May 25?*

The following points compile the obstacles and challenges that may remain inadequately addressed for a more extended time period. Table 4-2 in the previous chapter explains each of those:

- Breach identification
- Security baselining
- Information governance
- Lack of documentation
- Network security
- Full data deletion capabilities
- DPOs with clear job description

Compiled are issues that have shown incapacities of companies that are difficult to develop overnight. It shows that obstacles mainly lie in the past (lack of documentation, low information governance in unregulated businesses) and will accompany them for quite a while in the future.

Concluding remarks

The results have shown that the current rate of implementation is meagre, and most corporations might not be ready by May 25. It was demonstrated that the perceived difficulty of all major GDPR requirements is quite high, in particular when deep changes have to be undertaken to fulfil them. The low level of documentation poses a problem which could be observed in the survey as it shows that most changes needed to be performed on the organisational level rather than the technical one. As the regulation requires active demonstration with requirements, this could lead to negative audit findings in the future. Most security processes have received a capability maturity level of around '2' which indicates a mere managed process on the project level rather than a defined process which would increase efficiency in privacy governance and flexibility for new regulations that might be upcoming. An example would be the ePrivacy regulation which is forthcoming as a current proposal of the European Commission to repeal the well-known "cookie-directive" from 2002 (European Commission, 2017) as a complementary regulation to the GDPR. It could be shown that mainly processes have improved that were prominently highlighted like risk assessments and DPIAs while others have seen only minor improvements. As the regulation was treated in Sweden more like a legal issue than a regulatory one, many companies have started to work on GDPR too late in the transition and could now face problems. The necessary information governance enabling a quick adoption the regulation was mainly existent in companies that have already been regulated by SOX and PCI-DSS. Other companies needed to adopt many new processes and elevate their existing ones to keep up with the new requirements. It is also important to see that even though the regulation intended to have more organisational components, it poses considerable challenges in the technical realisation of the 'right to be forgotten (erasure)'.

Despite the negative current state that could be found by this study, one can see progress towards the right direction in compliance. All security processes and controls have increased maturity in the perception of the asked experts. This may be the case since the regulation's importance was elevated to a rather high level by senior management as stated in one survey question (-> 6.55 out of 10). Senior management buy-in is vital to receive enough budget and fund the activities towards compliance (Brotby, 2010).

In conclusion, this study investigates the maturity of 46 security processes and controls based on the perception of GDPR experts working in the field. The majority of companies still have a good way to go to manage their personal data sufficiently to comply with this new far-reaching regulation. Since all regarded aspects of this study could show an increase in maturity, the status quo is in constant change and points towards higher process maturities in the future to enable better compliance activities.

6. Discussion

In this chapter, the results are discussed concerning their implications towards practice and research. Furthermore, it includes a discussion on the research method and its limitations, as well as proposals for future research projects in the field of GDPR compliance and data privacy policy making.

6.1 Results discussion

The study was undertaken during the transition period of the GDPR until it gets enforced from May 25. Hence, the findings show the compliance mechanisms concerning security controls and processes regarding their implementation stages at the latest stage of this time frame. Through the identification of persistent compliance issues, this study intended to investigate them regarding GDPR compliance to compile those that might remain problematic after the regulation will be enforced.

In contrast to the study from Billgren and Ekman (2017), the conducted research provides a more precise picture into compliance activities and mechanisms and closes the gap that so far existed. Similar to Billgren and Ekman, this study concludes that continuous compliance is an issue since the information governance has not yet increased significantly, but this will take years to achieve. Contrary, this study has analyses 46 specific controls and processes based on the opinion of GDPR consultants which enhances the view into the problem areas. Notably, certain technical challenges cause complications in the compliance process. Since the regulation is not only a legal framework but entails regulatory components, the implementation of 'full deletion capabilities' and 'breach identification systems' causes technical obstacles. Still, most implications are of organisational nature which affects major processes which were more profoundly investigated by this study.

Implications for practice

The implications for practice are to consider organisational controls as a means to be prepared not only for this regulation but for others to come. It could be shown that the regulation achieved, as intended, to be non-technical while implicitly requiring technical solutions on a need-to-be basis grounded on risk assessments in each field. This makes the GDPR an excellent case study for far-reaching future regulations in the EU, not only in privacy but in general aspect that involves IT, which is nowadays basically everything.

The results of this study underline the importance of mature IT governance processes to organise the cyber defences and control the information security of large and small corporations. Due to the fast-changing environment in which businesses operate, flexibility is the key to success in adapting to changes in the regulatory situation. It not only reduces the risk of being subject to high fines but also increases the efficiency of compliance activities which leads to lower costs. Businesses should allocate more resources into information governance processes and acquire consultancy services that may support them in building efficient structures. The regulation itself can be handled in an ad-hoc manner, but this approach is highly inefficient and will merely end in a non-stop compliance implementation. Corporations should start to see the regulation holistically by understanding its purpose. A full comprehension will enable the creation of a more flexible information governance that may prevail until the next major regulation arrives.

Implications are not only attached to businesses, but also to the European Union as the regulatory authority that has created this regulation. As the study shows, the 'right to be forgotten (erasure)' is a significant concern for many companies due to the difficulty of its implementation towards an automated solution that finds the entirety of the stored data. It

shows the unpreparedness towards this requirement which created a higher demand for support in this field. Even though the EU published a multitude of guidelines that can be downloaded on the websites of national data protection institutions (in Sweden *www.datainspektionen.se/dataskyddsreformen/),* the implementation was not as good as it could have been expected. It shows that in key issues of any new regulation, a more in-depth research should be undertaken to identify in which areas regulatory subjects will be affected the most. This analysis may help not only in creating guidelines but strengthen the capability to **actively incite businesses** to tackle the most demanding fields **early** in the transition period. As the regulation was seen in Sweden more as a legal issue, it would have been desirable to present GDPR as a regulation which entails far-reaching regulatory components.

Implications for research

The study results may have effects to research in a way that it could guide through other compliance issues that are dependent on several of the controls and processes that were regarded in this research. The purpose of those controls is not to prepare solely for GDPR, but for all current and future regulations. By focussing on a clear alignment between compliance activities and regulation purpose, controls can be put more specifically into context. This opens implications for research as it could assess the **value of purpose alignment** and **compliance flexibility capabilities** and in which extent, they are connected to the general maturity of information governance of a corporation. Since this thesis converges the fields of IT compliance and data privacy, it enhances the body of knowledge in IT and corporate governance which connects to IS/IT risk management. While it does not provide any new framework, it identifies common implementation issues in GDPR which concern not only data privacy but corporate governance in its attempt to mitigate compliance risk. This allows further research in this area to create new theories about the root causes of these effects and their entanglement in a corporate environment. Therefore, the main theoretical contribution of this thesis lies in clarification of compliance activities that companies use in practice to abide to new rules and their efficiency in this process.

6.2 Method discussion

The method was chosen for this research based on criteria of feasibility and relevance to the issue. Hence, a delimitation was chosen that limits this research to an investigation of key aspects of the GDPR regulation of how it affects the implementation in Swedish corporations. This delimitation enabled narrower research but limits the results to only those aspects which deters a holistic view of other aspects were disregarded. It was attempted to filter the most relevant security controls and processes based on commonly accepted frameworks like the CIS controls and ISACA's GDPR workstreams to regard the most relevant ones. Even though it was part of the delimitations of the research, a holistic approach that includes the entirety of aspects would be desirable, but this would include dozens of forensic audits in corporations which fall under confidentiality. Due to this unfeasibility, this alternative approach by using mixed methods was chosen to attain similar capabilities. A single method approach would not have had the ability to fully gain confidence about the answering of the research question, in particular, since this study intends to be descriptive and explanatory. The quantitative method could satisfy the descriptive element, whereas the qualitative method the explanatory element. The result was the deeper understanding of GDPR compliance issues in Sweden and allowed a narrower view.

Limitations of the study

Since the research focussed on GDPR consultants and experts, it cannot generalise to the population in a probabilistic sense but achieves transferability in a general understanding

towards compliance practices in the 46 security controls and processes as this mixed method research intends. The full discussion about the transferability criterium was outlined in chapter 3.5.3. Due to the fact that the number of respondents of the survey is limited, a higher number would depict the view of GDPR consultants more credible. A higher number of interviews (up to 30-40) which would not go in-depth (e.g. superficial interviews) could also have the capability to compare different opinions and work out the prevailing opinion of the GDPR community. Same goes for the survey, a larger number of participants among experts could increase the accuracy of the picture. It also needs to be considered that the study only regarded 46 security processes and controls and not the entirety of the CIS controls. Hence, it cannot form a valid construct which could measure the full picture of compliance, this study merely forms a partial but narrow picture.

Strengths of the study

Since the study focussed on respondents who are working as GDPR consultants, it was possible to gain a less biased view. If GDPR implementation managers were asked, as this was the case in the Billgren and Ekman (2018) study, the respondents would have been affected by a confirmation bias since they only know their own environment from which they could be convinced to do things the right way. Consultants, on the other hand, can look from a holistic view since they have seen many different companies and their processes. This is a strength of this research. Additionally, by applying mixed methods, the study can serve as a replacement to a probabilistic study by focussing on relevance rather than representativeness. This is in particular true since the survey was very detailed and gives already by itself valuable insights. The interviews with experts support the findings of the study and enrich them with context by giving background information which increases the utility of the actual results.

6.3 Further research

The study revealed several critical obstacles and challenges that may affect the future compliance capability of companies in Sweden. As the study was undertaken in the last months before the regulation gets enforced, these issues still have the potential to be resolved to a certain degree, even though the results show that this will be difficult to achieve. Hence, as soon as the regulation comes into force, new research opportunities open up for future research.

First of all, the fines for non-compliance can lead to a high motivation in defence as soon as enforcement authorities ascertain critical issues which could lead to a financial and reputational loss. Tedious legal cases will emerge in the future which will reveal which security controls or processes have led to data breaches or compliance inconsistencies. These cases present the opportunity to **analyse case studies** of future breaches and their relation to information governance in the firm. A more precise picture could be drawn that builds upon the results of this study by narrowing it down to specific issues of either technical or organisational form that has led to a payment in fines. An example could be a change of a business practice that results in a new purpose for data usage than was actually communicated to the data subject. Due to a lack of proper documentation, a collection of renewed consent was not undertaken. This could be a **case study** that could investigate the **root cause** of this breach in compliance.

Secondly, after several years of enforcement, a study could investigate **holistically** which security controls and processes have caused penalties and which have caused data breaches. This information could help future policymakers in updating the GDPR or amending it with separate EU-directives to increase the cyber policies of the member state. For future experts in information security, such studies can support in improving standards and frameworks regarding those breaches to raise companies' cyber resilience and information governance.

Thirdly, a mere **monetary evaluation** can be made to assess the costs of actions taken towards compliance and the likelihood of fine payments. This kind of study could also be used to evaluate the cost-saving potential in well-conducted IT risk assessments which could lower compliance costs. The study could have vast influence in the way IT consulting firms price their services and how the EU calculates their fines to keep the motivation of companies to bother about compliance with data privacy.

7. References

Billgren, P., & Ekman, L. W. (2017). Compliance Challenges with the General Data Protection Regulation. Lund University, Lund.

Bonde, J.-P. (2009). *Consolidated reader-friendly edition of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) as amended by the Treaty of Lisbon (2007)* (2. ed.). [S.l.]: Foundation for EU Democracy.

Brotby, W. K. (2010). *CISM Review Manual: Certified information security manager*. Rolling Meadows (Ill.): ISACA.

Calder, B., Phillips, L., & Tybout, A. (1982). The concept of external validity. *Journal of Consumer Research*. (9.3), 240–244.

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: Essential for organizational accountability and strong business practices. *Identity in the Information Society*, *3*(2), 405–413. https://doi.org/10.1007/s12394-010-0053-z

Center for Internet Security. (2016). The CIS Critical Security Controls for Effective Cyber Defence Version 6.1. Retrieved from https://www.cisecurity.org/controls/

COSO. (2018). About us page. Retrieved from https://www.coso.org/Pages/aboutus.aspx

Regulation (EU) 2016/679, Council of the European Union 06/03/2016.

Daintith, J., & Wright, E. (2008). *A dictionary of computing* (6th ed. / [general editors: John Daintith, Edmund Wright]). Oxford: Oxford University Press.

Easterby-Smith, M., Thorpe, R., & Jackson, P. (2015). *Management and business research* (5th edition). Los Angeles: SAGE.

ENISA. (2014). Privacy and Data Protection by Design – from policy to engineering.

European Commission. (2012). *(final) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

European Commission (Ed.). *Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications): Eprivacy regulations.*

European Union Article 29 Data Protection Working Party. (2016). *Guidelines on Data Protection Officers ('DPOs')*. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Feilzer, M. (2009). Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm. *Journal of Mixed Methods Research*, *4*(1), 6–16. https://doi.org/10.1177/1558689809349691

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8(4),* 597–606.

Guba, E. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Communications and Technology*, *29*, 75–91.

Heimes, R. (2016). Global InfoSec and Breach Standards. *IEEE Security & Privacy*, *14*(5), 68–72. https://doi.org/10.1109/MSP.2016.90

Henning, E., van Rensburg, W., & Smit, B. (2004). *Finding your way in qualitative research*. Pretoria: Van Schaik.

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

Hert, P. de, Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2017). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*. Advance online publication. https://doi.org/10.1016/j.clsr.2017.10.003

Hert, P. de, Papakonstantinou, V., Wright, D., & Gutwirth, S. (2013). The proposed Regulation and the construction of a principles-driven system for individual data protection. *Innovation: The European Journal of Social Science Research*, *26*(1-2), 133–144. https://doi.org/10.1080/13511610.2013.734047

Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J. M., Mattern, F., Mitchell, J.,. . . Ikonomou, D. (Eds.). (2014). *Privacy Technologies and Policy*. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg.

ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise*. *Cobit 5*. Rolling Meadows, IL.: ISACA.

ISO/IEC 27000. *ISO 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. (ISO 27000:2016(E)). Switzerland: ISO.

ISO/IEC 27005. *ISO 27005 - Information technology — Security techniques — Information security risk management*. (ISO 27005:2011). Switzerland: ISO.

Förordning (2007:975) med instruktion för Datainspektionen, Justitiedepartementet 22.11.2017.

Karczewska, J. (2017). COBIT 5 and the GDPR. Retrieved from http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-the-gdpr.aspx

King, N., & Horrocks, C. (2010). *Interviews in qualitative research*. Los Angeles: SAGE.

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, *28*(2), 159–171. https://doi.org/10.1080/13600869.2013.801589

Lee, H. J., Yun, J. H., Yoon, H. S., & Lee, K. H. (2015). The Right to be Forgotten: Standard on Deleting the Exposed Personal Information on the Internet. In J. J. Park, I. Stojmenovic, H. Y. Jeong, & G. Yi (Eds.), *Lecture Notes in Electrical Engineering. Computer Science and its Applications* (Vol. 330, pp. 883–889). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-45402-2_125

Lee, N., & Lings, I. (2008). *Doing business research: A guide to theory and practice / Nick Lee ; with Ian Lings*. Los Angeles, London: SAGE.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. *The Blackwell Encyclopedia of Sociology*.

Marcut, M. (2017). *Crystalizing the EU digital policy: An exploration into the digital single market*. New York NY: Springer Berlin Heidelberg.

Metric Stream. (2017). *Decoding GDPR Roles and Responsibilities: Requirements for Data Processors, Data Controllers, and Protection officers.*

Morgan, D. L. (2007). Paradigms lost and pragmatism regained. *Journal of Mixed Methods Research, 1(1)*, 48–76.

NIST SP 800-53. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*: National Institute of Standards and Technology.

Osterman Research, Inc. (2017). A Practical Guide for GDPR Compliance: An Osterman Research White Paper. Retrieved from https://www.rsa.com/content/dam/pdfs/7-2017/A-Practical-Guide-for-GDPR-Compliance-Osterman-Research.pdf

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.): Thousand Oaks.

Pereira, R., & da Silva, M. M. (2013). IT Compliance Management Process Modeling Based on Best Practices Reference Models and Qualitative Data. In *2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops* (pp. 178–187). IEEE. https://doi.org/10.1109/EDOCW.2013.27

Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of counseling psychology, 52(2)*, 126.

Porta, M. S., Greenland, S., & Last, J. M. (2008). *A dictionary of epidemiology* (5th ed. / edited for the International Epidemiological Association by Miquel Porta associate editors Sander Greenland, John M. Last). New York, Oxford: Oxford University Press.

Raab, C., & Szekely, I. (2017). Data protection authorities and information technology. *Computer Law & Security Review*, *33*(4), 421–433. https://doi.org/10.1016/j.clsr.2017.05.002

Recker, J. (2013). *Scientific Research in Information Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg.

Roessing, R. von, & ISACA GDPR Working Group. (2018). *Implementing the General Data Protection Regulation*. Retrieved from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2018/Pages/ISACA-Releases-Guide-to-GDPR-Implementation-as-May-Deadline-Approaches.aspx

Sadeghi, A.-R. (2017). AI Industrial Complex: The Challenge of AI Ethics. *IEEE Security & Privacy*, *15*(5), 3–5. https://doi.org/10.1109/MSP.2017.3681049

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2016). *Research methods for business students*. Harlow, Essex, England: Pearson Education Limited.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Smith, B. (2017). Generalizability in qualitative research: Misunderstandings, opportunities and recommendations for the sport and exercise sciences. *Qualitative Research in Sport, Exercise and Health*, *10*(1), 137–149. https://doi.org/10.1080/2159676X.2017.1393221

Sober, E. (2013). *Core questions in philosophy: A text with readings* (6th ed.). Boston: Pearson Education.

Stewart, J. M., Chapple, M., & Gibson, D. (2015). *CISSP Certified Information Systems Security Professional Study Guide, 7th*: John Wiley & Sons.

Stibbe. (2017). Complying with the General Data Protection Regulation. Retrieved from https://www.stibbe.com/en/expertise/practiceareas/data-protection/general-data-protection-regulation/what-are-the-challenges

Team ITGP Privacy. (2016). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. Ely: IT Governance Publishing.

The European Parliament. (2018). *The European Parliament: Historical background - Fact sheet.*

Vicente, P., & da Silva, M. M. (2011). A Business Viewpoint for Integrated IT Governance, Risk and Compliance. In I. Staff (Ed.), *2011 7th IEEE World Congress on Services* (pp. 422–428). [Place of publication not identified]: IEEE. https://doi.org/10.1109/SERVICES.2011.62

Westin, A. (1967). Privacy and Freedom. *Washington and Lee Law Review, 25(1),* 166.

Wilhelm, E.-O. (2016). A brief History of the General Data Protection Regulation. Retrieved from https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

Wright, D. (2013). Making Privacy Impact Assessment More Effective. *The Information Society*, *29*(5), 307–315. https://doi.org/10.1080/01972243.2013.825687

Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8–11. https://doi.org/10.1016/S1353-4858(17)30060-0

8. Appendix

8.1 Contact Mail

Dear Mr./Mrs. xy,

I am a Master student at Jönköping University and currently researching the GDPR implementation status and current difficulties in Sweden for my final thesis. I have found your LinkedIn profile and seen that you are working as a GDPR consultant. For my research, I am looking for experts in the field of GDPR like you and would like to invite you to my study. The study consists of a questionnaire which takes approximately 10-15 minutes. The objective of my study is to assess the current state and the progress made by Swedish corporations during the GDPR transitioning period that ends in May 2018.

I am looking for respondents that have a holistic view on the GDPR efforts in Sweden to share their experiences and personal views. My goal is to put the views of several experts into a structured construct to analyse the current situation holistically. I do not intend to publish your name, you can respond to the survey anonymously. The survey asks based on a construct that shall measure the state and progress in GDPR and privacy governance in Sweden.

I would be pleased to receive a response from you to support my research. In case you have any colleagues that might be good respondents as well, I would be pleased if you could share my mail. You can contact me if you have any questions, either via mail or telephone. My LinkedIn profile is also linked in my signature.

The link below contains the survey. Your contribution will support the continuous effort of compliance with GDPR.

https://goo.gl/forms/KkDOIgfdS0l1lSd43

Thank you very much

8.2 Survey Questionnaire

The questionnaire can be viewed online via this link. Here a list of the questions inside the survey.

Current State of implementation

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

Do you agree with this statement? I am confident that most Swedish corporations will be compliant with GDPR once it comes into force.

How do you assess the current GDPR implementation state of most Swedish corporations?

How do you think that Swedish companies are assessing themselves at the moment regarding GDPR implementation?

Do you agree with this statement? Most Swedish companies have privacy governance and compliance processes in place that are efficient:

A - Personal data management, data subjects and consent

The following questions ask for the current state in this regard and for complications in implementing these requirements which you have seen that Swedish companies are facing.

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

A1 - Personal data inventory creation: How much of the personal data that companies store, collect and process is already identified?

A1 - How do you rate the level of difficulty/complications companies were/are still facing in implementing this requirement?

A2 - Identification of the "reason for data collection": How do you assess the identification process in Sweden?

A2 - Level of difficulty/complications?

A3 - In GDPR, data subjects have the right to receive their data in a machine-readable format, the "right to data portability". If a portability request is made, most Swedish companies have in place:

A3 - Level of difficulty/complications in implementing it?

A4 - Classification of personal data according to its sensitivity with appropriate protection accordingly. How confident are you about the implementation of this requirement?

A4 - Level of difficulty/complications?

A5 - The state of appropriate mechanisms for receiving and establishing consent from data subjects in Swedish companies?

A5 - Level of difficulty/complications?

A6 - To which extent is a mechanism for a user withdrawing consent deployed (preferred automatized)?

A6 - Level of difficulty/complications?

A7 - Data erasure capabilities of Swedish companies

A7 - Level of difficulty/complications?

A8 - Capability of keeping data up to date and deleted once contractual agreement is over?

A8 - Level of difficulty/complications?

A9 - Estimated percentage of companies that can "demonstrate" compliance with GDPR in case they get audited (level of formal documentation)?

A9 - Level of difficulty/complications?

B - Risk management and DPIA

This part asks for the maturity of processes in Risk management and procedures in data protection impact assessments (DPIA). The goal is to assess which extent, this might have improved during the GDPR transition period. For this, the Capability Maturity Model (CMM) is used. The picture below shows the model for reference purpose.

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

B1 - How do you classify the maturity in Swedish corporations regarding having established a formalized process for DPIA? For each question, please classify the maturity you see now and its development since January 2016. [Today]

B1 - How do you classify the maturity in Swedish corporations regarding having established a formalized process for DPIA? For each question, please classify the maturity you see now and its development since January 2016. [January 2016]

B2 - a Formalized process for risk management in information security: [Today]

B2 - Formalized process for risk management in information security: [January 2016]

B3 - Implemented Data Protection Officer with clear job description and education: [Today]

B3 - Implemented Data Protection Officer with clear job description and education: [January 2016]

B4 - Regular vulnerability scans run on the system and active threat analysis: [Today]

B4 - Regular vulnerability scans run on the system and active threat analysis: [January 2016]

B5 - Formalized patch management procedures incl. patch testing: [Today]

B5 - Formalized patch management procedures incl. patch testing: [January 2016]

C - Internal controls and assurance

This section asks for internal audit and other relevant controls for data protection monitoring and overview. Please answer, according to your own experience about Swedish corporations. The goal is again to see the current state and its development.

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

C1 - Regular internal IT audits: [Today]

C1 - Regular internal IT audits: [January 2016]

C2 - Regular analysis of aggregated logs from multiple machines: [Today]

C2 - Regular analysis of aggregated logs from multiple machines: [January 2016]

C3 - Formalized change management procedures for information systems and their configurations: [Today]

C3 - Formalized change management procedures for information systems and their configurations: [January 2016]

C4 - Status of appropriate access control and authentication for employees? [Today]

C4 - Status of appropriate access control and authentication for employees? [January 2016]

C5 - Status of regularly done account reviews (for employees and guests) to check for current access rights, etc.? [Today]

C5 - Status of regularly done account reviews (for employees and guests) to check for current access rights, etc.? [January 2016]

C6 - Status of multi-factor authentication for sensitive data and administrator accounts? [Today]

C6 - Status of multi-factor authentication for sensitive data and administrator accounts? [January 2016]

D - Personal data security as part of information security

This sector asks for security measures to protect information in regards to technical and organizational controls. It relates to the GDPR requirement of having "appropriate" safeguards in place. Please answer based on your personal experience with Swedish corporations. For each question, think how the majority has it implemented.

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

D1 - Process for secure hardware and software configuration management: [Today]

D1 - Process for secure hardware and software configuration management: [January 2016]

D2 - System hardening processes: [Today]

D2 - System hardening processes: [January 2016]

D3 - Security baselining process [Today]

D3 - Security baselining process [January 2016]

D4 - Implementation of breach identification systems (e.g. IDS and others): [Today]

D4 - Implementation of breach identification systems (e.g. IDS and others): [January 2016]

D5 - Firewall at perimeter: [Today]

D5 - Firewall at perimeter: [January 2016]

D6 - Demilitarized zone (DMZ) between perimeter and internal network: [Today]

D6 - Demilitarized zone (DMZ) between perimeter and internal network: [January 2016]

D7 - Implementation of DLP (Data loss prevention system): [Today]

D7 - Implementation of DLP (Data loss prevention system): [January 2016]

D8 - Encryption or pseudonymization of databases with highly sensitive data: [Today]

D8 - Encryption or pseudonymization of databases with highly sensitive data: [January 2016]

D9 - Data classification schemes to determine the level of protection: [Today]

D9 - Data classification schemes to determine the level of protection: [January 2016]

D10 - Proper access control on a need-to-know basis among employees for data viewing: [Today]

D10 - Proper access control on a need-to-know basis among employees for data viewing: [January 2016]

D11 - Proper access control on a least privilege basis among employees for executing programs: [Today]

D11 - Proper access control on a least privilege basis among employees for executing programs: [January 2016]

D12 - Highly sensitive data is encrypted and requires secondary authentication mechanism: [Today]

D12 - Highly sensitive data is encrypted and requires secondary authentication mechanism: [January 2016]

D13 - End-to-end encryption for customer servicing portals (e.g. SSL): [Today]

D13 - End-to-end encryption for customer servicing portals (e.g. SSL): [January 2016]

D14 - General application security for internet applications in regards to common attack vectors (SQL injection, XSS, session hijacking, etc.) [Today]

D14 - General application security for internet applications in regards to common attack vectors (SQL injection, XSS, session hijacking, etc.) [January 2016]

E - Personal data breaches, incident management, reporting

This section asks about incident response capabilities and breach reporting of Swedish corporations.

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

E1 - Backup management to alternate sites: [Today]

E1 - Backup management to alternate sites: [January 2016]

E2 - Secure physical storage space for backups (secure building and room): [Today]

E2 - Secure physical storage space for backups (secure building and room): [January 2016]

E3 - Backup encryption at rest: [Today]

E3 - Backup encryption at rest: [January 2016]

E4 - Regular testing of data restoration process: [Today]

E4 - Regular testing of data restoration process: [January 2016]

E5 - Incident response plan (overall capability to respond to disruptive events to minimize impacts and to restore normal operations): [Today]

E5 - Incident response plan (overall capability to respond to disruptive events to minimize impacts and to restore normal operations): [January 2016]

E6 - Disaster recovery plan (capability to restore operations in case of a disaster like floods, fire, earthquake that cause total or partial system collapse) [Today]

E6 - Disaster recovery plan (capability to restore operations in case of a disaster like floods, fire, earthquake that cause total or partial system collapse) [January 2016]

E7 - Business continuity plan (capability to maintain the most critical business functions in case of a disruption until normal operations are restored): [Today]

E7 - Business continuity plan (capability to maintain the most critical business functions in case of a disruption until normal operations are restored): [January 2016]

E8 - Regular external and internal penetration tests are conducted: [Today]

E8 - Regular external and internal penetration tests are conducted: [January 2016]

E9 - Regular testing of incident response plan (red team exercise): [Today]

E9 - Regular testing of incident response plan (red team exercise): [January 2016]

F - Awareness, training and culture

This short section asks for the security awareness of staff in Swedish companies. How do assess their level of education/awareness?

Please, try to answer as many questions as possible, but if you do not feel confident with some you can skip them!

F1 - The level of education/knowledge of Swedish Data Privacy Officers (DPO): [Today]

F1 - The level of education/knowledge of Swedish Data Privacy Officers (DPO): [January 2016]

F2 - Level of awareness and education about data PRIVACY among internal employees: [Today]

F2 - Level of awareness and education about data PRIVACY among internal employees: [January 2016]

F3 - Level of awareness and education about CYBER THREATS among internal employees (e.g. social engineering): [Today]

F3 - Level of awareness and education about CYBER THREATS among internal employees (e.g. social engineering): [January 2016]

Implementation issues/complications

This last section asks quickly for implementation issues.

Do you agree with this statement: In most Swedish corporations, the level of importance of GDPR implementation was elevated to the highest level by senior management?

The needed changes towards GDPR compliance in Sweden were more of technical or organizational nature?

If you want to add something or offer an explanation for GDPR situation in Sweden, here is some space for that.

8.3 Results – charts and tables

8.3.1 Overview results of expert survey

Section	Code	Workstream and CIS Controls	Results						Implementation Level per section
Discover	A	*Personal data management, data subjects, consent*	Implementation level now 1-10	Difficulty 1-5 (easy-hard)	Total Implementation Level		Total Difficulty Level		42%
	A1	Data inventory creation and tracing its location	4.83	3.83	4.28		3.70		
	A2	Analysis if the reason and purpose of collecting specific data is legally valid	5.00	3.42					
	A3	Implementing data portability of user data in common format (preferred automized)	3.00	3.75					
	A4	Privacy policy enforcement (data protection according to its sensitivity and usage as intended)	5.17	3.50					
	A5	Implementing a procedure to enable users to give and establish consent	4.75	3.25					
	A6	Implementing a procedure to enable users to withdraw consent	4.17	3.75					
	A7	Data dispute handling (a user wants to change data)	4.08	4.17					
	A8	Data completeness and accuracy (up-to-date)	4.08	3.67					
	A9	Visually demonstrating compliance with GDPR to auditors	3.41	4.00					
	B	*Risk management and DPIA*							
	Critical Security Control #4: Continuous Vulnerability Assessment and Remediation		CMM before	CMM now	*Change +/-*	Avg. CMM before	Avg. CMM now	Avg. +/-	
	B1	Formalized process for Data Protection Impact Assessment	0.83	1.50	*0.67*	1.19	1.78	*0.59*	
	B2	Formalized process for risk management in information security	1.17	2.00	*0.83*				
	B3	Implemented Data Protection Officer with clear job description and education	0.92	1.58	*0.67*				
	B4	Regular vulnerability scans run on the system and threat analysis	1.45	1.82	*0.36*				
	B5	Patch management procedures incl. patch testing	1.60	2.00	*0.40*				

Table 8-1 Overview of survey results per control / control group / section

Manage	C	*Internal controls and assurance*							48%
	Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs		CMM before	CMM now	*Change +/-*	**Avg. CMM before**	**Avg. CMM now**	**Avg. +/-**	
	C1	Regular internal IT audits	1.33	1.83	*0.50*	**1.58**	**2.17**	***0.58***	
	C2	Regular analysis of aggregated logs from multiple machines	1.85	2.30	*0.45*				
	C3	Formalized change management procedures for information systems and their configurations	1.57	2.36	*0.79*				
	Critical Security Control #16: Account Monitoring and Control		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	C4	Access control and authentication for employees	2.67	3.17	*0.50*	**1.97**	**2.64**	***0.67***	
	C5	Regular account reviews (for employees and guests)	1.49	2.42	*0.93*				
	C6	Multi-factor authentication for sensitive data and administrator accounts	1.75	2.33	*0.58*				
Protect	D	*Personal data security as part of information security*							50%
	Critical Security Control #3: Secure Configurations for Hardware and Software		CMM before	CMM now	*Change +/-*	**Avg. CMM before**	**Avg. CMM now**	**Avg. +/-**	
	D1	Process for secure hardware and software configuration management	1.60	2.10	*0.50*	**1.41**	**1.92**	***0.51***	
	D2	System hardening processes	1.40	2.00	*0.60*				
	D3	Security baselining process	1.22	1.67	*0.44*				
	Critical Security Control #12: Boundary Defense		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	D4	Implementation of breach identification systems (e.g. IDS and others)	0.89	1.44	*0.55*	**2.52**	**2.79**	***0.27***	
	D5	Firewall at perimeter	3.67	3.67	*0.00*				
	D6	Demilitarized zone (DMZ)	3.00	3.25	*0.25*				
	Critical Security Control #13: Data Protection		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	D7	Implementation of DLP (Data loss prevention system)	2.25	2.63	*0.38*	**2.02**	**2.45**	***0.43***	
	D8	Encryption or pseudonymization of databases with highly sensitive data	1.91	2.18	*0.27*				
	D9	Data classification schemes to determine the level of protection	1.91	2.55	*0.64*				
	Critical Security Control #14: Controlled Access Based on the Need to Know		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	D10	Proper access control on a need-to-know basis among employees for data viewing	2.20	2.50	*0.30*	**2.03**	**2.40**	***0.37***	
	D11	Proper access control on a least privilege basis among employees for executing programs	2.20	2.70	*0.50*				
	D12	Highly sensitive data is encrpted and requires secondary authentication mechanism	1.70	2.00	*0.30*				
	Critical Security Control #18: Application Software Security		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	D13	End-to-end encryption for customer servicing portals	2.70	3.10	*0.40*	**2.48**	**2.93**	***0.45***	
	D14	Server-side input validation for databases like SQL	2.25	2.75	*0.50*				

React	E	*Personal data breaches, incident management, reporting*							
	Critical Security Control #10: Data Recovery Capability		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	E1	Weekly backups to an alternate site	2.36	2.64	*0.28*	**2.33**	**2.51**	***0.18***	**40%**
	E2	Secure physical storage space for backups	2.90	3.00	*0.10*				
	E3	Backup encryption at rest	2.38	2.50	*0.12*				
	E4	Regular testing of data restoration process	1.67	1.89	*0.22*				
	Critical Security Control #19: Incident Response and Management		CMM before	CMM now	*Change +/-*	**Avg. CMM before**	**Avg. CMM now**	**Avg. +/-**	
	E5	Incident response plan	1.50	2.20	*0.70*	**1.45**	**2.04**	***0.59***	
	E6	Disaster recovery plan	1.40	2.10	*0.70*				
	E7	Business continuity plan	1.45	1.82	*0.37*				
	Critical Security Control #20: Penetration Tests and Red Team Exercises		CMM before	CMM now	*Change +/-*	**Avg. CMM before**	**Avg. CMM now**	**Avg. +/-**	
	E8	Regular external and internal penetration tests are conducted	0.90	1.50	*0.60*	**0.95**	**1.50**	***0.55***	
	E9	Regular testing of incident response plan (red team exercise)	1.00	1.50	*0.50*				
Educate	F	*Awareness, training and culture*							
	Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps		Level before	Level now	*Change +/-*	**Avg. level before**	**Avg. level now**	**Avg. +/-**	
	F1	Level of education of your Data Privacy Officer (DPO)	2.45	3.27	*0.82*	**1.94**	**2.73**	***0.79***	**55%**
	F2	Level of awareness and education about data PRIVACY among internal employees	1.45	2.36	*0.91*				
	F3	Level of awareness and education about CYBER THREATS among internal employees	1.91	2.55	*0.64*				

8.3.2 Charts – higher level control categories

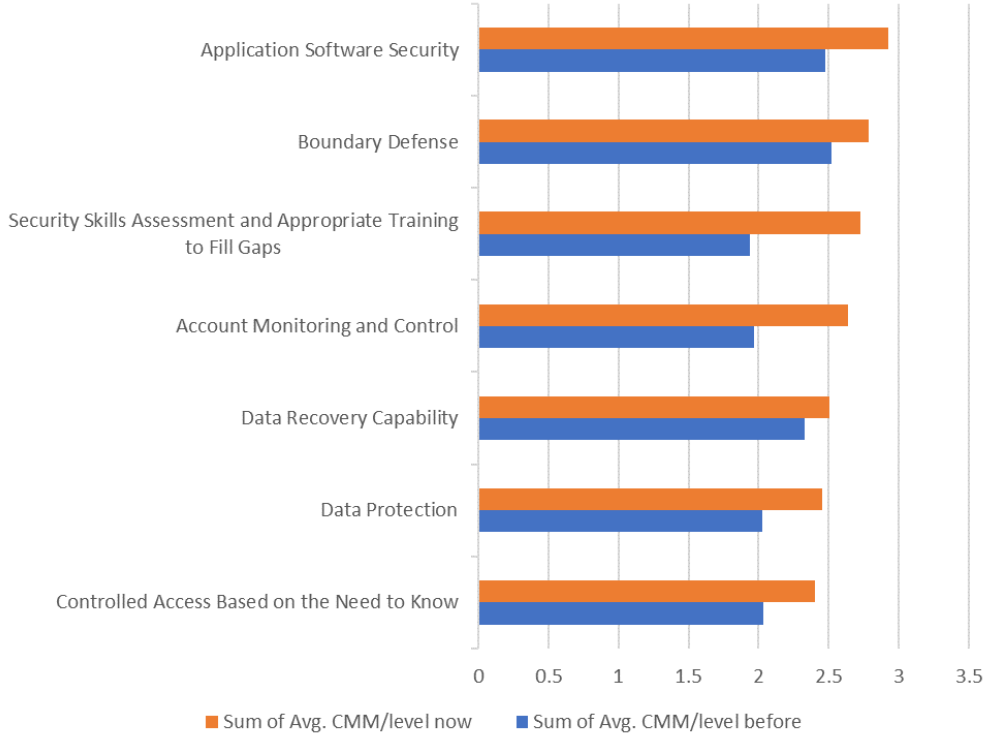

Figure 8-2 CIS Higher Level Control Categories measured by level 1-5 – sorted by current level

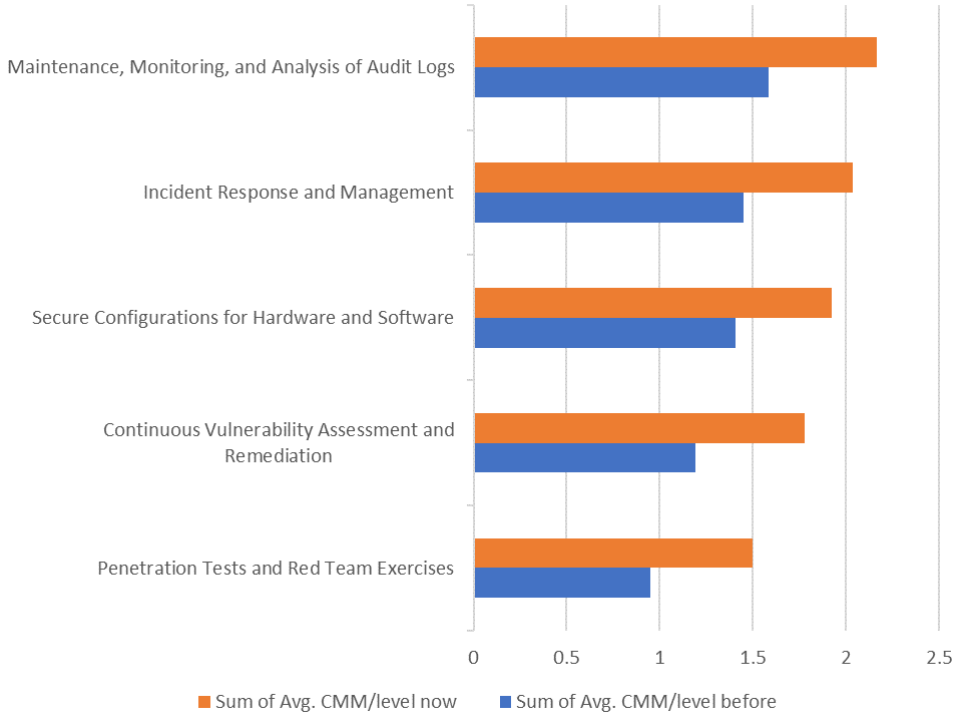

Figure 8-1 CIS Higher Level Control Categories measured by CMM 0-5 – sorted by current level

8.3.3 Charts – lower level processes and controls

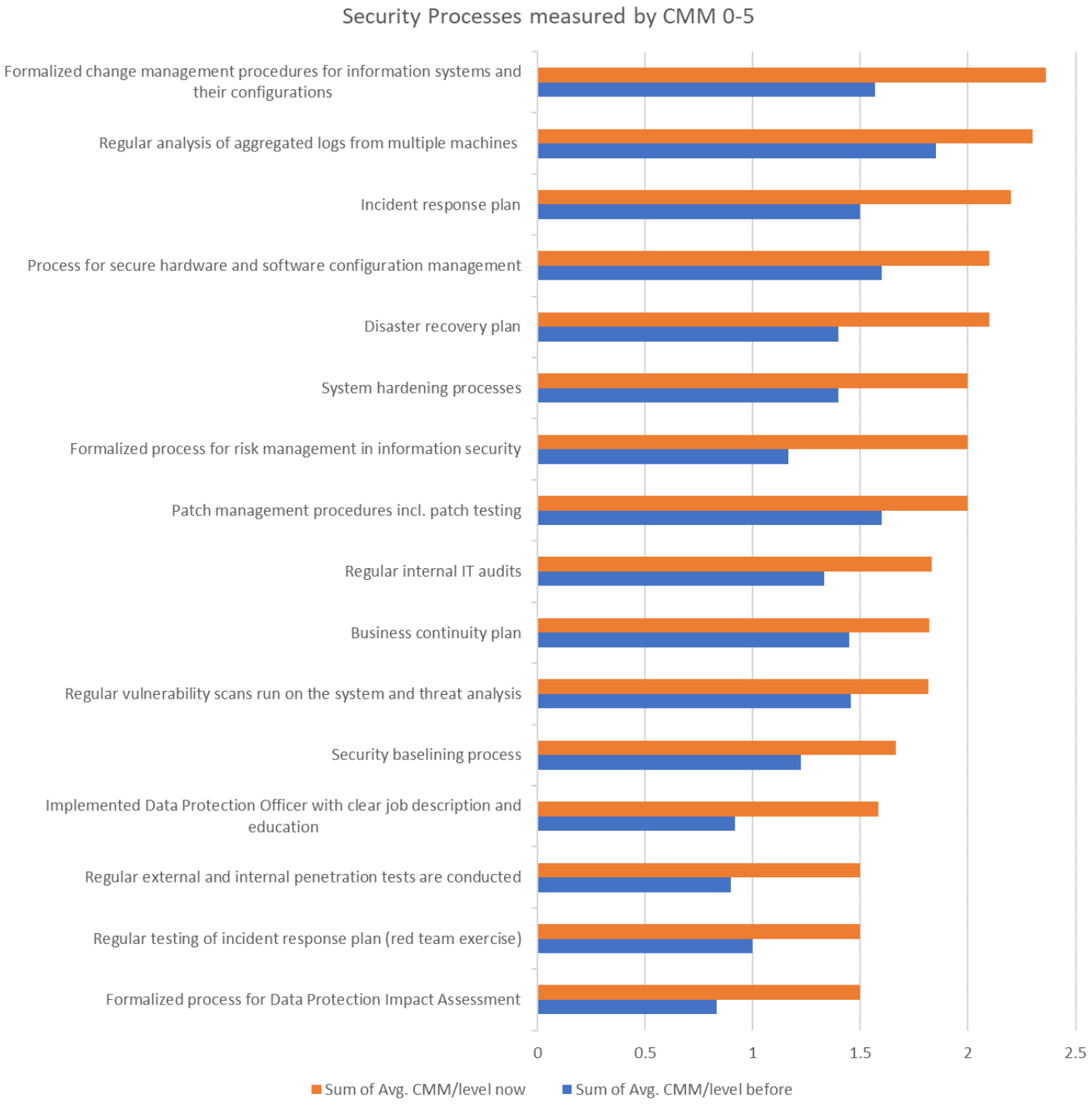

Figure 8-3 Result for security processes measured by CMM from 0-5 - sorted by CMM now

Figure 8-4 Result for security controls measured by levels from 1-5 - sorted by level now

8.3.4 Responses in text format

Two respondents have also provided a response in text form.

Respondent 1

Sweden has a culture of openness, public access to information and trust vis-a-vis governmental institutions. Hence, the public has until now not demanded much in terms of data privacy. (Example: the widespread use of "personnummer", which would be unthinkable in many other countries.) In short: Sweden is far behind many other countries. The introduction of GDPR has brought with it a significantly raised awareness among the public, employees and management (but notably starting from a very bad position).

Respondent 2

Very noticeable difference in GDPR readiness and security level between companies in different sectors.

Respondent 3

1. The organizational lawyers never understood that GDPR has a huge practical influence on the organization. Those I met and discussed with, have treated GDPR as another PUL, a pure legal issue. None of them have understood the practical implications of the law. Compared with US Sarbanes-Oxley Financial Act, which I worked with during 6 years, it is as day and night. The SOX:ed companies understood that SOX also was an audit framework, from the beginning. In Europe, all outside Germany and Austria has missed that fact and it will cost.
2. Most organizations have missed that it is both about penalties and punitive damages. It is not enough with maybe €20M in penalties, if 100.000 persons data is lost it can be €2-30.000 in punitive damages to each individual. 100.000 x €20.000 is €2KM. And even if public Swedish organization have a 90% rebate on the penalties, the punitive damages is not. They are 100% payable. GDPR will hurt and the money goes to EU, not the local government.

8.4 Interview questions and answers for social media groups

The following introduction text was used for postings on LinkedIn and Facebook groups to explain the that the answers will be used in the thesis.

Main text of the posting for LinkedIn groups:

Title of the posting: A GDPR research project needs you! What is your opinion on this question?

Give your opinion/statement about some of the questions below. If you are a GDPR implementor or consultant, your profile fits perfect! Please, use either the comment function (discussions are welcome) or write your answers to me personally via mail (sebastian.stauber@outlook.com). Your answers will be used in the research of a Master thesis for Jönköping University. Your responses will be treated anonymously in the study. In case you are willing to participate in a full skype interview, please inform me!

Main text for postings on Facebook groups:

<<<insert question>>>

I am trying to collect several answers to this question for my research project. Your answers will be used in the research of a Master thesis for Jönköping University. Your responses will be treated anonymously in the study. In case you are willing to participate in a full Skype interview, please inform me! Thank you!

Questions and answers

The following questions were posed in the postings, and following answers were given. The answers here are pasted in the same form as they were written by participants in the comment section of the social medium.

1. What capability maturity level (e.g. 0-5) of major GDPR connected processes would you consider high enough to have well enough defined and controlled processes in place that is fit to 'continuous compliance' with GDPR?
    a. *After a quick explanation to a group member what the question means, the member answered*: "If these are the "only" options, you must have "4" and then progress into "5". "3" is part of the Gap Analysis, therefore "the basis for everything". "2" doesn't seem logical when compared to "3". "0" is the current status :) and "1", it's the way most SME are doing it, yet it equals nothing and potentially means a "big mess"."

2. What do you see as the major complications that companies face when doing the analysis in which they try to figure out the "reason and purpose" of specific data collections?
    a. Not having someone who understand data and personal data in the company. Not having carried out a detailed data mapping.

b. From a very practical point of view, not having documented their processing ground, no data mapping to locate and retrieve data. They are a lot of confusion around consent, should they request re-consent?
c. Picking up and developing ... Data Governance is something that most companies do not have in an integrated and holistic manner (it is usually departmental). Assessing minimum required Data implies having in place a well-defined Service Catalogue and Data Flow + Data Map (so it comes down to defining the Data Governance model from the Service Catalogue (which mirrors the company Core Business). Then the need for having in place new Services and inherent workflows which assures Data Subjects rights (SAR, Opt-out, ... and so on). Lastly, but "the keystone" having Human Change Management which allows a smooth transition from establish habits (not aligned with GDPR requirements) towards new aligned and compliant MO. Hope it was useful...

3. What in your opinion is the most problematic concern regarding GDPR compliance in companies?
    a. The “right” to be forgotten” applied to back-ups.
    b. the biggest problem is the new consent for everything from everybody....
    c. From an IT perspective, I completely understand the backup issue. When an insurance company is asked to remove a person's personal information e.g. from a quote (that wasn't taken up) that record will have to be removed from numerous backup tapes / hard drives. The customer has say 20 days to take up and agree the quote, if they do that's fine, they consent to their data being used. If they don't then you have to get rid of everything, maybe up to 20 days’ worth of back up. Overwriting is not a clean deletion in some instances, only complete secure destruction will do. If a large number of people take up the right to be forgotten, this could potentially cause major issues for IT departments around the world.
    d. Having no right to privacy because of backups is a major issue as well. With a bit of time, everything will work fine. If businesses were not collecting totally useless data in the first place, or data consumers don't consent to give, their IT dept. would feel better. It's not only an IT issue IMO. The good part of GDPR is that it questions business practices and makes undesirable behaviours costlier. Data sobriety is a good thing, even (or especially) for IT depts.

4. The GDPR allowed a transition period of 2 years. In which compliance aspects do you see that businesses have improved the most and which do they lag behind? Why do you think this is the case?
    a. Negative: Not recognising that it applies to them and leaving it too late to realise that it does. Positive: Those that have embraced it I think have improved their identification and knowledge of exactly what personal data they hold / process and the controls and purposes around it. I think people lose sight over time.

b. I think that a lot of organizations have privacy policies, some of which provides rights similar to GDPR. This is an area of focus for most companies, because it is important to be transparent and to earn and retain the trust of customers, employees and partners. If there is trust, the data protection provided is shown by studies to be of a higher quality (Pew Research has a lot of papers that are in this area).

8.5 Interview guide and transcripts

1. In which extent do you see an improvement in information governance in companies and higher flexibility in adopting new regulations?
2. When doing the analysis in which companies try to figure out the "reason and purpose" of specific data collections, where do you see companies making the most mistakes? Meant by mistakes are issues that lead to incompleteness or inconsistencies.
3. Which 'security processes' will be most likely the downfall of 'continuous' GDPR compliance in corporations?
4. Was GDPR more technically challenging as companies have expected it to be? Which technical controls were hard to adopt? In which fields were technical changes higher than expected in the beginning?
5. Do you see a focus put on proactive controls (e.g. encryption, database security, authentication) than identifying controls (e.g. DLP, IDS)
6. In terms of incident response and management, which plan has seen the best implementation in the transition period – IRP, DRP, BCP? For which of these plans, companies ask for consulting the most often?
7. Do you think that DPIAs will mainly be outsourced to external providers or will companies try to adopt a well-defined process for it?
8. If the data portability right will mainly be used what do you think how companies will respond to the demands? Are companies mainly trying to solve the issue in-house or do they contract consulting firms to employ a technical solution to this issue?
9. How did the IT risk management processes in companies improve?
10. How do you see the situation in Sweden? Is there one problem that stands out in comparison to the other countries?
11. How is it with SMEs and data breach identification?
12. Did GDPR have any effects on BCP?

8.5.1 Interview Transcript - Lars Magnusson

Paragraph	Text	Summary
1	**Question**: In which extent do you see an improvement in information governance in companies and higher flexibility in adopting new regulations?	
2	If you look at your question, I would start how the readiness in Swedish organizations are regarding GDPR then I would say that it is catastrophic. At least 80% of all Swedish have not done particularly much in regards to GDPR, and in most cases, they have not understood what it basically entails. When we look at companies in the SOX and PCI environment. in these companies, there has been a regulatory understanding what GDPR might entail. The legal departments didn't understand that GDPR has a regulatory dimension and that is not just like the Swedish PUL which is the old Data Privacy Law in Sweden. PUL did not have the regulatory components which we have now in the GDPR. When the legal departments were trying to understand this old requirement, basically everything was ready, and no department needed to do anything, and this is the big mistake which the industry has made now with GDPR by thinking this is the same or at least similar.	Catastrophic, 80% of companies have not even understood what it implies, only some did more than in particular SOX, and PCI companies have a better understanding, no understanding that GDPR has regulatory components because PUL had no regulatory components
3	**Question:** When doing the analysis in which companies try to figure out the "reason and purpose" of specific data collections, where do you see companies making the most mistakes? Meant by mistakes are issues that lead to incompleteness or inconsistencies.	
4	They do not have the basic data to base their mapping on. What I see and what I was trying to do in my work is that documentation is brittle and basically detailed information is missing to do a valuable data mapping You need to remember SOX is similar to GDPR, so it is a direct analogue to GDPR. Based on my experience you can see the main problem of the GDPR, that there is no documentation which is sufficient to handle the mapping criteria and the database requirements. I asked customers that I worked with until I retired, and I asked them if they have all data connections documented and everyone said we don't know. It's mostly I can see that the most companies in Sweden at least 10 to 20% of communication is not documented. and therefore, they failed the data mapping the requirements of GDPR.	They don't have the basics; documentation is too brittle, SOX is similar to GDPR, you don't have any documentation that is sufficient to handle this analysis. The data connections are not documented, or they don't know.
5	**Question**: Which 'security processes' will be most likely the downfall of 'continuous' GDPR compliance in corporations?	
6	Financing the information security processes is maybe the biggest problem. A lot of companies are starting to understand that it costs money if you lose data and therefore, they will concentrate on I would say two things in my opinion: 1. Data encryption in storage and in the transfer, because SOXed companies have developed tools which are applicable to GDPR requirements.	Financing of cybersecurity processes is the most significant problem. Until the companies understand they lose money when they lose data. Then they will try to encrypt data in storage and transfer.

	What I am fearing is that other processes will move into the background. This, for example, might be networking security, of course, they do understand that networking is critical, but they don't have the competence, and they don't have the economy to put the right solutions into place.	
7	**Question:** Was GDPR more technically challenging as companies have expected it to be? Which technical controls were hard to adopt? In which fields were technical changes higher than expected in the beginning?	
8	It was definitely more challenging because they were thinking about it in the wrong way. I think the people who have developed in GDPR in the European Union had a good understanding of what they are doing because when I, as an information security manager, looking on GDPR, would say that this regulation is the best data Protection Law which was ever created. It is better than Sarbanes-Oxley, and I would say it is on par with PCI. I would say that a lot of corporations will try to remediate stuff that they should mitigate and that they should look from a helicopter point of view on their organization. It is better to have a globally integrated solution but having a separate and individual solution for each system. For example, it is better to look at the bigger picture and try to transfer data of higher sensitivity into Data networking areas which are more secure. Risk can be mitigated instead of remediating.	More challenging because they had expected because it was tackled wrongly. EU did not make the mistake; they had an understanding in terms of the driver for information security. Companies should start looking at the full picture. Risk-based perspective should be used, but risk management is not efficient
9	**Question**: Do you consider the risk assessment and management procedures of companies as sufficient and efficient?	
10	I haven't met any organization in my 35 years where the risk reviews and business continuity management has been efficient and sufficient.	
11	**Question**: In terms of incident response and management, which plan has seen the best implementation in the transition period – IRP, DRP, BCP?	
12	They are all on the same level because they don't receive sufficient funding. So, I would say it is a funding issue. It always has been a funding issue. I have talked with people from the executive level about these things and responses have been that they will do something when it has happened. The problem is, then it is too late. It does not touch the bottom line; they see it as an over-insuring the organization.	All are on the same level. Funding is the problem in Sweden. BCP is seen as over-insuring.
13	**Question**: For which of these plans, companies ask for consulting the most often?	
14	There was no real Consulting Market until January 2018. There have been only some consulting firms which have been doing GDPR consulting before with companies that have tackled the issue early on. This highly complicated issue was tackled too late.	Many organisations started to receive consulting late in the transition phase.
15	**Question**: Do you think that DPIAs will mainly be outsourced to external providers or will companies try to adopt a well-defined process for it in-house?	

16	I would say, they do not have any strategies yet, because they don't understand the problem context of this assessment. If you are a company, I would say that you are trying to find any possibilities in regards to outsourcing. If it is a government organization or Public Authority, they are trying to control it internally. I have a feeling that many company directors will say, let's outsource this that it becomes anyone else's problem, and they don't understand that they still own the problem, even though, they outsourced it.	Very few have a strategy yet. But companies will want it to be anyone else's problem.
17	**Question**: Do you see a focus put on proactive controls (e.g. encryption, database security, authentication) than identifying controls (e.g. DLP, IDS)	
18	I would answer this like this; when I worked with SOX, it was very visual, it was one of the key functions of SOX. But with GDPR everyone was hoping that it will just blow over, but this is stupid because we have remediation and control templates from SOX that show us how to handle this. This is no rocket science because we have what it needs from material on how to do a SOX remediation or PCI remediation. So, I would say, practically everything exists and is proven, but no one before January 2018 was doing anything.	There are control templates for SOX and PCI; it is no rocket science. The material does exist. He does not know any difference in improvement.
19	**Question**: Do you have any other thing that you consider important to tell me in this interview?	
20	As long as leadership does not understand the consequences and as long as the leadership does not understand the costs, it is not going to happen. It will be interesting to see what companies are going to be audited as soon as the regulation is in effect because then they will understand that it is heavily expensive. In particular, when they see that someone of their peer companies will have to pay a very high fine. The reason why nothing has happened so far is because of the concept of accountability is not understood by leadership. I would also say that the legal department is to blame for this because that department has seen it as a new PUL regulation as it has been in Sweden. As I have said in the beginning, PUL does not have any remediation or mitigation components; it is just a paper thing.	The concept of accountability is not understood. When peer companies have to pay a high fine, it will be standing on top of the agenda. Legal departments are to blame for this situation. They have seen it as a PUL replacement only.
21	Thank you for the interview!	

8.5.2 Interview Transcript – Debbie Chong

Paragraph	Text	Summary
1	**Question**: In which extent do you see an improvement in information governance in companies and higher flexibility in adopting new regulations?	
2	I think it is difficult because information governance comes from corporate governance which is developed by the executive board. And there it is lost in translation. It simply does not triple down from the top to the bottom. Even though, I think this has approved a lot, but it depends on the corporate culture. So for example, when you have a company like Salesforce, that company is always talking about trust and that it is hard to earn and easily lost and that permeates through the entire company. It also depends how regulated a company is, for example, a security firm would most likely have better information governance.	She sees no increase in information governance in particular to GDPR. The improvement in information governance is based on corporate culture.
3	**Question**: When doing the analysis in which companies try to figure out the "reason and purpose" of specific data collections, where do you see companies making the most mistakes? Meant by mistakes are issues that lead to incompleteness or inconsistencies.	
4	The problem is when you have people from different departments; they only understand their own department, but not the others. This lead in particular to incompleteness and inconsistencies if the data mapping is done by several people. And then you have a problem when certain data is sent all over the place, and no one really knows where it ended up. Also, as soon as you're trying to update the data mapping list, you will run into issues like incompleteness due to the fact that on a conference, for example, it is very hard to gather all data as you are dealing with many different data types.	The major mistake is incompleteness for a variety of reasons, in particular, departmentalisation.
5	**Question**: Which 'security processes' will be most likely the downfall of 'continuous' GDPR compliance in corporations?	
6	We need to stress that compliance is an ongoing process if you are compliant today you will not be compliant tomorrow if you have not planned for it. For example, you might have changed your business practice. So, you are running into a problem if you are spending more money on staying compliant than on making profits in this sphere. The good thing is that there are a lot of tools that are either for free or paid that can support you in staying compliant. Suppliers, in particular, have to be more proactive because your clients are turning to them.	Changing business practices change regulatory requirements in GDPR
7	**Question**: Was GDPR more technically challenging as companies have expected it to be? Which technical controls were hard to adopt? In which fields were technical changes higher than expected in the beginning?	
8	The regulation is mainly treated by the legal department and normally not entirely by the technical departments, and of course, there must be an interaction between these two departments, but I see that the legal department has taken charge of it. So, I can say	First command by the legal department, second in command, the technical departments.

	it was more treated as a legal and organizational thing rather than the technical one.	
9	**Question:** Do you think that DPIAs will mainly be outsourced to external providers or will companies try to adopt a well-defined process for it?	
10	I think it is very hard for them to do it in-house when they don't know what it entails. I know that they have engaged many consulting firms to help them. and most of the people will simply take an off-the-shelf tool that they find appropriate. This is simply the most cost-effective solution even for the bigger companies. I have done DPIA's, and I can say that they are rather simple. They all asked you for if you have personal data, if yes what type of data, and is it secure. And these are basically questions which we also answer all the time. As it is not so difficult, the best solution is to do it in-house with off-the-shelf solutions, but anyway for major things, I'm sure that consulting firms will be engaged. It also has to be said that the degree of sophistication varies depending on the size of the corporation.	Of-the-shelf solutions are sufficient, but if the sophistication is higher, consulting firms might be hired.
11	**Question**: In terms of incident response and management, which plan has seen the best implementation in the transition period – IRP, DRP, BCP? For which of these plans, companies ask for consulting the most often?	
12	We are always focusing on having a good business continuity plan, but this is not common to have. It is also good to know that your suppliers have one. But it extends if you look at Cambridge Analytica where no one actually validated that they got their data back. But what happens is that companies mainly focus on incident response planning. Because what I see in business continuity plans is that they range from being simple to ridiculously simple. The problem is that these templates are designed for large companies. But I actually think that the focus is on incident response, in particular on the breach, because companies have experienced breaches and are scared. Looking at the amount of data stolen from Equifax, it was huge.	Focus on IRP because companies are scared as they see that breaches happen rather frequently.
13	**Question**: If the data portability right will mainly be used what do you think how companies will respond to the demands? Are companies mainly trying to solve the issue in-house or do they contract consulting firms to employ a technical solution to this issue?	
14	This really depends on what type of company you are. So, if you have a central database in which every data is stored whichever touched your organization. I actually don't really know what people are going to do with that data when they have it, but from a consumer point of view, I don't think the demand will be so high. And I see as some studies show, that the right to be forgotten is the big one, and I think the people who exercise this right. I think that the right to be forgotten is more important than the right to data portability.	Right to be forgotten is the bigger one, the right to portability will not be executed so much in her opinion.
15	**Question**: These were all my questions if you have more things which you want to tell me, I am open for that.	

16	Well, I have been talking to procurement people, about what is keeping them up at night is supplier vulnerabilities and information security. Because they feel the need to keep out the bad guys as far as possible. They know that their suppliers vary in sophistication, they vary in size and in terms of their resources. So, they see that the bad guys are trying to get to them. I was at a conference, and one person was asked on stage, what is keeping you up at night. And he answered information security and supplier vulnerabilities as well. The difference is with companies that have been under regulation before like PCI or SOX, GDPR is easier to implement. For other companies that have not experienced regulations before have bigger problems.	Supplier's vulnerabilities and information security are major concerns
17	Thank you for the interview!	

8.5.3 Interview Transcript – Alexander Hanff

Paragraph	Text	Summary
1	In which extent do you see an improvement in information governance in companies and higher flexibility in adopting new regulations?	
2	I think it is currently too early to tell; we will see in the near future if it has worked or not. What it seems to be in many respects is a wait and see attitude whether you get your own house in order, so we are going to see if there will be any significant changes in data governance. In the last four years, I have seen that clients are very happy in making changes in this regard, but this does not mean that it is a direct effect from the regulation.	Too early to say, but changes are undergoing at the moment.
3	Which 'security processes' will be most likely the downfall for 'continuous' GDPR compliance in corporations?	
4	Human error, using emails as a filing system is some of the biggest issues I've come across, people just don't delete emails. I think encryption could help mitigate some of the stuff, but we'll see that social engineering is still one of the top causes of security breaches of organizations. I've recently read 75% of security breaches are internal. It is probably the biggest issue in regards to security, the human aspect.	Human error, no deletion of emails, encryption is good to mitigate; social engineering is the problem.
5	How did the IT risk management processes in companies improve?	
6	IT is only part of the solution when it comes to GDPR; organisational changes are in my opinion by far more important. As I said, most breaches happened due to human issues not because of technology issues. And we have to bear in mind when we talk about risk-based approaches; we have to talk about the risk to data subjects and not to the organisation - that is what is meant by the risk-based approach. GDPR is data subject centred. Where we might see less risk, again it is impossible to say at this moment, maybe 12 months after GDPR, we might see fewer data breaches.	It is about the risk to data subjects and not to the organisation. There could be fewer data breaches in the future, but it cannot be said by now.
7	Was GDPR more technically challenging as companies have expected it to be? Which technical controls were hard to adopt? In which fields were technical changes higher than expected in the beginning?	
8	I don't think that organisations find it technically challenging, I think the problem is that most organisations, nowadays, is to find a particular service or tool that they need without thinking about the consequences. So, when an organisation is not checking if an American provider is listed in privacy shield. This is effective for the consumers as well, this convenience factor. Companies need to do more due diligence; they need to be more aware of the risk of handing their data to a third-party processor. Many of the problems you see from a privacy perspective are not related to GDPR and all, they are related to the privacy directive, so you need a more holistic approach of the data landscape in the future.	Convenience factor, more due diligence is needed, ePrivacy Directive also needs to be considered

9	How do you see the situation in Sweden? Is there one problem that stands out in comparison to the other countries?	
10	I think companies in Sweden are like companies everywhere. Obviously when it comes to law in Sweden, Sweden is particularly lacking, I would say even with existing European data protection. This Is something which is not unknown, but the amount of data which is freely available about individuals is troublesome and certainly, in my mind and many minds I speak to, think that this is not compatible with the European order. So, from a company perspective, I would say the problems are quite the same if it's in Sweden or other European countries, but the sharing of individual data it is more problematic.	In companies no real difference, but the data which is available to individuals is troublesome.
11	What is more problematic and why? The right to be forgotten or the right to data portability?	
12	As long as companies are aware of their data pools, the right to deletion is not such a problem. The right to data portability, as we don't have standardised models as of yet. Bear in mind that the regulation says it must be in a machine-readable form, but there is no specifics about which form is has to be. So, I would say, data portability is probably the more difficult issue.	Data portability because models are missing as of now.
13	How is it with SMEs and data breach identification?	
14	Identifying breaches is always problematic, especially in smaller companies. The cost of breach identification services can be quite expensive. In large companies this is not such an issue, they simply increase some budget, but for smaller companies, it's much more a problem. But again, as I said earlier, most breaches are internal and are of human issues and not technology issues. I always say that a janitor has more information than the CEO has because people leave stuff lying around. A clean desk policy could be a good change that companies could make. Having shredding machines, many companies don't have shredders within the organisation. There are so many things that happen on a day-to-day basis which are analogue which is significantly more of a threat. From a technological perspective, breach identification systems have to come down in cost, or they should be integrated into infrastructure that they don't have to be purchased as an add-on, and that would fit beautifully with privacy by design principles. And from a human perspective as I have said changes in the organisational field would be very useful.	Breach identification systems are expensive and must come down in price or integrated into infrastructure. But analogue issues are by far more problematic. Clean desk policies can help.
15	Do you think that DPIAs will mainly be outsourced to external providers or will companies try to adopt a well-defined process for it in-house?	
16	There are software tools available so the DPIA, resources are available to be able to do this themselves. But for most, it's a daunting task. I think it's not a problem having someone from outside and taking care of those; it makes it more efficient if an organisation has not done a DPIA before, they may not know exactly what they need to do. So, if you have someone coming in who has done hundreds of DPIAs, the process is much more efficient,p and the results will hopefully be better.	Someone from outside provides more efficiency and better results. It also helps in the learning process.

17	Did GDPR have any effects on BCP?	
18	I think this is not much an issue because most companies are using third party service providers. So, most of the infrastructure is based in the Cloud as opposed to internal systems. So, from the availability side of things, these cloud providers have massive infrastructure and the SLAs are usually quite good. Also, we see that it is improving, downtimes have decreased. The most significant threat to downtime nowadays are DDoS attacks, and even there are significant improvements in how we handle it these attacks. Availability isn't such an issue as it used to be from a security perspective, but this does not mean that we will not see future problems along this line.	Availability is not such an issue anymore because most companies use the cloud and have good SLAs.
19	These were all my questions; if you have one more thing that you want to tell me, this is the space.	
20	As I said, GDPR is not the only thing which we have to consider when we talk about privacy. There is constant neglect of other regulations which are important and there is a lot of misinformation out there. We need to consider many different laws which affect data protection and privacy.	A more holistic view is necessary.
21	Thank you for the interview!	