LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Compliance Challenges with the General Data Protection Regulation

Master thesis 15 HEC, course INFM10 in Information Systems
Presented in [June, 2017]

Authors: Petter Billgren
Leon Wipp Ekman

Supervisor: Azadeh Sarkheyli

Examiners: Paul Pierce
Odd Steen

Compliance Challenges with the General Data Protection Regulation

Authors: Petter Billgren and Leon Wipp Ekman

Publisher: Dept. of Informatics, Lund University School of Economics and Management.

Document: Master Thesis

Number of pages: [127]

Keywords: [GDPR, General Data Protection Regulation, Compliance in Information Systems, Personal Data, Data Security]

Abstract:
The General Data Protection Regulation are coming as a response to the outdated Directive from 1995. With this, a lot tougher pressures are put on organisations regarding the demand for compliance, which is mainly done through higher penalties, giving organisations an incitement to oblige. Seen from the perspective of information systems, organisations have to implement the requirements of the regulation into their data processes in order to stay compliant. In the literature there is a lack of understanding of what challenges organisations face when striving for compliance in information systems. The General Data Protection Regulation was used as a lens to examine the available compliance theory. This was done by interviewing employees working with and in organisations trying to comply with the General Data Protection Regulation in positions such as security management, product management and project management. We found seven challenges and one sub-challenge concerning data processes that organisations face as they adjust to the General Data Protection Regulation.

Content

Figures

Tables

1 Introduction

As technology have advanced during the last 20 years organisations have found more intuitive ways to use personal data (Lynskey, 2015). According to Fuller (2015) and Lynskey (2015) the ever growing number of devices connected allow organisations to collect and store rich data about their users. With Big Data analytics huge data sets can be processed to predict personal behaviours, preferences and actions (Fuller, 2015). Lynskey (2015) argues the old legislation within the European Union, the Data Protection Directive from 1995, controlling how this is done have been lagging behind, which have made data a commodity traded relatively freely. The citizens of the EU have little to say about how their personal data is combined and processed (Financial Times, 2017). This is however changing. As a response to the obsolete directives, the European Union have decided to implement a new regulation called the General Data Protection Regulation (GDPR). The regulation will be enforced on the 25th of May 2018 giving more power to the citizens of the European Union and their privacy (Ec.europa.eu, 2017). According to Financial Times (2017) and Lynskey (2015) this will impact the way that organisations will be able to gather, store and process personal data as it will be tighter regulated for all organisations. The law could be considered ambitious both in its scope and for the penalties for not complying (Lynskey, 2015). The author argue that the regulation will apply to all organisations that handles personal data to some extent, even for non-European companies that handles EU-citizen data. ComputerWeekly (2017) points at the fines for non-compliance is up to 4% of the annual turnover or €20 million, whichever of the two that is the highest. This gives strong incentives to adapt to the new laws as the penalties are high (ComputerWeekly, 2017; Financial Times, 2017). The GDPR mainly targets user consent and data processes (Lynskey, 2015). Data processing have a quite broad definition; any operation which is performed on data (e.g. collecting, storing, combining, manipulating or deleting) by automated or manual means (Regulation 2016/679/EU Art. 4, EUR-Lex, 2016).

1.1 Problem

Moving towards a more regulated data market is considered as a step in the right direction for privacy and integrity for the citizens of the EU (Lynskey, 2015). According to Computer Weekly (2017) the European Union says it will contribute to trust between the user and organisations, and clearer lines for what is lawful data processing will be established. But the author also argues that organisations seem to be unaware of the implications and consequences of the GDPR. Operating in accordance with agreements or legislation is becoming increasingly important in several industries, but there is a lack of understanding of how to implement the required changes (Sadiq, Governatori & Namiri, 2007). Seen from the perspective of information systems, organisations must implement the requirements of agreements or legislation into their data processes in order to stay compliant. (Knackstedt, Braeuer, Heddier & Becker, 2014). According to Abdullah, Sadiq & Indulska (2010) the growth of attention for compliance is due to the raised stakes that comes with non-compliance. The authors argue that this could be in the form of fines, which generally cause significant economic loss. Moreover, the reputation for violation could be disastrous for any organisation (Abdullah et al. 2010). The way data is processed in some organisations needs to change fundamentally, and this has to be

done in a short period of time (Computer Weekly, 2017). With limited academic coverage on regulations in information systems (Eggert, Winkelmann, Lohmann & Knackstedt, 2013; Panitz, Wiener, & Amberg, 2011; Sadiq et al. 2007), there is a lack of understanding of what challenges organisations face when striving for compliance. The GDPR is as mentioned considered to be demanding in character, have a large scope and high penalties (Lynskey, 2015), therefore this is as an opportunity to examine whether the available theory surrounding compliance in information systems is able to explain the challenges that organisations are facing when adapting to the GDPR.

Therefore, our research question will be:

> *What challenges, concerning data processing, do organisations face when striving for compliance with the General Data Protection Regulation?*

1.2 Purpose

The purpose of this Master thesis is to evaluate if information system compliance theory is able to define the challenges that arise with adjusting to the General Data Protection Regulation. We will use the adoption of General Data Protection Regulation as a lens to examine the available theory.

1.3 Delimitation

We will not investigate whether the GDPR is complied with in a lawful manner. Neither will we evaluate or examine if the legislation fulfils its purpose. We will only focus on the parts of compliance theory that consider the challenges of adjusting data processes. Furthermore regarding the theory of compliance, the focus will only be on regulatory compliance.

2 Literature Review

The literature review begins with an explanation of how the prior law, the Data Protection Directive from 1995, works and the idea behind it. We then in short explain the idea behind the GDPR. We further explains the most important aspects of the GDPR in relation to data processes and what types of effects the different aspects are believed to have. This is done to give a better understanding of the regulations and its possible impacts. Lastly we explain the theory behind compliance in information systems.

2.1 Data Protection Directive

The current legislation that protect the rights concerning personal data of citizens within the EU is the Data Protection Directive from 1995 (Lynskey, 2015). This directive was when ratified an attempt to harmonies the way data can be stored and processed within the EU, but has been interpreted differently in all member states according to Lynskey (2015) and Wong (2012). Therefore Lynskey argues, that it is unclear whether the Data Protection Directive is correctly adopted and implemented by the national courts. Despite this she writes that the directive did introduce several purposes and definitions which remain in the GDPR. Key concepts like data controller, data processor and personal data are defined and have changed little in the forthcoming regulation (Lynskey, 2015). Even if the Data Protection Directive is relatively new compared with other EU laws, Lynskey (2015) points at the fact that the directive is obsolete in some aspects. Since the law is written when only a fraction of the citizens of the EU used the internet regularly, aspects that were unpredictable at the time is now a reality (Lynskey, 2015). This has led to the Data Protection Directive becoming inadequate when protecting the EU citizen´s rights. While some parts of the GDPR and the Data Protection Directive are closely related, issues like the reuse of personal data and uniform adoption by member states is not handled in the current legislation (Lynskey, 2015). Another issue with the current directive is its approach to trans-border flows of data. It states that if this is done, the appropriate measures must be taken to ensure the safety of the data, which according to Poullet (2006) can be interpreted differently. Laws concerning cross border flows of data has therefore been adopted differently by member states (Poullet, 2006). Even with its apparent flaws to serve as a holistic approach for the EU to protect its citizen's rights, it is still argued by Lynskey (2015) and Poullet (2006) the fundamental ideas are still noteworthy. The GDPR and Data Protection Directive serve the same purpose and share definitions and concepts. The new regulation is rather the addition of sharper layers, such as higher penalties and more specific requirements, to the blunt directive (Lynskey, 2015).

2.2 The General Data Protection Regulation

The General Data Protection Regulation does not come out of a vacuum, but as a response to the rapid technological advancement (Gilbert, 2016). As mentioned above The GDPR have clear ties to the Data Protection Directive from 1995 and serve the same purpose; to regulate

how personal data is handled by an entity, and protect the rights concerning personal data by a citizen of the EU (Lynskey, 2015). But as storage and processing power have increased the ability to do data analytics of huge sources have become a reality (Lynskey, 2015).

"Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data." - (Regulation 2016/679/EU Recital 6, EUR-Lex, 2016)

The directive from 1995 is too unspecific and indistinct when it comes to regulating data processing, which the GDPR tackles more specifically (Lynskey, 2015). Lynskey points at one specific change that the EU Data Protection Directive does not cover is the reuse of personal information with new purposes. The mapping and restructuring of personal data can currently be done relatively freely (van Loenen, Kulk & Ploeger, 2016). Since the directive was adopted at a time when as little as 1% of the citizens of the EU was using the internet it was difficult to predict how personal data would become a commodity (van Loenen et al., 2016; Lynskey, 2015). Moreover, the GDPR will be regulative instead of a directive, which means that there will be no discretion between member states (Gilbert, 2016). The goal is to ensure consistent application of the law throughout the European Union (Lynskey, 2015). Lynskey writes that a directive still needs to be implemented by all member states, but can be done in accordance with domestic laws and culture. A regulation on the other hand, must be adopted the same way by all, making it clearer and more holistic. (Gilbert, 2016; Lynskey, 2015). The GDPR still leaves interpretation and adoption of some minor aspects of the regulation to the member states, hence, all rules will not be the same throughout Europe. Therefore, data controllers must be careful not to consider the GDPR perfectly consistent in all states and need to look into how the legislation is adopted (Gilbert, 2016).

2.2.1 Definitions

The GDPR divide the responsibility of personal data between data controllers and data processors (Regulation 2016/679/EU art. 4, EUR-Lex, 2016). Data controllers are defined as a legal person or organisation that collect and decide the purpose and method of processing (Regulation 2016/679/EU art. 4, EUR-Lex, 2016) In short; the legal body that acts to collect and process personal data. The regulation (2016/679/EU art. 4, EUR-Lex, 2016) also define the processor as someone who acts on the behalf of the controller, and merely handles the data. Personal data is by the regulation defined as information that is associated with an identified or identifiable person. The identification could be indirect or direct, and could refer to a name, telephone or social security number, location, culture, economic data, or other identifier (Regulation 2016/679/EU art. 4, EUR-Lex, 2016). All data that is linked to an individual will be considered personal data (Regulation 2016/679/EU art. 4, EUR-Lex, 2016). Processing is by the GDPR defined as:

"[...] any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" - (Regulation 2016/679/EU art. 4(2), EUR-Lex, 2016)

2.2.2 Consent

Consent is an important aspect of the new regulation (Gilbert, 2016). The GDPR and the old data directive shares the law that the data controller, usually a company or public institution, have to have the data subjects, for example, user or customer informed consent in order to lawfully collect their data (Lynskey, 2015). But how this is shown differs. Unambiguous consent, as it is referred to in the GDPR, is shown by an affirmative action. This could be ticking a box or showing in a similar manner your approval. Pre-checked boxes or silence is not enough to obtain the user's consent. There must be an active, informed response to lawfully collect data, passive or default consent will not do (Regulation 2016/679/EU Recital 32, EUR-Lex, 2016). In addition to this, the controller have to be transparent in what way they are going to use the data, which means terms and condition cannot be stated in an unclear manner. Instead, it has to be easily accessible and the organization have to use a comprehensive language and clearly show the user how their data will be used (Lynskey, 2015).

While the need for consent is similar to current legislation, the GDPR introduces stricter laws when it comes to the purpose of the processing. The new laws forces the controller to be purpose specific when it comes to consent, as soon as the purpose of the data processing changes, renewed consent is required (Regulation 2016/679/EU art. 6, EUR-Lex, 2016). According to Lynskey (2015), an organisation that process collected data for new purposes without consent from the user will violate the law. This means that user data no longer can be used in a new context without consent from the subject (Regulation 2016/679/EU art. 6, EUR-Lex, 2016). This is a fundamental change from earlier legislation, and it aims to give subjects more power over the data already passed to controllers (Lynskey, 2015). Generally, public institutions and private organisations wish to collect more data in the belief that it will help them in decision making (Lynskey, 2015). User data becomes more useful as it can be merged and processed again with other data sets, and in this way the sum of the user data becomes bigger than its parts (Lynskey, 2015). The GDPR attempts to regulate the use and reuse of user data more tightly and put more obligations on the data controller (e.g. organisations). (Ec.europa.eu, 2017; Lynskey, 2015). Moreover, the age limit for the collection of user data is currently 13 and will be 16 when the GDPR comes into force. It is however possible to collect data with parental consent for minors (Regulation 2016/679/EU art. 6, EUR-Lex, 2016). According to the regulation, legal processing of personal data can be summarized as the following;

- When the subject explicitly consented to the specific processing.
- When a contract that subject have agreed on previously is not fulfilled.
- When the controller have to comply with other laws.
- When necessary for individual or public purposes.
- When the subject is 16 years of age or have parental consent.

Another important difference from the Data Protection regulation (Regulation 2016/679/EU art. 7, EUR-Lex, 2016) is that a citizen of the EU has the right to withdraw the consent with the same ease as it was given. However, this is not clearly stated in the current directive. This right to withdraw must be presented before the consent is actively given (Regulation 2016/679/EU art. 7, EUR-Lex, 2016).

2.2.3 The Right of Access, The Right to be Forgotten and The Right to Portability

Data subjects have the right to access the data that has been collected about them by an organ-

isation (Regulation 2016/679/EU Recital 63, EUR-Lex, 2016). This includes what information that has been processed, for what period of time, the purpose of the processing and who have been the recipient of the information (Regulation 2016/679/EU Recital 63, EUR-Lex, 2016). If a data subject no longer wish to share their data, the regulation grant them that organisation must be able to erase their information without undue delay. As long as the data is no longer needed to fulfil the purpose that was agreed on, the data subject have the right to be forgotten (Regulation 2016/679/EU art. 17, EUR-Lex, 2016). As the data subject have the right to access their data, they also have the right to portability. This means that a person should be able to transfer their data across different services. In order to comply with the right to portability section of the GDPR the data controller has to offer the data subject the reuse of their data securely and conveniently. (Regulation 2016/679/EU art. 20, EUR-Lex, 2016).

2.2.4 Territorial Scope

One important aspect of the regulation is that it applies to all organisations, wherever they reside, that use any personal data of citizens of the European Union (de Hert & Czerniawski, 2016). The processing of personal data could take place outside the EU, the controller or the processor will still be under the authority of the GDPR (Gilbert, 2016). According to Gilbert (2016) non-EU organisations will be affected by this law when the organization processes personal data about citizens of EU, either by offering goods or services, or if they are monitoring the behaviour of the citizen (Gilbert, 2016). This could be advertisement in mobile apps or on web pages that is accessible and aimed for EU citizens. A service that collect data about user, for instance cookies on web pages, will also be enough to make the regulation applicable (Cuijpers, Purtova & Kosta, 2014; Gilbert, 2016). The connection between the controller or the processor will be established through a representative in one of the states that the controller is active. This legal person must be assigned by the controller or processor and will be responsible for compliance of the GDPR (Regulation 2016/679/EU art. 4, EUR-Lex, 2016).

2.2.5 Data Privacy Officer

A Data Privacy Officer (DPO) will have to be appointed when a controller or processor have large scale and systematic monitoring of EU citizens (Regulation 2016/679/EU art. 9, EUR-Lex, 2016). Exactly what the large scale processing entails is not defined in absolute numbers. An example of large scale processing is a hospital keeping track of its patients or a food-chain that advertise based on customer behaviour (Data Protection Working Party, art. 29, European Commission, 2016). The European Commission further states that organisations that handles special categories of personal data or operate in high-risk areas will also have to appoint a DPO. Special categories of personal data is sensitive information related to political opinions, sexual orientation, beliefs or other delicate data that can be connected to an individual (Regulation 2016/679/EU art. 9, EUR-Lex, 2016). Gilbert (2016) argues that the DPO is supposed to act like an accountant, hired by the organisation but independent enough to investigate and question how personal data is being handled. Therefore, this service could be outsourced from another company, as long as the DPO is easily accessible (Gilbert, 2016). Even if a controller or a processor is not required by law to employ a DPO, it would help the organisation to comply with the GDPR. It is recommended by the EU to assess whether a DPO is necessary or not in order to demonstrate that all data processes are done in accordance with the regulation. (Data Protection Working Party, art. 29, European Commission, 2016)

2.2.6 Transparency and Documentation

All data processing of personal data is by the GDPR required to be transparent (Lynskey, 2015). The principle of transparency focuses on the accessibility of information, easy to comprehend, and written in a clear language (Regulation 2016/679/EU art. 12, EUR-Lex, 2016). According to Lynskey (2015) the focus on transparency goes through the entire GDPR and is especially important when a data subject is directly involved. As mentioned earlier, the foundation for consent from the user is that it is informed (Lynskey, 2015). This focus on transparency characterize the entire GDPR and is reflected in most of its articles. (Regulation 2016/679/EU, EUR-Lex, 2016). In order to keep this high level transparency, documentation is necessary (Lynskey, 2015). Both controllers and processors are obligated to keep records of how they process personal data (Regulation 2016/679/EU art. 12, EUR-Lex, 2016). According to Gilbert (2016) his means that a controller will need to know exactly how their data is handled by third-parties. Stating who is the controller and the purpose of the processing is straightforward, more complicated is to be able to show the entire data flows under its responsibility (Gilbert, 2016). Moreover, the regulation (Regulation 2016/679/EU, EUR-Lex, 2016) requires the controllers and the processors to be able to show who the data is disclosed to, both within the EU and outside. However, this demand of extensive record of processing is only applicable to organisations with 250 employees or more, or if the processing of the data controller is likely to cause high risk to the subject (Regulation 2016/679/EU art. 30, EUR-Lex, 2016). With a complete record of policies, reports and contracts the controller or processor can, if a supervisory institution wants to take a closer look, show how their data processing is handled (Gilbert, 2016).

2.2.7 Penalties

If an organization does not comply with the regulation it can be fined (Regulation 2016/679/EU art. 83, EUR-Lex, 2016). The highest fine that can be given is either 4% of the annual global turnover or €20 million, whichever is the highest according to the mentioned article. It is also possible for organisations to get a smaller fine of 2% of the annual global turnover for not having their records in order, if they do not tell authority and the affected citizen about a breach (Gilbert, 2016) The rules includes both controllers and processors which means that cloud services are included (Regulation 2016/679/EU art. 83, EUR-Lex, 2016) The punishment for non-compliance with the current Data Protection Directive is not as decisive (Gilbert, 2016) Under the directive, offenses in different member states have different consequences according to Lynskey (2015). The author further explains that punishment for violations under GDPR will be harder, showing that the EU will provide the legal tools to enforce the new regulation with clearer and homogenous penalties.

2.3 Data Processes

There will be tougher requirements on how data will be processed, stored and transferred according to Tankard (2016). Moreover he argues that organisations have to add technological and operational safeguards to secure the data, this includes strong privacy controls. This means according to the author that organisations must consider the data protection and privacy right at the beginning of the security planning process. While the GDPR demand more in terms of security measures, it also offers guidance how this could be achieved (Regulation 2016/679/EU, EUR-Lex, 2016). For instance, pseudonymous data is allowed to be stored by

organisations and falls outside of the scope of the regulation, this is data that has been altered so that it cannot be attributed to an individual person (de Hert & Papakonstantinou, 2016). Another way of securing data proposed by the GDPR is by encryption. (Regulation 2016/679/EU art. 6, EUR-Lex, 2016) When organisations gather and store personal data they become responsible for protecting that data from breaches (Tankard, 2016). By encrypting the data in a correct manner or by making the data pseudonymous, organisations are able to protect the data subject from harm, and itself from responsibility if data breaches occurs (Tankard, 2016). Organisations should be aware that any data that is contained in an e-mail, including the e-mail address and third parties mentioned in the e-mails count as personal data. (Ryz and Grezt, 2016).

The responsibility over the data goes beyond data security (Tankard, 2016). If a breach of personal data were to occur, the organization have to inform the supervisory authority of the breach within 72 hours (Regulation 2016/679/EU art. 33, EUR-Lex, 2016). In cases where the data subject could suffer from the breach to a high extent, the organisation must inform the individual (Bridge, 2014). If they haven't protected the data in a correct manner the organization are also liable for fines. Organisations that have documented compliance with measures recommended in the GDPR will most likely not be fined (Bridge, 2014). Therefore, pseudonymisation, encryption or other types of protections are often the key to satisfy the new regulation. If the data subject no longer is linkable to the data, the organisation is in the clear. (Bridge, 2014; Koščík, 2017).

2.3.1 Storage Limitation and Data Minimisation

Under the GDPR (Regulation 2016/679/EU, EUR-Lex, 2016) organisations are not allowed to store personal data indefinitely without good reasons. The GDPR (art. 5) states that as soon as the storage of personal data no longer is necessary for the declared purposes it should be deleted or anonymized/pseudonymised. Therefore, an organisation can keep and process personal data for extended periods of time if this serves the agreement with the customer (Regulation 2016/679/EU art. 5, EUR-Lex, 2016). Storage limitation is included in the Data Protection Directive as well, with a similar definition. Nonetheless, this is an important aspect of the coming regulation (Koščík, 2017). Moreover, the GDPR will include a stricter demands for data minimisation, which means that only purpose related data can legally be processed. If the processing does not serve the purpose, it will be unlawful. This means that organisation will have to look over their data processes to see whether data is limited to what is necessary (Regulation 2016/679/EU art. 5, EUR-Lex, 2016) Koščík (2017) points at how the GDPR also is concerned with how the collected data is tied to the individual and advocates for anonymisation as an approach to comply. This means that the data no longer is related to an individual and cannot be traced back to the person who had their data collected. In this way an organisation can comply with the demand for storage limitation. But there are different levels of de-identification (Koščík, 2017).

2.3.2 Levels of De-Identification

According to Hintze (2016) different levels of de-identification need to be defined to be able to scrutinize and understand the regulation. Hintze (2016) gives a simplified explanation of the different grades of identifiability through four levels; Identified, Identifiable, Article 11 De-Identified, and Anonymous/Aggregated. Identified data is information that is directly related to a person or identifies a person. Hintze (2016) uses the examples of name, e-mail ad-

dresses and government issued ID-numbers as identified data. Identifiable data is connected to a person but the identity of the individual is not obvious from the data (Regulation 2016/679/EU art.11, EUR-Lex, 2016). The regulation also states that it is possible to create a connection or link the data to the specific person with the help of identifying data. By combining or triangulating different sets of data the identity of the individual can be revealed. Pseudonymous data as defined by the GDPR are a subset of identifiable data according to Hintze (2016). Article 11 De-Identified data are named after how de-identified data is defined by article 11 of the GDPR (Hintze, 2016). De-Identified data could be related to a specific person but it is not traceable from the specific data. In addition to this, the data is not directly linked nor connected to data that would identify the person (Hintze, 2016). For the data to be re-identified it would have to be matched to additional identifying data provided by the specific person. Anonymous/aggregate data is stored without any identifiers for the person related to the data as well as being aggregated with enough amount of data about other persons so that it cannot be linked to a specific person. Even with additional information provided it would not be possible to pinpoint (Hintze, 2016).

2.3.3 Pseudonymous Data

With the GDPR pseudonymisation of data is one of the ways that organisations can protect data and make sure that it cannot be linked to a specific person (Hintze, 2016). According to the regulation (Regulation 2016/679/EU art. 4, EUR-Lex, 2016) this is one of the ways that a controller or processor can protect itself and the data. By making data pseudonymised organisations are able to protect themselves from being liable of possible data breaches (de Hert & Papakonstantinou, 2016). In the GDPR pseudonymisation is defined as:

"'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"- (Regulation 2016/679/EU art. 4(5), EUR-Lex, 2016)

The GDPR states that if controllers cannot identify a data subject, they do not have to give a specific person access, rectification, erasure or data portability. For controllers to be able to de-identify a data subject they can pseudonymised data in such a way that it is not possible to re-identify a specific person (Regulation 2016/679/EU art. 11, EUR-Lex, 2016). If the controller deletes identifying data that can be used to link data to a specific person it may not be possible, without collecting other data, to re-identify the specific person. (Regulation 2016/679/EU art. 11, EUR-Lex, 2016). The only way that data controllers are allowed to deny the data subjects and its requests are if: "The controller is able to demonstrate that it is not in a position to identify the data subject". (Regulation 2016/679/EU art. 11, EUR-Lex, 2016) If the specific person provides data to the controller that makes it possible to re-identify the person they are again able to ask for access, rectification, erasure or data portability. (Regulation 2016/679/EU art. 11, EUR-Lex, 2016).

2.3.4 Encryption of Data

According to Tankard (2017) encryption should be considered the cornerstone of data security. Tankard further explains that encryption is to be considered the most important security aspect of the GDPR and the safest way to protect any data. Pseudonymisation has its flaws and there are known cases where anonymous data has been de-anonymized. (Tankard, 2017) The need for encryption includes both structured and unstructured data according to Tankard (2016). The data can be stored in databases, spreadsheets, word documents, presentations, emails or archives, the data can also be stored in the cloud or on endpoints it should still be encrypted. (Tankard, 2016). Keys for the encryption should be kept by the responsible of processing data within the organization according to Tankard (2016). The level of encryption that an organization needs depends on risk analysis such as what types of personal data that are being handled, affordability and technology available. (Heimes, 2016) The GDPR do not give any clear guidelines of what types of encryptions that should be used, only that encryptions could be used to protect personal data. (Regulation 2016/679/EU, EUR-Lex, 2016).

2.3.5 Breaches of data

Breaches of any personal data where the subject faces risk of economic, material or non-material loss the organisation must notify the user, this must be done swiftly and without delay, no later than 72 hours after the incident (Regulation 2016/679/EU art. 33, EUR-Lex, 2016). All breaches must be reported to to a data protection authority, unless there is no risk to cause the user damage (Regulation 2016/679/EU art. 33, EUR-Lex, 2016). It is notable that all data breaches are not done by external persons; it can also be caused by employees of the organization (Hooson, 2015). According to the author 43% of all US businesses have had problems with data breaches and most of them were caused by employee negligence. Overall, bad data handling or human error is increasing as a cause for security issues and companies with harder internal policies have fewer breaches. (Lyons, Van Der Werff & Lynn, 2016). There are several cases in UK as well were organisations have not managed to destroy the data that should have been removed (Bridge, 2014). Organisations have to be aware of this in order to comply with the GDPR (Bridge, 2014).

2.4 Business Compliance

With the tougher regulations on data processing and harder penalties for non-compliance the EU is pushing for a higher standard when it comes to handling personal data (Kleindienst, Nüske, Rau & Schmied, 2017). The strive for better processing is not only a matter of following the laws, organisations put effort into handling and securing personal data to stay ahead of competitors and avoid scandals. (Kleindienst et al., 2017). The importance of a proper digital business model have increased over the last years, and so has the concern from customers over security issues (Smith, Milberg & Burke, 1996). However, this is not a new phenomenon and security concerns have been a hot topic within the IS field since the 90s. Several security scandals have shed light on these issues and it is argued that a higher priority of security of personal data is a way to gain a competitive advantage (Kleindienst et al., 2017) But customers act inconsistent with their own beliefs and actions. It is often the user that voluntarily share their data even if this goes against their privacy concerns (Norberg, Horne & Horne, 2007). The lack of understanding of how the data is used is a reason for worsened privacy. Norberg et al. (2007) pointed at the possible solution of protecting the user against itself. This

is partly changing with the GDPR as the laws for data collection will be much stricter, often in favour of the user's privacy (Lynskey, 2015).

As mentioned above, the GDPR and the data protection directive from 1995 are similar in many ways. The purpose of the new regulation aligns with the old directive, and the objectives are overall the same. It is rather the technological advancement and cross border flows of personal data that is addressed in the GDPR (Koščík, 2017). Broad definitions and the ambition to protect the privacy of EU citizens makes the GDPR a legislation that will shape data processing, primarily within the EU, but also outside (Gilbert, 2016). As most organisations handles personal data to some extent they are likely to be affected by the GDPR (Oprysk, 2016). According to Koščík (2017) the GDPR focuses on a few topics that is relevant for organisations. These are the principle of storage limitation, data protection by design, processing of data, the right to be forgotten, and anonymization (Koščík, 2017).

Koščík (2017) argues that an organisation that has previously had control over its data processes and security measures will be able to adjust to the GDPR with little difficulty; that is, "the change is more a matter of more precise formulation of these principles than any fundamental change in basic concepts" (Koščík, 2017, p. 43). A solid foundation for complying with the new laws is to have data protection by design as a way of handling personal information (Hansen, 2016). He further explains that data protection by design is a method where the organisations value the privacy of persons through the whole process of developing a system. This needs to be taken into consideration from the beginning of the project and is thought of throughout the process (Koops & Leenes, 2014).

2.4.1 Requirements of Data Controllers

The data controller is an important aspect of the GDPR since it represents the person, organisation or other body that determines the purpose and means of the data collection and processing (Lynskey, 2015). This entity carries a lot of the responsibilities presented in the GDPR and is along with the data subject recurring through the entire regulation; where the data subject have rights, the data controller have obligations (Lynskey, 2015). Data controllers will need to demonstrate that they comply with these obligations in a transparent way, meaning that a supervisory authority at any time should be able control the data processes. (Regulation 2016/679/EU art. 30, EUR-Lex, 2016). This requires complete knowledge about all types of processes that include personal data, which potentially could turn into lots of documentation (Lynskey, 2015). The same type of documentation is demanded by any data processor, which makes it possible to follow how personal data is processed (Regulation 2016/679/EU art. 30, EUR-Lex, 2016). More documents and stricter control will possibly force organisations to change their way of work (Tankard, 2016). This goes in line with the Right to be Forgotten, the Right of Access, and the Right to Portability (Gilbert, 2016).The data controller will need to understand their data processes to ensure that all data can be accessed or erased if this is the will of the user (Lynskey, 2015). In order to keep track of all processes and documentation, a Data Protection Officer is recommended and in some cases required (Regulation 2016/679/EU art. 37, EUR-Lex, 2016). This could be a burden for smaller organisations, but will help the controller understand its processes and reduce the risk of fines (Tankard, 2016). Consent for collecting data is not a new aspect, it is however harder to get valid consent (Gilbert, 2016). Gilbert (2016) believes that organisations will have to look over how they get the subjects approval. Since consent must be freely and actively given, which is stricter than what is currently allowed, organisations must see to that their method for receiving consent is valid

(Gilbert, 2016). The GDPR do state techniques that are suitable for obtaining consent in a correct manner;

"This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data." - (Regulation 2016/679/EU recital 37, EUR-Lex, 2016)

Moreover, the subject needs to be informed on the purposes of the collection and processing, which is more demanding than the current legislation (Poullet, 2006). This means that organisation will have to ensure that the subject is informed, something that will require additional measures when the consent is given (Wong, 2012). Failing to inform the user will result in invalid consent (Regulation 2016/679/EU art. 4, EUR-Lex, 2016).

2.4.2 Requirements of Data Processors

Data processors acts on the behalf of data controllers but still have responsibilities as they handle personal data (2016/679/EU art. 4). However, the processor does not have a specific purpose with the data they are asked to manage (Eldred, Adams & Good, 2016). One example of this is cloud-computing, any type of cloud-service fall into this category; Infrastructure as a Service, Platform as Service, and Software as a Service (Eldred, Adams & Good, 2016). They argue that cloud-services have been widely adopted as a way for organisations to rapidly increase their computing and storage power. However, this trend has been more dominant in the USA than in the EU, partly because of the unclear and different application of the Data Protection Directive in EU member states (Eldred et al. 2016). As cloud-services often operates across borders it is difficult and costly to comply with the current legislation (Eldred et al. 2016). With the GDPR, as a homogeneously adopted regulation, these problems will be mitigated (Oprysk, 2016). While the rules will be coherent and make complying easier, the demand for documentation will increase (Koščík, 2017). Clear contracts between the controller and the processor must be established and if the data processor will employ another processor, this must be in this contract according to Koščík (2017). Overall the processor must comply with the same rules as a controller when it comes to documentation and storage requirements (Koščík, 2017). Therefore, the controller must be able to ask their processor to fetch or erase personal data about an individual with short notice or be able to show authorities how personal data is handled. A data processor must also appoint a data protection officer on the same grounds as a data controller (Regulation 2016/679/EU art. 28, EUR-Lex, 2016).

2.4.3 Privacy by Design and Default

According to article 25 in the GDPR the controller have to both prior to and during the processing of data implement measures and techniques to protect the rights of the data subject (Regulation 2016/679/EU art. 25, EUR-Lex, 2016). Data Protection by Design is one of the most challenging aspects of the GDPR because it starts a new type of legal concept by which the regulation follows, the concept of Privacy by Design (Hildebrandt & Tielemans, 2013).

Privacy by design was adopted as an international privacy standard in 2010 (Cavoukian, 2012). The idea of privacy by design are that organisations work proactive with implementing privacy aspects for the personal information that is stored within an organization and that it is secured Cavoukian (2012) further explains. It is preferable to the other alternative which is to

adapt a service on a later stage in the development process (Danezis, Domingo-Ferrer, Hansen, Hoepman, Metayer, Tirtea & Schiffner, 2015). Working proactively with privacy throughout the whole design process implementing privacy features, includes the full lifecycle of the personal data and how the data is used and stored. (Danezis et al., 2015). Privacy by design is based on seven foundational principles (Cavoukian, 2012).

- Proactive not reactive; Preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric (Cavoukian et al., 2010).

Controllers of personal data have to implement technical and organisational measures to provide data protection by default (Hansen, 2016). Privacy by default is defined as a standard configuration by the author. The standard configuration should prevent gathering of personal data that is not necessary i.e. the controller do not gather data that they do not ask for, that they do not store data longer than necessary, that the data is erased as soon as possible after it has been used and that the data is securely stored so that the access is limited (Hansen, 2010). The main object of protection by default are protecting the data subjects from situations where they have little to no understanding or control of the processing of their data (Hansen, 2016).

2.5 Compliance in Information System

An information system is compliant when data processes are adjusted to a set of recommended or prescribed criterions that is supposed to be followed (Turetken, Elgammal, van den Heuvel & Papazoglou, 2011). From an IT perspective, organisations must appropriately introduce the requirements of agreements or legislation and implement these into their respective information systems in order to stay compliant. (Knackstedt et al., 2014). Operating in accordance with legislation, agreements or other forms of forcing documents is becoming increasingly important in several industries, but there is a lack of understanding of how to implement the required changes (Sadiq et al., 2007). The growth of attention for compliance is according to Abdullah et al., (2010) a result of the increased stakes involved with non-compliance. For instance, the fines generally cause significant economic loss and the reputation for violation could be disastrous for any organisation. The solution to a compliant information system is often technical in nature as several data processes have to change in order to handle information properly (Abdullah et al., 2010).

There is not one prescribed way of handling data to ensure compliance in all cases, therefore changes in data processes must be done in accordance with its context (Lohmann, 2012). However, there are certain aspects that influence the way data processing advance to meet certain requirements (Abdullah et al. 2010). Abdullah et al. (2010) points at a set of important aspects that have an influence over the data processes and how they are transformed. The authors argue that these are of importance if an organisation wants to reach a high level of compliance and adjust their information system correctly. Parallel to this there are different approaches when adjusting data processes; corrective, detective and preventative (Sadiq et al., 2007). The authors describe corrective as auditing the information system after the implementation is done. This is usually expensive and ineffective as it is time consuming and difficult to make adjustment after the system is up and running (Lohmann, 2012). A detective approach is argued to be a more automated process, where certain safety measures are installed in the system to monitor and report back to the users. This allows better control over the system, but it is still argued by Sadiq et al. (2007) to be a responsive rather than preventative. Moreover, Turetken et al. (2011) writes that these solutions often are proprietary and bound to specific vendors of software, which is problematic if systems are replaced. Preventative compliance or compliance by design is argued by Sadiq et al. (2007) to be the most sustainable approach. Generic solutions to compliance requirement are the most effective way to handle data processes, as it will facilitate the implementation of new or modification of current data processes (Sadiq et al., 2007).

In literature regarding compliance and information systems we have found some challenges that have impact on the outcome of data process changes. As we aim to get insight into data processing and the changes that have to be made to comply with the GDPR, we have summarized these aspects.

2.5.1 Interpretation of Regulations

Documents that constitute the basis for compliance is rarely specific in how and where a change to a process is supposed to be done, but rather puts emphasis on that a certain set of data needs to be handled in a specific way (Lohmann, 2012). Lohmann (2012) writes that this puts pressure on the organisations to correctly interpret and understand the formal rules, and to be able to translate these into practical requirements. This can become problematic if the guiding document has vague and abstract explanations (Turetken et al., 201). Turetken et al.

(2011) argues that this often takes an expert to analyse and make the law into specific and implementable requirements. Eggert et al. (2013) argue that legal experts can greatly contribute to projects aimed to manage regulations, as it improves software quality from a compliance perspective. Therefore, the interpretation is of importance as it is the first step towards compliance and impacts the shape of future processes (Lohmann, 2012).

2.5.2 Ad-hoc and Generic solutions

As mentioned above, compliance is a set of recommended or prescribed set of criterions that is supposed to be followed (Lohmann, 2012). These can be translated into requirements that are supposed to be implemented in information systems in order to follow the legislation, but how this is done is rarely included (Turetken et al., 2011). Therefore, Turetken et al. (2011) argue that many companies achieve compliance through ad-hoc solutions and work with specific cases instead of creating generic solutions. Without generic approaches the processes is often custom made to satisfy specific requirements (Turetken et al., 2011). According to Abdullah et al. (2010) organisations must be ready for changes in the agreements or laws since they tend to advance over time. The authors writes that a more holistic approach to the adoption of process requirements easier. By designing processes with compliance in mind to begin with, the adaptability of the processes increases (Lohmann, 2012). The organisation should try to look at their information systems as a whole striving for compliance, if the organisation only focuses on details in processes they could end up with fragile systems that is vulnerable to change (Lohmann, 2012).

"*They lack the flexibility needed to rapidly adapt to ever-changing business environment, as they usually involve hard-coded requirements across multiple systems. With such ad-hoc solutions, it is difficult to verify compliance of business process specifications, and to monitor and ensure compliance of their execution.*"

" - (Turetken et al., 2011, p. 3)

2.5.3 Organisational Compliance

Adjusting data processes and complying with regulating documents is not only a matter of technical aspects; with robust systems that handle data correctly, employees can still violate the rules (Abdullah et al., 2010). Julisch, Suter, Woitalla, & Zimmermann (2011) argue that employees often violate the documents that state how data is supposed to be handled. According to Abdullah et al. (2010) it is difficult to achieve a compliance culture, where the employees know how to handle data in a correct manner, but if implemented it has great benefits. An information system can be made compliant in a more categorical way than humans, and are often used by organisations to ensure that data is handled appropriate (Bulgurcu, Cavusoglu, & Benbasat, 2010). Bulgurcu et al. (2010) argues that the weakest link when handling data is humans; hence it is of importance to have policies that guides the employee. The authors suggests that employees should get proper training, be rewarded for their compliance and that organisations make sure that the employee's daily tasks are streamlined for correct data handling (Bulgurcu et al., 2010). It is about infusing compliance into the organisation, and make sure that the employees understand why this is important (Abdullah et al., 2010).

2.5.4 Resource Allocation

Sadiq et al. (2007) argues that organisations mostly see compliance as a burden and not opportunities to improve the way their data is handled. However, the authors write that this partly is changing, more organisations expect to gain advantages from compliance. Abdullah et al. (2010) concur with this and write that valuing compliance measures remains difficult for organisations. The view that altering processes adds risk and complexity to the business is common, which could make data process compliance a project that only strive for the minimum requirements (Abdullah et al. 2010). Because of this, resources set aside for compliance is often short. Becoming compliant with all data processes is expensive, and could prove to be high-priced even for established businesses (Abdullah et al. 2010). Without enough resources, the changes made may not be sufficient, making the data processes of an information system poorly done (Abdullah et al. 2010; Sadiq et al., 2007). Moreover, Eggert et al. (2013) see a relationship between management support to compliance projects and the outcome. With management support the information system tend to have a higher compliance rate than without it (Eggert et al., 2013).

2.5.5 Documentation and Monitoring

As mentioned, the GDPR requires transparency in how an organisation processes its data (Regulation 2016/679/EU art. 12, EUR-Lex, 2016). As part of staying compliant with the law the organisation need monitoring tools; it is not only a question of being technically compliant, an organisation must be able to prove that they are (Abdullah et al. 2010). But keeping track of processes and monitoring compliance is not only for the regulative authority (Turetken et al., 2011). By understanding processes and documenting what and how data is handled the organisation can demonstrate compliance and notice if breaches occurs (Turetken et al., 2011). In this way Turetken et al. (2011) argue that organisations can prevent problems instead of violating the agreements. However, monitoring can prove to be problematic since it needs to be comprehensive in order to handle the amount of data and not to miss a breach (Abdullah et al. 2010).

"This leads to a need for comprehensive monitoring tools that have the ability to oversee all business operations, to issue breach reporting, and to provide incident recording." (Abdullah et al. 2010, p. 553)

2.5.6 Legacy systems

Designing new data processes that fit into the technological landscape of an organisation is not an easy task (Sadiq et al., 2007). Sadiq et al. (2007) argue that compliance requirements are hard to implement to distributed systems with legacy components which is common. It is not always feasible technically due to lack of knowledge or economically defendable to make legacy systems compliant (Julisch et al., 2011). The decision to include a legacy system could according to Julisch et al. (2011) require careful planning from employees with expertise in the current systems since it could turn out to be a lot of work.

Aspects from the GDPR relevant for our study and the compliance theory is summarised respectively in a table on the next page. These will be the foundation for our research.

Table 1: GDPR Aspects.

GDPR Aspect	References
Consent	(Ec.europa.eu, 2016), (Gilbert, 2016), (Lynskey, 2015), (Regulation 2016/679/EU Recital 32, EUR-Lex, 2016), (Regulation 2016/679/EU art. 6, EUR-Lex, 2016), (Regulation 2016/679/EU art. 7, EUR-Lex, 2016),
The Right of Access / The Right to be Forgotten / The Right to Portability	(Regulation 2016/679/EU Recital 63, EUR-Lex, 2016), (Regulation 2016/679/EU art. 17, EUR-Lex, 2016), (Regulation 2016/679/EU art. 20, EUR-Lex, 2016)
Territorial Scope	(de Hert & Czerniawski, 2016), (Gilbert, 2016), (Cuijpers et al., 2014), (Regulation 2016/679/EU art. 4, EUR-Lex, 2016)
Data Privacy Officer	(Regulation 2016/679/EU art. 9, EUR-Lex, 2016) (Data Protection Working Party, art. 29, European Commission, 2016), (Gilbert, 2016)
Transparency and Documentation	(Lynskey, 2015), (Gilbert, 2016), (Regulation 2016/679/EU art. 12, EUR-Lex, 2016)
Penalties	(Gilbert, 2016), (Lynskey, 2015), (Regulation 2016/679/EU art. 83, EUR-Lex, 2016)
Storage Limitation and Data Minimisation	(Koščík, 2017), (Regulation 2016/679/EU art. 5, EUR-Lex, 2016)
Pseudonymous Data	(Hintze, 2015), (de Hert & Papakonstantinou, 2016), (Regulation 2016/679/EU art. 4, EUR-Lex, 2016), (Regulation 2016/679/EU art. 11, EUR-Lex, 2016)
Encryption of Data	(Heimes, 2016), (Tankard, 2016), (Tankard, 2017), (Regulation 2016/679/EU, EUR-Lex, 2016)
Breaches of Data	(Hooson, 2015), (Bridge, 2014), (Lyons et al. 2016), (Regulation 2016/679/EU art. 33, EUR-Lex, 2016)
Privacy by Design / Protection by Default	(Cavoukian, 2010), (Cavoukian, 2012), (Danezis et al., 2015), (Hansen, 2016), (Hildebrandt & Tielemans, 2013), (Regulation 2016/679/EU art. 25, EUR-Lex, 2016)

Table 2: Compliance Challenges.

Compliance Aspect	References
Interpretation of Regulations	(Eggert et al. 2013), (Lohmann, 2012), (Turetken et al., 2011),
Ad-hoc Changes	(Lohmann, 2012), (Turetken et al., 2011), (Abdullah et al., 2010)
Organizational Compliance	(Abdullah et al., 2010), (Bulgurcu et al., 2010), (Julisch et al., 2011)
Resource Allocation	(Abdullah et al. 2010), (Eggert et al. 2013), (Sadiq et al., 2007)
Documentation and Monitoring	(Abdullah et al. 2010), (Regulation 2016/679/EU art. 12, EUR-Lex, 2016), (Turetken et al., 2011)
Legacy systems	(Julisch et al., 2011), (Sadiq et al., 2007)

3 Methodology

3.1 Research Strategy

When we began our study, our problem area was not covered to a large extent in existing research, and the GDPR was a relatively new aspect for organisations to consider. In order to find a suitable way to approach our research, we began by examining our research question. As we aimed to investigate in the GDPR a topic where little previous understanding exist and compliance in information systems, our open research question became our outset. With this in mind, we decided to conduct a qualitative research as this is according to Recker (2013) most appropriate for an open "what" question. Recker (2013) argues that qualitative studies provide richer and contextualised data compared to quantitative, which is desirable when exploring or describing a new phenomenon. In this way we could conduct interviews that allowed us to collect details about what challenges organisations face concerning the GDPR. Since it is the effects of the regulation that was studied we wanted rich input to help us understand the problem area. Combined with the fact that relatively little empirical research have been done in the field, we found a qualitative approach the most suitable as it can provide insight to problems that might not previously be highlighted (Jacobsen, 2002; Recker, 2013).

We have conducted a qualitative research since our goal have been to understand a new phenomenon affecting our problem area. Therefore, the research have a set of factors that gives us a clear idea where to begin our study (Bhattacherjee, 2012). We have systematically studied a phenomenon to broaden the understanding of the impact of GDPR on data processes by aiming to find patterns, scoping its extent and magnitude. This will according to Recker (2013) give initial insight to a problem, which in our case is compliance and the GDPR. We used the available literature to frame our problem area and understand what parts of the GDPR that is considered to be a challenge for compliance. This guided us when designing our interview guide and selecting interviewees, which Recker (2013) see as a good approach.

One of the biggest challenges with accomplishing a qualitative research are getting access to a site (Recker, 2010). We contacted several organisations in order to get a broad understanding of the problem area. We aimed to conduct interviews with key personnel such as the security manager and project leaders, as they have insight into the processes that will be affected as well as what the organisations will do to comply with the GDPR. We employed coding, a technique based on qualitative data, which is suitable for this kind of study (Kvale, 1996; Recker 2013). In the model below we have summarized our research plan.

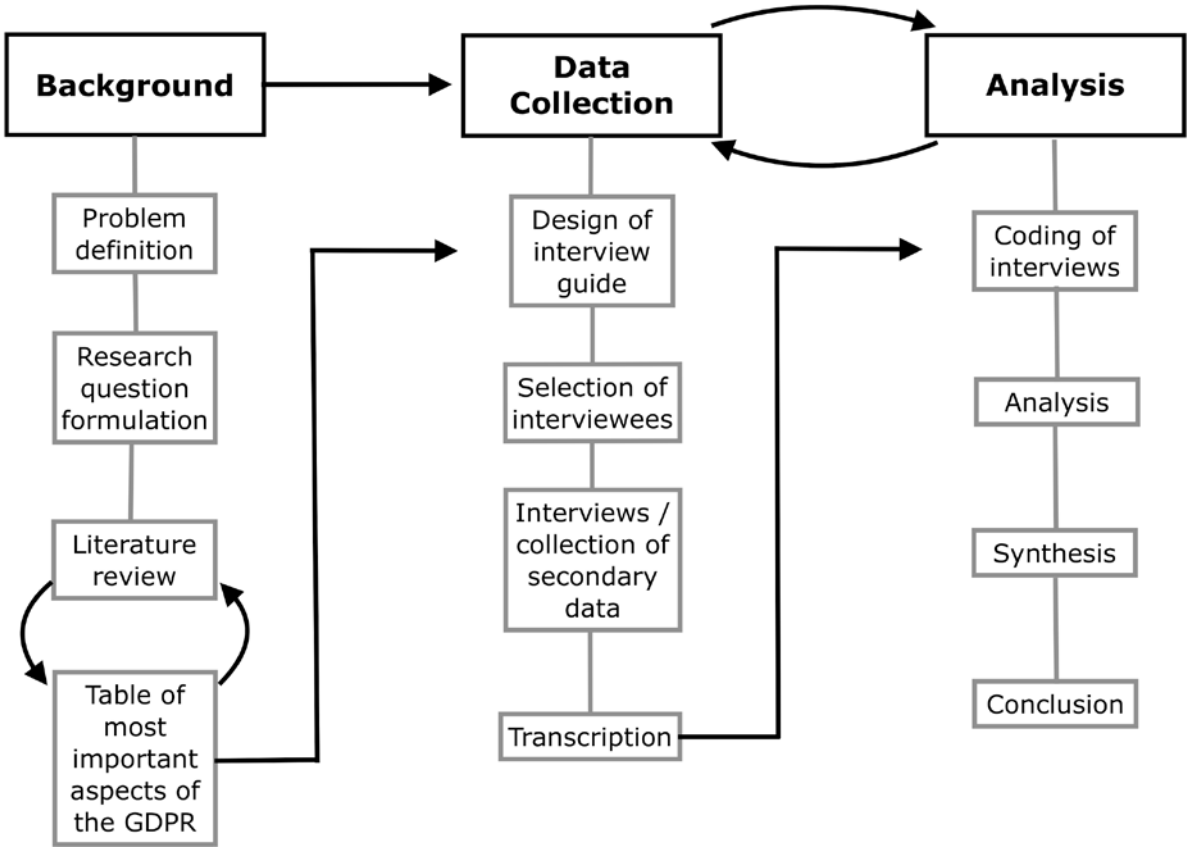

Figure 1: Research Plan.

3.2 Design of interview guide

When we designed the interview guide we used our literature review as a foundation. We followed the recommendation of Recker (2013) to break the interview guide into several parts that cohere with categorisation in the literature review, beginning with some more general questions. This was done so that we could ask questions about the various fields that we have decided to include in our report and to establish a clear structure for us and our interviewees. We did not include the theory in the interview guide, as we wanted to use the GDPR as a lens for our research. The organisations selected for our study were well aware of the GDPR, but not as likely to be informed about compliance theory. Therefore we focused on the legislation rather than the less approachable compliance theory. Some categories mentioned in the literature review, such as levels of de-identification, are neither part of the interview guide. This is because these categories serve to give the reader the necessary understanding of key concepts in the GDPR. Questions about these concept would not serve our purpose, and are therefore not included.

As our interviews used the format of semi-structured, the interviews had a set of questions that was already decided. This worked as a framework for us to lead the interview, but we still had the possibility to ask further questions about subjects that was being mentioned during the interviews. Bhattacherjee (2012) and Recker (2013) argue that having a semi-structured interview also opens up the possibility of the interviewee asking questions creating a two-way communication which make it easier for more in-depth and sensitive questions. This made our

interviews more into dialogues about the GDPR, which allowed us to find challenges not mentioned in the theory.

As the GDPR is a comprehensive piece of legislation it would be unreasonable to believe that all interviewees would be able to answer all aspects. Because of this, we started every new concept with a broader question, where the respondent could let us know whether or not they had insight into this field. In this way we avoided spending time on aspects that the respondent did not know. This adds to the flexibility of the interview, which is desirable in semi-structured interviews (Myers & Newman 2007; Recker, 2013).

In the table below is the different aspects of the GDPR included in the interviewee guide and what question they are represented in. Our interview guide can be found in the Appendix.

Table 3: Design of interview guide

Categories	Interview Question
Role of the Interviewee	1.1-1.3
Consent	2.1-2.4
The right of Access, the Right to be Forgotten and the Right to Data Portability	3.1-3.6
Territorial Scope	4.1-4.2
Data Privacy Officer	5.1-5.3
Transparency and Documentation	6.1-6.2
Penalties	7.1
Storage Limitation and Data Minimisation	2.5
Pseudonymous Data	8.1-8.3
Encryption of Data	9.1-9.3
Breaches of Data	10.1-10.2

Privacy by Design and Default / Data Protection by Design and Default	11.1
Most difficult aspect of the GDPR	12.1

3.3 Selection of interviewees

We used what Recker (2013) call purposive sampling, which means that we actively chose organisations and interviewees with the right properties for our research. Which in our case meant organisations that handle personal data either as a data controller or as a data processor, preferably large (more than 250 employees). With this in mind we contacted several organisations, both private and public. At these organisations we looked for people who worked with the implementation of the GDPR. We also used snowballing, which according to Myers and Newman (2007) is a concept where the interviewers ask the interviewees of contact information to other interview objects. There are known risks with this such as, getting in contact with persons with similar positions or situations as the one who provides the contact (Myers & Newman, 2007). To make sure that this did not happen we made sure that if we got a contact from someone in a management role they gave us contact information to someone with a different role (e.g. security) and vice versa. Most interviewees are employed to work with IT within one organisation but we had one consultant who could speak in more general terms giving us an overview of the work with GDPR.

Table 4: Table of interviewees

Interviewee	Position	Size of the Organisation	Job Description	Date and type of interview
Alex	Security Manager	More than 250 employees.	Are in charge of IT-Security and Information-Security. Are also in charge of the preparation for the GDPR as well as customer relations regarding GDPR.	27th of April, 2017 Face-to-face
Bob	Project manager & Portfolio Owner	More than 250 employees.	Are in charge of projects in the organisation, at the moment most of them are just starting out.	27th of April, 2017 Face-to-face
Charlie	IT-Security Architect	More than 250 employ-	Have responsibilities such as Incident Response and	9th of May,

	50% Manager IT-Security Group 50% IT-Security responsible 25%	ees.	have just finished the report on the first step in preparation for the GDPR	2017 Face-to-face
Douglas	Executive Director	Less than 250 employees.	Are responsible of all the organisations processes, continuity management, all contracts with outsourced suppliers, IT-development and IT-operations	10th of May, 2017 Face-to-face
Eric	Head of production development	More than 250 employees.	In charge of the development of the organisations production system. Which is both frontend and backend.	15th of May, 2017 Skype
Fred	Senior Consultant	More than 250 employees.	Are helping other organisations becoming mature in their GDPR processes.	18th of May, 2017 Telephone

3.4 Collection techniques

As mentioned, we conducted semi-structured interviews as a mean for data collection. Since we explored a new area of interest, we wanted understand the perceived challenges of the compliance with GDPR in order to properly address issues not mentioned in the literature. A qualitative method gives you understanding of things that would be unseen with quantitative (Myers & Newman 2007). An interview can be divided into four categories; structured, unstructured or semi-unstructured, and group interview. We conducted semi-structured interviews for a number of reasons. By doing semi-structured interviews we had a prepared script, which is open for adjustments during the interview. Having an interview guide makes it possible to prepare the subject and let them know what the interview will be about, to give an idea of what type of questions that will be raised (Recker, 2013). It also encourages a two-way communication that could make things more comfortable for the interviewee as the character of the conversations is less of an interrogation. Which can lead to more open answers and richer data to be collected. (Recker, 2013).

Moreover, this allowed us to do interpretation while conducting the interview. This is according to Kvale (1996) an important part of the interview-process. If questions are blindly asked each and every subject, we would have ended up with too much data. Instead, we adjusted the script to the interview. As a result the collected material will be less but with higher quality (Kvale, 1996). We conducted our interviews preferably face-to-face but in two cases that was not a possibility and therefore we had to them on skype and per telephone.

In order not to take the method for granted and simplify it as a mean of data collection, several steps of precaution should be taken (Myers & Newman 2007). With all types of interviews there is a risk of making mistakes, such as; lack of trust, lack of time, or ambiguity of the language (Kvale, 2006). We sent the interviewee guide beforehand, allowing the respondent to prepare itself, but also let them know of our intentions. Being honest about your purpose and not trick someone into an interview is an important aspect (Kvale, 2006). We offered all respondents confidentiality, making clear that their identity nor the organisations name would be revealed. However, we asked permission to reveal the positions of the interviewees as it is of importance to the study. Yet, too much trust can be a bad thing, as it can result in manipulation (Kvale, 2006). We tried to keep it as formal as possible at all times to avoid this. The interview is a delicate process (Kvale 2006; Myers & Newman 2007) and we aimed at keeping a balanced distance to the interviewee subjects.

3.5 Data analysis method

As we gathered data from interviews, the best way to evaluate the data is by a qualitative analysis (Bhattacherjee, 2012). Especially text documents such as transcripts from interviews are fitting for a qualitative analysis (Bhattacherjee, 2012). One of the most common ways to analyse data from interviews is coding (Recker, 2013). This entails labelling and structuring the interviews into categories (Recker, 2013, Bhattacherjee, 2012). In this way we organised the data around key themes that we found. There are different approaches to this (Bhattacherjee, 2012), where we found open coding the most straightforward and best suited for our study of the GDPR and compliance in information systems. With this approach we organised the data into more general concepts, which according to Recker (2013) and Bhattacherjee (2012) reduces the number of categories to keep track of. We used the software Annotation to help us with the coding. It allows the user to create categories, subcategories and colouring of the text.

We did not begin the coding without any idea what to look for. According to Walsham (2006) the literature review offers a ground to start from and an idea in what direction you are heading with the coding. For example, the different aspects of the GDPR first served as a guide for the interview, and then a way to approach the transcribed data. Moreover, this gave our method some continuity (Walsham, 2006). When we were done with the coding based on the GDPR aspects, we further coded the selected paragraphs in accordance with our theory. For instance, we first found challenges expressed by the interviewees of a specific aspect of the GDPR, we then analysed if it fitted into the challenges highlighted in the theory. In this way we could understand where the challenges of GDPR adjustment emerged.

As mentioned, we analysed the data as we conducted the interviews as well. This approach is argued for by Kvale (1996) as a way to keep down the amount of text but still get quality results. Time is limited when sitting face-to-face with the interviewee, but it is possible to steer the interview in a direction to limit the amount of data. We planned the interview guide with

more open questions to begin with, if the interviewee had insight to the specific field, we could dig deeper. Otherwise we left the topic behind and moved on (Kvale, 1996).

Below are two tables with the two separate codings that we have done. The first table contains the paragraphs that is connected to the different aspect of the GDPR that was covered in the literature review. The second table contains paragraphs based on the ones that was highlighted in the first table, but now arranged according to the compliance challenges presented in the literature review.

Table 5: Coding for the aspects of the GDPR

GDPR	Alex	Bob	Charlie	Douglas	Eric	Fred
Consent	P. 12, 14,16	P. 20, 22	P. 16, 18, 20	P. 14, 18, 20, 70	P. 10, 12, 28	P. 16, 18, 20, 22
The Right of Access, the Right to be Forgotten and the Right to Data Portability	P. 20, 22, 24, 26, 28, 30, 32	P. 34, 36, 40, 42, 44	P. 26, 28, 38, 40, 44, 78	P. 22, 34, 90, 92	P. 14, 16, 28, 30, 32, 34	P. 34
Territorial Scope	P. 34, 36	P. 46, 48	P. 48, 50, 52, 74, 78, 80	P. 46	P. 46	P. 38, 40
Data Privacy Officer	P. 38, 40, 42, 44, 46,	P. 50, 52, 54, 56	P. 46	P. 44, 46, 52, 54	P. 40, 48, 52, 54	P. 42, 44, 46, 48
Transparency and Documentation	P. 48, 50, 56, 58	P. 58, 60, 62	P. 56, 90	P. 56, 58, 60, 66	P. 36, 42, 56, 58	P. 36, 52
Penalties	P. 60	P. 64, 66	P. 44, 52, 72, 74	P. 68, 72	P. 44	P. 60, 62, 80
Storage Limitations and Data Minimisation	P. 12, 16, 24, 28	P. 14, 28	P. 30, 54	P. 28, 88	P. 18, 40	P. 24, 26, 28, 30, 32, 76, 78
Pseudonymous Data	P. 62, 64, 70, 72, 74	P. 74, 76, 78, 80	P. 62, 64, 66	P. 74	P. 18, 22, 24, 38	P. 64, 70
Encryption of Data	P. 66, 68, 70, 72	P. 78, 80	P. 62, 64, 66, 68, 70, 72	P. 74, 76, 78	P. 60, 62	P. 64, 66, 68, 70
Breaches of Data	P. 74, 76, 78, 82, 84	P. 82, 86, 88, 90, 92, 94		P. 80, 82, 84	P. 64, 66, 68, 70	P. 72, 74
Privacy by Design and Default	P. 86, 88, 90, 92	P. 96, 98, 100, 102, 104	P. 40, 42	P. 62, 86		P. 54, 56, 58

Table 6: Coding for compliance challenges.

Compliance Challenge	Alex	Bob	Charlie	Douglas	Eric	Fred
Interpretation of Regulations	P. 28, 30, 42, 43	P. 52, 56	P. 38	P. 34, 44, 46, 88, 90	P. 54, 68	P. 16, 18, 40
Ad-hoc and Generic solutions	P. 94, 96	P. 28, 100	P. 40	P. 76		P. 40, 56
Resource Allocation	P. 38, 48, 60	P. 50, 58, 64	P. 44, 46, 52, 72, 74	P. 44, 56, 60	P. 44	P. 36, 60
Organisational Compliance		P. 94	P. 38, 44, 52, 84, 88	P. 20, 60, 66		P. 82, 84
Documentation and Monitoring	P. 48, 58, 74, 110	P. 58, 84	P. 48, 56	P. 36, 56, 80	P. 64	P. 36, 40, 52, 72
Legacy systems	P. 28, 48, 66	P. 34, 36, 40, 42, 44, 100	P. 38, 40, 42, 56, 88	P. 14, 34, 56, 76 90		P. 56, 58, 76
Competing Compliance Measures	P. 24, 26, 28, 30, 40	P. 44, 100	P. 38	P. 18, 34, 76, 80, 82, 90	P. 12	P. 16, 18

3.6 Reliability

Rigor for our qualitative research was not achieved without thought. Klein and Myers (1999) points at the subjectivity of interpretive research which makes it more difficult to generalise the findings. To make sure that we maintained reliability in our research we coded the transcripts of the interviews separately. We then merged our separate results by comparing and combining them into one coding. Agreeing on one coding made sure that we both had the same understanding of the transcripts. In this way we separately ended up with similar conclusions about the material we gathered (Bhattacherjee 2012). We have used open question as this makes it possible for the interviewees to give their full answer. Moreover, we have recorded all interviews with the help of recording applications on our mobile phones.

According to Jacobsen (2002) it is important for the interviewee to feel comfortable during an interview to be able to achieve the best possible result. There are several ways of making sure that this is done. We have conducted the interviews at the interviewee's office, or where they felt most comfortable, we gave them the chance to decide where to conduct the interview. We also sent them the questionnaire framework beforehand with an approximation of the duration of the interview so that they could be prepared and be able to set aside the right amount of time from their day (Jacobsen, 2002).

3.7 Validity

As with all qualitative research, internal validity is hard to achieve (Bhattacherjee, 2012). In order to determine that our findings were confirmable we sent the finished thesis to the interview participants. In this way they could confirm that our inferences about the impact of the GDPR was reasonable, and see that their transcripts were used in a proper way (Bhattacherjee, 2012).

The external validity of our findings and conclusions, also known as the transferability (Bhattacherjee 2012; Recker, 2013), was assured by rich descriptions of how our research was done. This allow others to get an understanding if the findings are applicable to other settings. Moreover, we conducted interviews on different sites, which allowed us to search for patterns that was not bound to a specific context. The interviewees were selected based on organisation and position, making sure that they had knowledge about the GDPR and how they will adapt. This strengthen our generalisability (Bhattacherjee 2012; Recker, 2013).

3.8 Quality and Ethics

There is a notion that qualitative research is inherently ethical in itself compared to its counterpart quantitative research (Brinkmann and Kvale, 2005). Brinkmann and Kvale (2005) argue that this is a false idea and that the interview is potentially one of the most dangerous forms of research. They also propose that ethics is the result of a cultural discourse, which science is a part of this and therefore must be seen from an ethical lens. A qualitative researcher must not only respect its subjects but must also the context (Brinkmann and Kvale, 2005). This is highly applicable to our research since we, as researchers interact in different ways with the interviewees and the organisations where they work. Even if it is not always explicitly said or written, researchers are supposed to follow an ethical standard when conducting science (Brinkmann and Kvale, 2005). What is unethical is not always illegal. There are a few ethical tenets that are widely accepted within the scientific community (Brinkmann and Kvale, 2005), which we have followed when conducting our research. Firstly all participation should be voluntary and done with consent (Brinkmann and Kvale, 2005). Both when we first contacted the interviewees and before the interviewee started we made sure we had clear consent for conducting the interview and recording. Anonymity or confidentiality should always be offered someone who participates in an interview or similar (Brinkmann and Kvale, 2005). We have only been able to offer confidentiality as we have met in person during the interview. We gave all the interviewees fictional names to improve the readability. We have removed names of organisations and the involved persons to minimize the risk of identification. The subject should also be informed about the study before they participate. In order to comply with this we sent our interview guide to potential participants. Even if our interviews were semi-structured and partly followed the guide, it contained all of the issues that would be brought up, which Recker (2013) argues for.

3.9 Bias

Research overall are biased because it is done by humans and prone to the same types of wrongdoings as other human activities (Norris, 1997). As a measure to control our bias we have let other people read our research and give their take on our work (Ehrlinger, Gilovich & Ross, 2005) Ehrlinger et al., (2005) expands on the subject and explains with their research that we are more prone to miss our own bias then we are at detecting biases in other. Since it can be problematic to detect our own biases we have tried being transparent in our method of research and how we have conducted it. This includes our findings which are shown in detail, such as our interviews.

4 Results

4.1 Consent

It will be a challenge for organisations to tackle the requirements surrounding consent in the GDPR, as they manage consent with customers in many situations (Bob, P. 22; Alex, P. 10; Douglas, P. 20; Charlie, P. 18, 20; Eric, P. 10; Fred, P. 16, 18). For instance a business to business organisation might still have some communication with the end customer, therefore it is important that they understand what consent their customer has from the end user (Bob, P. 22). Another example brought up by Bob (P. 22) is that one challenge will be to keep the deals with data controllers generic while still giving the customers individual configurations. Currently, data processor have had the possibility to form their services to their client's needs, now they have to be more specific as their customer are the ones with consent from the customers, not the processor (Alex, P. 10).

The organisations need to be clear on how they will process the data and that the services are streamlined in order to ensure that personal data only are in the way it should (Alex, P. 10). The key here is communication so that everyone are aware of how processes works and that the customer gets the right consent to begin with (Alex, P. 10). Eric (P. 10) has the same argument, that communication with their customers is the biggest change. The customer needs to be informed about the new conditions during the change to the GDPR. The customers need to accept the conditions on several points and the conditions need to be approved (Eric, P. 10; Douglas, P. 14, Fred, P. 16). Fred (P. 16, 18) extends this and explains that a lot of organisations will try to go through other legal grounds to lawfully acquire data because if you need consent for all your collection purposes it will very complicated. Two of the organisations have other laws they have to follow that overrides the GDPR in some aspects (Charlie, P. 18; Douglas, P. 14). This has to be explained so that the customers understand that the GDPR are overruled in this case while writing a contract (e.g. storing personal data for 10 years as a bank) (Douglas, P. 14). This is something they haven't decided how to formulate (Douglas, P. 22).

There are some differences considering PUL (current Swedish law for collection of personal data) and the GDPR according to Douglas (P. 18), where the new legislation is a lot tougher, and that you cannot manage customer data with the same ease as previously. Eric (P. 12) believes that they are safe because they worked closely with PUL and have established ways of getting access to data and other parts of integrity.

4.2 The right of Access, the Right to be Forgotten and the Right to Portability

There is a need to remap the data in legacy systems according to most of the respondents (Bob, P. 34, 40, 42; Alex, P. 28; Charlie, P. 38; Douglas, P. 34, 90; Fred, P. 76) in order to effectively find data stored in their information systems. Since the organisations have information in their archives from former data collection, it exists personal data that they currently are unsure if they can access (Bob, P. 34; Charlie, P. 38; Alex, P. 28; Douglas, P. 34). In order to do this too effectively and be able to oblige to the laws a system mapping is required (Bob, P. 34; Charlie, P. 38; Alex, P. 28). The organisations needs to identify where and in what system the user data resides (Bob, P. 40, 42). It comes down to understanding the technological landscape of the organisation and create an indexed structure for all data, allowing the organisation to find, fetch or delete personal data (Bob, P. 36, 42, 44; Alex, P. 28; Charlie, P. 38; Douglas, P. 34, 90; Fred, P. 76). Eric (P. 14) see their customer database as structured enough to comply with access and deleting. It is rather a question of making these functions more accessible through their webpage, simplifying both for the organisation and the customer (Eric, P. 14). As a processor, Alex (P. 20) also see self-service as way to compliance, if the customers can access their systems to delete the information themselves, an unnecessary step is removed. Alex (P. 24, 28) points at the importance not to keep data where it does not belong. This is the case at the moment, where data is redundantly stored along the data process as a safety measure (Alex, P. 24, 28). This is problematic if all data have to be removed with a short time frame (Alex, P. 24, 28). From the controller side Douglas (P. 34) argues that they will have to go through all their outsourced systems to make sure that it will be possible to get all customer data with ease.

Mapping the structured data in databases is technically achievable (Douglas, P. 90; Charlie, P. 38, 44; Bob, P. 42). Files created by employees like excel sheets and other lists of personal data will be very difficult to find and control (Douglas, P. 34, 92; Alex, P. 28; Charlie, P. 44). Charlie (P. 44) see very different levels of data managing in his organisation, and expect this to be long and difficult work to harmonize the way personal data is processed. To understand where their data resides, they will have to employ staff full time to classify data (Charlie, P. 44). Alex (P. 28) also see difficulties with data that is not indexed. Plain text could be considered personal data, and must be thought of when striving for compliance (Alex, P. 28). Alex (P. 96) also see that the organisations will patch together the processes to be able to follow the GDPR, something that he believes that most organisations will do (Alex, P. 98).

Removing specific individuals from a system or make their data portable is currently not possible without issues rising (Alex, P. 18; Charlie, P. 38; Bob, P. 44). Alex (P. 18) see a need to develop more granular deleting processes. At the moment entire tables might have to be removed if a customer demands to be forgotten by the system (Alex, P. 40). It is also unclear how the right to be forgotten compliance is going to affect other systems, where technical controls will have to be implemented to ensure that things run smoothly (Alex P. 40). Portability poses problems as well. Bob (P. 44) argues that generic solution to this is required, so that one file can be delivered to the individual that requests their data. Charlie (P. 38) say their system do not support portability today, which will have to be managed by changed guidelines for data processes. The organisation aim to have researchers move their data seamlessly between universities (Charlie P. 38).

There are however exceptions to the right to be forgotten (Charlie P. 38; Douglas P. 34, 90). Other laws override the GDPR that forces the organisation to keep certain data (Charlie, P. 38; Douglas, P.34, 90). This must be considered when designing the processes that are supposed to comply with the GDPR (Charlie, P. 38; Douglas P. 34, 90).

4.3 Territorial Scope

Neither Bob (P. 46), Alex (P. 34) nor Eric (P. 46) have any data outside of EU and aim to stay within the union's borders. The biggest problem they see with the law are cloud services and if they are outside of EU (Alex P. 34) or if their backups reside outside of EU (Eric P. 46). As long as the organisation write a contract with the cloud services operator that make sure that they have to handle the data inside EU the organisation should be fine (Alex P. 36). Fred (P. 38) adds that most of his customers have their data storage in Sweden or at least in the Nordics. He continues with that it shouldn't be seen as a goal to keep all the personal data inside of EU but rather understand the organisation's data processes. If there is an understanding of how the data flows, the compliance of moving data outside of the EU is not too difficult (Fred, P. 40).

Both Douglas (P. 36) and Charlie (P. 48) have data outside of the EU. To still be compliant the organisations have written contracts with their supplier on the subject of personal data and that they are aware of the GDPR (Douglas, P. 36; Charlie, P. 48). What Charlie did as well was to get a promise that personal data should be managed inside EU (Charlie, P. 48). Since they have data all over the world they have to inform all employees of what they can do with their data (Charlie, P. 50). This will lead to a lot of education about how to use personal data (Charlie, P. 52). The organisation are starting a one-stop shop where you can go and ask about the personal information that you have or will gather and they will tell you how you have to handle it (Charlie, P. 52). Charlie (P. 52) also wants to have steps in the processes that makes all employees at least think about GDPR when they are starting a new project.

4.4 Data Privacy Officer

Most organisation that have been interviewed have employed or are in the process of employing a DPO (Bob, P. 50; Alex, P. 38; Douglas, P. 44; Charlie, P. 46) and others need to know more about the position before they decide anything further (Eric P48). Fred (P48) is adding that it is a must to add a DPO, and that organisations should find one in house. How organisation select the DPO are a little bit different. The approaches differ between a more technical approach where they choose someone with a technical background (Bob, P. 52; Alex, P. 38) a legal approach (Douglas, P. 46) where they are considering a mixture of both, (Eric, P. 48) and where they aren't quite sure who to choose (Charlie P46). Some organisations are obligated to have a DPO because of the amount of sensitive data that they the organisation handles (Bob, P. 54; Alex, P. 38). Alex and Bob's organisation will have two DPOs, one for the organisation that owns their organisation and one at their organisation, the idea is that they can get help from each other (Bob, P. 50; Alex, P. 38). What most organisations agree on are that they will revisit the subject of the DPO, if it is a working strategy or if they have to change it (Bob, P. 52; Bob, P. 56; Alex, P. 44; Douglas, P. 52). Bob (P54) further explains that as it is the Chief Information Officer (CISO) that also will be the DPO at first, and will be having two roles which is too much for one person to handle, therefore they want to distribute

the responsibility as soon as possible. Preferably having the DPO working side by side with the CISO (Bob, P. 54). Alex (P. 42) adds that it shouldn't be someone working in operational IT, as it will be for them now, but rather someone who is closer to the legal department but still has a lot of knowledge about the processes. This is something that many of the interviewees consider a future requirement, someone competent in both fields (Eric, P. 54; Alex, P. 42; Douglas, P. 44, 47; Bob, P. 56).

Overall, the interviewees mention responsibility and ownership for data processes as an important aspect (Fred P. 82, 84; Charlie P. 38, 44; Bob P. 92). The importance of distributing and anchoring responsibility for data processes is used as a control mechanism for that to ensure that the processes are compliant (Fred P. 82; Bob P. 92).

4.5 Transparency and Documentation

At the moment most of the organisations are trying to improve the structure in their systems as a way to make it more transparent (Bob, P. 58; Alex, P. 48; Douglas, P. 56; Charlie, P. 56; Fred, P. 36). The only organisation that already thought they had a good enough structure to handle the transparency and documentation to begin with (Eric P. 36, 56) where Eric, however he saw this as an excellent moment to better the structure their system, a discussion they have had for quite some time (Eric, P. 42). Some of the organisations regard their systems to be compliant concerning transparency and documentation to some extent (Douglas, P. 56; Eric, P. 56). This made possible since they have maps over their processes and registries over their systems (Douglas, P. 56; Eric, P. 56). Most organisations understand that they will need to comprehend and document their process flows in detail (Alex, P. 48; Douglas, P. 14, 56; Charlie, P. 56; Charlie, P. 88). Fred (P. 52) adds that it is very important to document and that it is communicated to all stakeholders within the organization.

Alex (P. 48) says that they have focused most on the demands of logging processes. With logging the organisation records who accessed what at what time, and aim to do this even more. He also explains that the customers (data controllers) wants to have a lot more transparency, so from now on they have a lot more meetings with their clients (Alex, P. 50). Alex (P. 56) argue that they need to be more transparent about how they process data towards their clients, even give them access to parts of their system. Otherwise they might lose customers since there will be further demands from controller to processor (Alex, P. 56). Douglas (P. 60) and Charlie (P. 38) see mapping all personal data as a problem as the files could be stored on old computers, in excel sheets or similar files. According to them the best solution for this is education and workshops, creating awareness and clear guidelines in order to have more careful employees when using personal data. (Douglas, P. 66; Charlie, P. 88)

4.6 Penalties

Most of the interviewees regard the penalties to have influenced the GDPR to become attended in the way it is (Bob, P. 64; Alex, P. 60; Douglas, P. 68; Charlie, P. 44, 72; Fred, P. 60). Charlie (P. 72) are certain that it is the penalties that made it discussed at management level.

"[...] it was the fines that made it end up at management level, suddenly it had moved three pay grades up." - Charlie P. 72

The concern for the new law on a management level have increased funding for projects for GDPR compliance (Alex, P. 60; Charlie, P. 72). According to Charlie (P. 72) it is now possible to compare fines with costs, which makes funding more likely. Many of the projects are welcomed by the IT personnel since they have been needed. This would not be possible unless extra money came into the picture (Charlie, P. 74). The penalties create some dilemmas that already have been noticed by Alex (P. 58) who explains that while writing contracts with clients, they have started to push over as much as possible of the responsibility on the data processor, which in this case is their organisation. If the contracts do not clearly state who has the responsibility, they will risk both to not getting paid for their service and pay the fines for noncompliance (Alex, P. 110).

Eric (P. 44) have respect for the high penalties but he does not think that the organisation should change because of that, he wants them to change because it will improve their processes. Most of the other interviewees agree that this is an excellent moment to improve what they have wanted to change for years, or at least to have a way to motivate these projects. (Charlie, P. 52; Alex, P. 60; Douglas, P. 60; Bob, P. 64).

Bob (P. 64), Fred (P. 60) and (Charlie, P. 72, 74) consider the penalties an eye-opener for added business value. It is not just that organisations are being compliant of the GDPR by changing organisations improve transparency and protection of personal data, which comes naturally in the period of digitalisation (Bob, P. 64; Fred, P. 60).

4.7 Storage Limitations and Data Minimisation

Data minimisation is difficult since this is a new way to approach data collection (Douglas, P. 88; Eric, P. 40; Alex, P. 12; Bob, P. 14; Charlie, P. 30; Fred, P. 26, 56), mostly because data have been something that you at all times have tried to collect, because there might be use for it in the future. This changes with the GDPR according to Alex (P. 12) and Charlie (P. 42), now all organisation have to be careful with why they collect the personal data (Douglas, P. 88; Alex, P. 12; Fred, P. 24). Data processors will need close communication with their clients in order to minimize data collection and storage (Bob, P. 28). They need to look over shared data together and collaborate to streamline their data processes to only hold the necessary information (Bob, P. 28). Douglas (P. 88) also see the need to have a dialogue with their contractors to deselect data that ended up in a process when data minimisation still was not a concern. Alex (P. 16) agree that it will come down to communication, it will be tiring work to go through, but not too technically complex. In the end the organisations will have to scrutinize their processes, to see if the data handled is aligned with the purpose for which it was collected (Alex, P. 12; Douglas, P. 28; Eric, P. 40; Charlie, P. 30). It is also important to understand your systems, investigate to see where personal data exists and how it flows. Where personal data is not needed, it should not exist. Customer specific information should be in certain systems (Douglas, P. 14). An aspect of this is to see to that employees know what systems they are allowed to put customer data in (Douglas, P. 34). Alex (P. 28) see difficulties with unstructured data like text, which until now have not been considered personal. There might be problems if this needs to be compliant with GDPR (Alex, P. 28).

Alex (P. 24) regard some former processes to have redundant data. Personal data have been kept in several places along the way to its destination, something that will have to change (Alex, P. 24). Eric (P. 30) see it as an opportunity to give added value to the customer by allow them to see how they act online. If the organisation can show why they need to collect the

data, it will be accepted by their customers and therefore fulfil its purpose (Eric P. 40). In other cases personal data is removed 6-12 months after an individual stopped being customers to follow the current rules of PUL (Eric, P. 30, 32).

There are exceptions to the storage limitation and data minimisation. Research data and information concerning finance is often excluded due to other laws that override the GDPR (Douglas, P. 28; Charlie, P. 30).

4.8 Pseudonymous Data

The ideas about pseudonymous data goes apart between the interviewees. Bob (P. 78) and Alex (P. 62) argue that this is not done to any extent at the moment, mostly because encryption have been the recognized way of securing data. According to Alex (P. 62) they are running tests with systems that pseudonymous data, and remove the connection to any social security number. Eric (P. 18, 20) have detached individuals and data for some time. There have been no real reason to keep them together, and for security measures the data have been kept apart. It is however reconnectable if the organisation wishes to do so (Eric, P. 18, 20). In other cases, the organisations will go through their data processors to whom they outsource a lot of data (Douglas P. 74). Charlie (P. 62, 64) argue that pseudonymous data have been used as a technique for scientist and researcher for a long time. In order to protect data and still be able to see development and patterns over time, it is crucial to reconnect data to individuals (Charlie P.62, 64). Among researches there is well established mind set to protect data that concerns individuals, and keep their sources are protected (Charlie P. 64). Other organisations do not collect too much information about their customers, but realises that this could be useful in the future. Therefore, Eric (P. 22) says they end up in a grey-zone where they could collect more, but then would have to work more with pseudonymisation or find other ways to comply with the GDPR. Moreover, they will avoid handling payment info and other sensitive data through third party plugins (Eric P. 38). Fred (P. 70) explains that pseudonymization hasn't been known for that long and that is the reason that most organisations do not use it, but he argues that this will change and that his clients will use a combination of encryption and pseudonymisation.

4.9 Encryption of Data

Encryption is considered to be an established approach to protect data (Bob, P. 80; Alex, P. 66; Douglas, P. 78; Charlie, P. 64; Eric, P. 60; Fred, P. 64). According to Bob (P. 78), Alex (P. 66) and Charlie (P. 66) encryption could however be risky, encryption-keys and the data could become corrupted, resulting in loss of data. Charlie (P. 64, 66) points at the risk of losing everything if the data and the backup is encrypted, despite this it is still widely used to protect sensitive data linked to individuals. Bob´s (P. 78) organisation deal with encryption on a daily basis and see it as an accepted way to secure data, but that pseudonymisation probably will increase as a mean to bypass the GDPR legislation. According to Alex (P. 66) their organisation do not currently encrypt all data, but that this will change. More databases will become encrypted step by step, when new versions of the database will be made. Charlie (P. 68) believe they will see an increase in interest concerning encryption. Douglas (P. 74) says that they are in dialogue with their data processors, but argues that the banking industry has

rigid encryption as it is. This encryption is however more connected to transferring data rather than storing, which Eric (P. 60) agrees with.

4.10 Breaches of Data

Bob (P. 82), Alex (P. 74), Douglas (P. 80) and Eric (P. 64) all see the increased obligations surrounding data breaches as a challenge, or at least, that this issue must be looked into. They also agree that changes will have to be made in order to comply with the requirement to report back both to authorities and customers. It could not be achieved through the existing systems without modification. But, some of the organisations already have a practice for data breach detecting, this is however often limited to parts of the information system and needs to be extended (Douglas, P.80, 82; Alex, P.76; Eric, P. 66). The banking industry have well-structured ways to handle attacks, but also reporting to authorities according to Douglas (P.80). Douglas (P.82) believe most things to handle a breach are in place, but personal data will have to be incorporated into this. Alex (P.76) also argue that the monitoring of data breaches is already done through logs implemented in the system, however, these are not aligned with GDPRs broad definition of what is to be considered personal data. Eric (P. 66) point at good possibilities to contact both individuals and authorities with the current systems.

Exactly how the organisations will go about and implement data breach detection and monitoring that allow to see what data that is affected, in a way that is compliant with the GDPR is not clear (Bob, P. 82; Eric, P. 66; Douglas, P. 84). Bob (P. 82) do not think it is necessary to develop a system for this themselves, and that they are in the process of buying a solution. Bob interpret data breach compliance as big changes, but that they will be scalable and implemented top-down as clear guidelines for each responsible system-owner to follow. Douglas (P. 84) and Alex (P. 82) argue that extended logs for tracking data along with incorporating current breach measures to include more personal data is sufficient. Eric (P. 70) see it as a fairly straight forward technical problem that would be solvable, they just have to figure out exactly what is demanded by the GDPR. Fred (P. 72) also consider it easy when it comes to the technical aspect, and that the problem rather is a communicational.

4.11 Privacy by Design and Default

All interviewees agree that Privacy by Design is desirable and something to strive for (Bob, P. 96, 98; Alex, P. 86; Douglas, P. 62; Charlie, P. 40; Fred, P. 56). This is however not seen as something feasible at all times, especially with the tight time scope that the GDPR gives (Bob P. 102; 107, Charlie, P. 40). Legacy processes in the different organisation have not, or only partly been developed to satisfy Privacy by Design (Bob, P. 96, 98; Alex, P. 92; Charlie, P. 42). Some industries already have highly regulated processes for handling data, like banking, where data flows is required to be done in specific ways and only certain data can be published (Douglas, P. 76; Bob, P. 100). According to Douglas (P. 76) and Bob (P. 100) this makes the processes compliant as they are. Moreover, banks are forced by other legislation to ask for and store certain information which overrides the GDPR (Douglas, P. 28).

Alex (P. 86) argues that the changes that have to be done to existing data processes are fairly standard in character and not too complicated. But, he also points out that there is a lot of processes that they need to go over in order of ensure that the right amount of data is handled at

the right place. Bob (P. 102) argues that most processes will need more than a refinement. Even if it is not a question of rebuilding from scratch, considerable refactoring will be needed (Bob, P. 102). Charlie (P. 40) and Fred (P. 56) points to the fact that there is not enough time or money to rebuild systems completely, it would not be possible to redesign everything according to Privacy by Design. Charlie (P. 42) says that most systems were built after the principle of what was needed. If it was possible to collect more data about someone it was done as a safeguard for the future, since it could become useful someday. With this design principle Charlie (P. 42) argue that too much data was gathered.

Instead of completely redesign systems, the interviewees see Privacy by Design as an important aspect to consider for all future software development. (Bob, P. 98; Alex, P. 86, 92; Charlie, P. 40; Fred, P.56). It is impossible to implement privacy by design in all legacy applications within an organization, especially if you have thousands of them (Fred, P. 56). Instead the focus should be to design for the future with the security and integrity of personal data in mind, it is something that cannot be ignored (Bob P. 98; Alex, P. 86, 92; Charlie, P. 40).

"When it's (the software) finished in January, you should not have to rebuild it in May, so you have to consider GDPR from scratch. System development is a rather long process, it takes months even for a small system to become operational." - (Charlie, p. 40)

Douglas (P. 20), Fred, (P. 82) and Charlie (P. 84) all discuss the importance of integrating the compliance of the GDPR into their processes, so that it becomes a part of the organisational habit. It is easy to make employees follow guidelines the first year but the problem is to keep it that way (Charlie, P. 40). A start is by training personnel in the GDPR with the help of e.g. workshops (Alex, P. 92; Douglas, P. 94). The next step is to make it a natural part of your workday, make the employees think about the GDPR before they make a decision on personal data (Charlie, P. 86). It is important to find ownership within the organisation for all processes, then anchor these processes deep into the organisation, so that the organisation can keep the processes recurrent (Fred, P. 82).

5 Discussion

In the discussion we will evaluate how organisations adjust to the GDPR in contrast to our theory concerning compliance in information systems. Firstly we will discuss how GDPR compliance is affected by the aspects covered in the literature, and then we will discuss findings we have not seen mentioned earlier.

5.1 Interpretation of Regulations

All of the interviewees describe some difficulties when interpreting the GDPR and translating it into implementable requirements (Fred, P. 16, 18, 40; Douglas, P. 34, 44, 46, 88, 90; Alex, P. 28, 42; Charlie, P. 38; Bob, P. 52; Eric, P. 54, 69). This goes in line with what Lohmann (2012) argues for; the challenge of making a correct implementation of abstract requirements. However, overall the GDPR is viewed as quite clear, with exception for some details (Alex, P. 28, 30; Fred, P. 40). This could be if certain data should be considered personal or not (Alex, P. 28), but these kinds interpretations issue seems to be an unusual. Eric (P. 68) see some measures as easy to fix technically, but the organisation need to interpret the GDPR to finish the solution. But, this is not necessarily seen as difficult. Overall, the respondents expressed little concern for interpreting the GDPR in a correct manner. As Lohmann (2012) argues, the interpretation is an important step as it is the first, and the interviewees seem to be aware of this. Still, it is not perceived as very problematic, and certainly not considered the biggest concern. But without legal consulting it would probably been a different story.

Douglas (P. 88) see the need for legal counselling concerning *consent* and how to formulate requests, which aligns with Turetken et al. (2011). Turetken et al. (2011) and Eggert et al. (2011) points at legal experts as one way of securing compliance, which most respondents see as a good approach to the *Data Protection Officer*. The interviewees want someone with a background of IT and law as their DPO, to anchor responsibility with someone who understands their data processes and can interpret the law correctly (Eric, P. 54; Alex, P. 42; Douglas, P. 44, 46; Bob, P. 56). Responsibility for information system processes could become tightly connected with legal tasks in most organisations. But, Fred (P. 40) argues that it comes down to understanding your data processes, and not interpreting the law. With clear understanding of how data move within the organisation, compliance is not too difficult to achieve.

5.2 Ad-hoc and Generic solutions

As argued in the literature review by Turetken et al. (2011), organisations usually achieve compliance, but it is generally done with ad-hoc solutions, specific measures for one purpose, when it should be solved with generic solutions. Alex (P. 94) felt as if they had to patch together their systems to be able to comply with *storage limitations and data minimisation*. This is a typical ad-hoc solution. By preparing for it with a generic solution, the implementation could have gone much easier. Alex (P. 96) went as far as claiming that this was probably the

way that all organisations would manage it. Charlie (P. 40) and Fred (P. 56) are pointing out that it is not possible to redesign all legacy systems to make it follow *privacy by design and default*, but that the focus in the future should be to follow this concept. This is a similar situation, systems and applications have been built without generic compliance solutions in mind. Organisations should be ready for changes in agreements and laws as these are not static (Abdullah et al., 2010). The organisations that already are working in areas where privacy and security is of great significance (e.g. banks) have systems with measures similar to *privacy by design and by default*, than the rest of the organisations (Douglas, P. 76; Bob, P. 100). Lohmann (2012) argues that organisations should look at information systems as a whole and not go too much into specific processes to be able to comply. Bob (P. 28) and Fred (P. 40) argue for, which is in line with what Lohmann proposes, are understanding the flow of the processes and streamlining them. By streamlining the process, only the necessary data will flow through the systems. While generic solutions is desirable, it is just not feasible at all times. The short time scope force the organisation to implement ad-hoc solutions even if they rather would, provided the time and the money existed, create what Sadiq et al. (2007) calls preventative solutions.

5.3 Resource Allocation

The high amount of *penalties* (Gilbert, 2016; Lynskey, 2015) seems to be the reason that the GDPR has gained the interest from the managerial levels (Bob, P. 64; Alex, P. 60; Douglas, P. 44; Charlie, P. 72; Fred, P. 60). This in its turn lead to more resources available for compliance as the organisations now compare fines with costs (Alex, P. 60; Charlie, P. 72), which gives an incitement to fund the process changes (Charlie, P. 72). This is in line with Eggert et al. (2013) argues, that better compliance will be achieved with involvement from the managerial level, which has become the case. As discussed in our literature review, organisations perceive compliance as a cumbersome task rather than a possibility to improve their processes (Sadiq et al., 2007). However, this is also changing (Abdullah et al., 2010; Sadiq et al., 2007) organisations now want to gain advantages by complying (Abdullah et al., 2010), something that is supported by three of the interviewees (Bob, P. 64; Fred, P. 60; Charlie, P. 74). Both Fred (P. 60) and Bob (P. 64) see business possibilities by complying with the GDPR as they will add both transparency and protection of personal data and Charlie (P. 74) explains that the extra resources gained from compliance will serve them well as GDPR compliance are improvements they have wanted to make, something that almost all interviewees agree on (Charlie, P. 52; Alex, P. 60; Douglas, P. 60; Bob, P. 64; Eric, P. 44). As the organisations see an added gain by complying with the GDPR the risks of minimum compliance should be limited, a problem discussed by Abdullah et al. (2010).

The authors (Abdullah et al., 2010) idea that altering processes could lead to risks and complexity is actually seen as the opposite by our interviewees as they now get the opportunity to improve and structure their processes, developing both *transparency and documentation* (Bob, P. 58; Alex, P. 48; Douglas, P. 56; Charlie, P. 56; Fred, P. 36). For instance Charlie (P. 44) explains that they will hire a person, full-time, that will work with locating, mapping and classifying the organisations personal data so that they can oblige to *the right of access, the right to be forgotten and the right to data portability.* Almost all of the interviewees have either assigned or are in the process of assigning a *Data Privacy Officer* (Bob, P. 50; Alex, P. 38; Douglas. P. 44; Charlie, P. 46) a step to hindrance poorly made information system processes, one of the problems mentioned by Abdullah et al. (2010) and Sadiq et al. (2007). As

the work of the DPO is to investigate and question how organisations handle their personal data (Gilbert, 2016).

5.4 Organisational Compliance

According to Bulgurcu et al. (2010) it is important to have policies that guide the employees of the organisation in management of their data, as they are the weakest link when it comes to data handling. This should be done with the help of training and that the tasks of the employees are streamlined for a correct data handling (Bulgurcu et al., 2010). Both Douglas (P. 66) and Charlie (P. 88) believe that education and workshops are how their organisations are going to create an organisational compliance. They both see mapping of personal data as a big problem, for *transparency and documentation*, due to the fact that a lot of personal data are stored in excel sheets on old computers (Douglas, P. 60, Charlie, P. 38) and that educating the staff will create awareness and clear guidelines for the usage of personal data. This is a good start for creating organisational compliance, the employees will become aware of why data is handled in a certain way, which will be supported by guidelines helping organisational compliance become anchored in the organisation. Anchoring compliance into organisations are something we have not found in the literature but has been mentioned by many of our interviewees (Douglas, P. 20; Fred, P. 82; Charlie, P. 84). We will from here on refer to this challenge as *continuous compliance*.

To create continuous compliance in organisations, Charlie (P. 52) gives some examples. The organisations could open up one-stop-shops, a place you can go and receive all information about if what you are doing are legal. The other example is that organisations could create process steps that you cannot pass without considering GDPR (Charlie, P. 52). This would create a more lasting compliance, a continuous compliance, as it would be part of the organisation although employees would come and go. Organisational guidelines is a step along the way, but as Julisch et al. (2011) mentions, this is not a guarantee for compliance. Bob (P. 94), Fred (P. 82, 84) and Charlie (P. 38, 44) see clear ownership as a measure to keep data processes compliant. Anchoring the right structure for responsibility could be a way to make sure that data processes become and stay correct.

In essence, systems can have correctly working data processes and employees could still be able to fail the process (Abdullah et al., 2010). Data processes begins and ends with humans. Therefore, the human factor is of importance, because an organisation can have lawful data processes but if the employees do not understand the way to manage, the information system will not be compliant. Moreover, compliance is a continuous process that will have to go on.

5.5 Documentation and Monitoring

Transparency and Documentation is argued to be a cornerstone of the GDPR by the interviewees, which see both a need to demonstrate compliance to authorities and understand their own data processes (Bob, P. 58; Alex, P. 48; Douglas, P. 56; Charlie, P. 56; Fred, P. 36). This aligns well with what Abdullah et al. (2010) and Turetken et al. (2011) argues for, which is documentation both as mean to prove lawfulness and chart data processes. Monitoring *data breaches* is also mentioned in both literature and by interviewees as seen an important aspect (Abdullah et al., 2010; Turetken et al., 2011; Bob, P. 84, Alex, P. 74, Douglas, P. 80; Eric, P.

64). Alex describes comprehensive work surrounding logging to be able to follow up on data breaches, which is a match with the view of Abdullah et al. (2010).

Fred (P. 40, 72) view monitoring of the information system as a crucial part, if the organisation is aiming to become compliant in any aspect. He argues that this is not technically complex, the communication part is often more problematic. Therefore, these documents should be distributed to all stakeholders (Fred P. 52). Douglas (P. 36), Alex (P. 58, 110) and Charlie (P. 48) agrees with this and both see a need for more formal documentation between data controllers and processors. Alex (P. 110) argue that contract need to clearly states responsibility for data. With higher stakes as mentioned by Abdullah et al. (2010), there might be an increase in formal documents demonstrating compliance to stakeholders.

5.6 Legacy systems

Legacy systems is described by literature as complicated and demanding to make compliant (Sadiq et al., 2007; Julisch et al., 2011). This is expressed by the interviewees as well (Bob, P. 34, 40, 42; Alex, P. 28; Charlie, P. 38; Douglas, P. 34, 90; Fred, P. 56). Understanding what the technological landscape looks like and mapping data to make it accessible as required is the primary concerns, but the interviewees see several problems with compliance and legacy systems (Bob, P. 36, P. 42, P. 44; Alex, P. 28; Charlie, P. 38; Douglas, P. 34, 90; Fred, P. 56). Just like Julisch et al. (2011), Charlie (P. 40) and Fred (P. 58) see it as economically unfeasible to redesign all information systems to be designed to be compliant. However, even if legacy systems is seen as a big obstacle to reach compliance, it is not considered futile to take measures to adjust current systems (Bob, P. 36, P. 42, P. 44; Alex, P. 28; Charlie, P. 38; Douglas, P. 34, 90). Therefore, the difficulty is rather making a legacy system to be designed to comply than to make it lawful. Charlie (P. 42) argue that most systems were built when it was considered a good thing to collect more data than needed, which is the opposite of the aspects of the GDPR that deal with *data minimisation and storage limitation.* Even if the legacy systems were designed for a different cause, it seems as if the interviewees are willing to modify these systems into compliance.

Sadiq et al. (2007) see a difficulty in addressing distributed systems, which is confirmed by the interviewees. Bob (P. 36, 42, 44), Alex (P. 28), Charlie (P. 38), Douglas, (P. 34, 90) and Fred (P. 76) see the flow of data through different systems as a challenge. They see a need to understand and document their process flows in detail (Alex, P. 48; Douglas, P. 14; Douglas, P. 56; Charlie, P. 56; Charlie, P. 88). Moreover, the implementation of compliance measures in data processes is not easy. To recognize all aspects of the GDPR, like *Breaches of Data, The right of access, the Right to be Forgotten and the Right to Data Portability, Storage Limitations and Data Minimisation* and so forth, the organisations will just like Sadiq et al. (2007) argue have cumbersome work. But, it is still considered a better option than redesigning from scratch. While over time, the information systems will be modified or replaced until it becomes what Sadiq et al. (2007) calls preventative. Alex (P. 66) says that their information systems will be more compliant with time as more measures are implemented. Some of the interviewee's legacy systems even have data processes that follow strict regulations as it is (Douglas, P. 76; Bob, P. 100), and therefore makes compliance easier to achieve. In short, both the literature and the interviewees see legacy systems as major impediments to compliance.

5.7 Competing Compliance Measures

Competing compliance measures is something that the current literature considered too little extent (Abdullah et al. 2010). Abdullah et al. (2010) argue that regulations tend to change which requires a holistic approach to compliance. However, many of the interviewees mentions other laws, contracts or safety measures to impact the compliance in their information systems (Douglas, P. 18, 34, 90; Eric, P. 12; Alex, P. 24, 26; Charlie, P. 38; Bob, P. 44, 100). Foremost, other laws and framework for managing data help the organisations comply with the GDPR. Douglas (P. 76, 80, 82), Bob (P. 100) and Eric (P. 12) points at already strict rules for some data processes that will allow compliance for the organisation through minor adjustments. An already compliant system could therefore be an advantage when new regulations becomes a reality.

Former safety measures such as storing data redundantly (Alex, P. 24, 28) or other laws (Charlie, P. 38; Douglas, P.34, 90; Fred, P. 16, 18), is also to be considered when designing to become compliant. There is a need for a holistic view of the context when adjusting an information system. This is further confirmed by Alex (P. 40) that point at the risks with interdependencies and changes to systems. If specific segments of a process is removed as a measure to become compliant, there is a risk that other systems fail to deliver because of this. To highlight the interconnections documentation and charting of the organisations information system is important.

6 Conclusion

> *What challenges, concerning data processing, do organisations face when striving for compliance with the General Data Protection Regulation?*

In this study we have found seven challenges and one sub-challenge concerning data processes that organisations face as they adjust to the GDPR. These are; *Interpretation of Regulations, Ad-hoc and Generic Solutions, Resource Allocation, Organisational Compliance* and *Continuous Compliance, Documentation and Monitoring, Legacy Systems* and *Competing Compliance Measures*.

Interpretation of Regulation is considered problematic in both literature and by the interviewees, but not as a major challenge. Overall the GDPR is considered straightforward, still the organisations seek counselling in legal matters. We found support for *Ad-hoc and Generic Solutions* as a challenge. Generic solutions is desirable, but not always feasible, especially with the tight time scope given by the GDPR. Therefore, ad-hoc solutions is a reality. *Resource Allocation* have been a problem according to the interviewees, but the high penalties have increased budgets and resources set aside for compliance. Moreover, the added business value of compliance is perceived as a way to secure resources for the future. *Resource Allocation* is still considered a key to compliance, but something that have been less problematic with the GDPR, as it has gotten attention from managerial levels. Data processes is to a large extent automated and most compliance measures is aimed at adjusting information systems, *Organisational Compliance* is still a challenge. Education of employees and guidelines are some measures to control this. We also encountered what we refer to as *Continuous Compliance*, as a part of organisational compliance, a challenge not found in the available literature. Anchoring responsibility with clear ownership and adding mandatory steps to certain processes is two of the countermeasures that point to this as a difficulty. *Documentation and Monitoring* is considered vital to compliance with the GDPR. Both in the sense of understanding and showing compliance, but also for monitoring data breaches. Even more with the GDPR, the higher stakes in form of penalties, more comprehensive contracts between data controllers and processors are perceived to be needed. *Legacy Systems* is regarded as a big challenge. Understanding the technological landscape of the organisation, learn where data resides and make the data processes compliant is both complex and time consuming. Still, it is often viewed as worth patching legacy systems rather than building a new system with compliance in mind as a design feature. *Competing Compliance Measures* is also a challenge for organisations. Former security measures, other regulatory documents and interdependencies between systems are difficulties for organisations to consider when adjusting to the GDPR. Conforming all systems to the GDPR could lead to violation of other laws or incomplete data processes.

Below is a table of our summarised findings.

Table 7: Findings

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.

6.1 Limitations and further research

The challenges connected to data processes for compliance was not described in deep detail in previous literature. We found these compliance challenges and two further aspects relevant for the adjustment to the GDPR, but this study did not have the scope to explain these in detail or prescribe countermeasures. Therefore, further research into the specific challenges is in need.

Our research and findings are also limited in the sense that we examined the challenges of GDPR adjustments according to organisations from very different sectors. As discussed, some challenges seems to be more prevalent in specific domains. Regulatory compliance in information systems could therefore differ in character from domain to domain. Further research in specific sectors could bring more knowledge which is more applicable to practitioners.

Appendix 1

1. General

1.1 What position do you have in the organization?

1.2 How long have you been at that position?

1.3 What does a regular day for you look like?

2. Consent

2.1 Will the changes with purpose specific consent and informed consent affect your work?

2.2 Will you change how you obtain valid consent?

2.3 Will it be harder to see to that the consent is informed?

2.4 Will the purpose specific processing in anyway limit the way you handle data?

2.5 Will you look over your processes in order to comply with data minimisation?

3. The Right of Access / The Right to be Forgotten / The Right to Portability

3.1 Will any of the above stated rights change how you handle data?

3.2 How will you grant access to data?

3.3 How will you satisfy the right to be forgotten?

3.4 How will you allow data subjects the right to portability?

3.5 As the user now are allowed to access and delete information about themselves it also puts some pressure on organizations to know exactly where all personal information is stored at all times. How will this change affect your processes?

4. Territorial Scope

4.1 What will be the effects of the territorial scope be for you as an organization within EU?

4.2 Will you or the processor have to employ a contact person within the EU?

5. Mandatory Data Privacy Officer

5.1 Will you have to appoint a data protection officer?
5.1.1 Required by law?

5.2 Within the organisation or external?

5.3 Difficulties?

6. Transparency and Documentation

6.1 Will you document all of your data processes?

6.2 How will this be done?

7. Penalties

7.1 How important is the severity of the penalties for you when making the decision to change the processes?

8. Pseudonymous data

8.1 Will you use pseudonymisation of data to protect personal data?

8.2 How will you pseudonymise the data?

8.3 How will pseudonymisation of data affect you data processes?

9. Encryption of data

9.1 Will you use encryption of data to protect personal data?

9.2 How will you encrypt the data?

9.3 Will the encryption of data affect you data processes?

10 Breaches of data

10.1 How will you deal with the requirement to notify authorities or data subjects?

10.2 Will you increase the security measures to stop breaches because of the GDPR?

11. Privacy by Design / Data Protection by Default

11.1 Have you adjusted your data processes to privacy by design/default and protection by design/default?

12. Overall

12.1 What is according to you the most important/difficult aspect of the GDPR?

Appendix 2: Alex

Paragraph	Person Speaking	Text	Coding Reference
1	Interviewer	Vad är din roll i organisationen?	
2	Interviewee	Jag är ansvarig för informations säkerhet så det är it säkerhet och informationssäkerhet och sen rapportera till CIO som i sin tur rapporterar till CEOn	
3	Interviewer	Hur länge har du haft den rollen?	
4	Interviewee	Suttit sen september i den rollen 6 månader	
5	Interviewer	Beskriv en vanlig dag?	
6	Interviewee	En vanlig dag är att man tar reda på var man satt in i kalendern man tar en koll i maillådan och ser vad som är uppsatt där. nu är det ju mycket som är upp-styrt mot GDPR och en ISO2700 certifiering som vi tittar på så dom två samtidigt . så det är rätt mycket planerade grejer framåt i kalendern. Sen är det de dagliga med kundrelationer och så många kunder har ju frågor kring GDPR nya avtal så mycket avtalsfrå-gor på senaste tiden.	
7	Interviewer	Ni hanterar andra kunders data?	
8	Interviewee	Ja vi processer så typ en underleverantör. ja mest processor men vi hanterar ju vår egna uppgif-ter så där finns ju dom delarna där vi är controller också men i förhållande till kundrelation, till våra kunder så är vi processor.	
9	Interviewer	Om vi går in på specifika delar av GDPR när det kommer till samtyckes biten. Kommer det här med ändamåls samtycke (purpose consent) och informerat samtycker (informed consent) kommer det påverka hur ni arbetar?	
10	Interviewee	Säkerligen. Som det varit nu har det vi haft lite fria händer, från insidan, att forma våra tjänster gente-mot våra kunder, nu måste vi vara mycket mer spe-cifika i med att kunderna är de som har samtycket med medborgaren, som egentligen har rättigheterna så det gäller att vi har satt att det är de så här vi	Consent

		kommer processa uppgifterna och det är det här du kan vänta dig att vi kommer leverera och att vi kanske mer streamliner våra tjänster. Lite bättre än vi gjorde innan så att data inte flödar in i någon annan tjänst.Utan den här tjänsten levererar detta och det är det här samtycket som gäller. Så jag tror det är mycket kommunikation med kunderna att få rätt på samtycket redan från början för de vet kanske inte hur vi processar data i dagsläget. Där ser jag att vi har mycket arbete med våra kunder att göra.	
11	Interviewer	ÄR det svårt att få den här biten med hur man minimerar datan som man processer, är det svårt att få datorn på rätt ställe?	
12	Interviewee	Ja hitintills har det varit så att man tar in all data som man kan, det kan vara bra att ha, men nu är det ju så att vad försöker vi leverera här? jo det är de här delarna , vad är det för data vi behöver för att leverera? Jo det är den, den och den delen. Det är det enda vi behöver. Ja då är det enda vi ska ta in från er sänd oss inte mer data. För vi ska bara ha det här och det måste de uttrycka i samtycket också. Det är dom här delarna vi tar och processer den sen levererar vi tillbaka till er.	Storage Limitation and Data Minimisation
13	Interviewer	Då är ni väl mest processor, men sånt här giltigt medgivande att det krävs lite mer från den som godkänner det, lite mer aktivt och informerat, har ni märkt någon skillnad där? Kommer det påverka er?	
14	Interviewee	Nä där tror jag inte det påverkar oss alldeles för mycket men sen så är det ju för oss själva där vi är controller där är det ju mycket som är anställda och då har vi anställningsavtal och hela den biten så där har vi inte så jättemycket direkt. Det är mer kundernas data som iv har i CRM system, så att vi har våra kunders persondata och där behöver vi kanske göra lite kontroller. För att ha rätt nivå där också.	
15	Interviewer	Upplever du det som svårt att hålla sig tillrätta med den här minimeringen av data och att man strömlinjeformar i de här processeran?	
16	Interviewee	Det är inte svårt men det är en övning i kommunikation det är de ju det gäller att ha rätt personer och att de förstår detta. Detta måste ni göra och detta måste vi göra och det är vägen framåt. SÅ det är mer att det tar tid att göra än att det är mer komplext. SÅ att säga.	Storage Limitation and Data Minimisation
17	Interviewer	Sen har vi lite rättigheter som kommer med GDPR, de har egentligen funnits lite sn tidigare men som blivit lite mer fokus på nu, rätten till tillgång, rätten att bli bortglömd och dataportabilitet, alltså att man	

		får hämta ut sin data och flytta den. Jag gissar att det påverkar er?	
18	Interviewee	Det kommer det göra speciellt det med att ta bort data, som vi inte har gjort, man har kunnat göra det men då har man tagit bort all data, då har man inte gått in på det granulära, på just den här kunden, ta bort det hära. Men där har vi uppgraderat våra backup strategier där vi har ett mycket bättre verktyg att kunna göra detta, kunna titta på enstaka tabeller i databaser istället för att se en hel databas. Sen är frågan hur våra system hanterar allt detta, om det går att ta bort en del av detta utan att något annat går sönder. SÅ det är mycket sådär tekniska kontroller att vi måste verifiera att det går att göra eller om vi måste göra det på något annat sätt. För att säkerställa funktionaliteten.	The Right to be Forgotten, the Right to Access and the Right to Data Portability
19	Interviewer	Så man får gå in på en mer specifik nivå?	
20	Interviewee	Ja och sen är det ju i dom lägena vi kan trycka det till våra kunder och säga det att ni har access in i systemet så ni kan ju ta bort dom själv. och vill dom göra det själv som går i vissa system och i andra får vi göra det åt dom.	The Right to be Forgotten, the Right to Access and the Right to Data Portability
21	Interviewer	När det kommer till såhär det går igenom alla dom här, innan har man använt sig av en bred pensel, tagit bort allting?	
22	Interviewee	Ja men det har ju varit så nu har vi detta kontraktet med er då förvarar vi datan till kontraktet är slut, sedan så antingen skickar vi datan till er eller så tar vi bort den	
23	Interviewer	Ni har också någon process för att hämta ut datan i en användbart format?	
24	Interviewee	Ja till viss del och i de andra delarna har det varit att man varit slö. Oftast när man processar data går de igenom många steg och det är många temporära lagringsplatser för datan. Så man är säker att man levererar allting i alla delarna, tex där gick fel då skickar vi om den datan. Och där kommer vi vara hårdare på det sättet att vi tar bort datan. Har vi flyttat den därifrån dit. Tar vi bort datan och blir det något fel senare får vi skicka om det från kunden. Så att vi startar om processen istället. Så att vi inte håller datan i de temporära delarna så länge som vi gjort av ren ja det har fungerat och säkert.	The Right to be Forgotten, the Right to Access and the Right to Data Portability Storage Limitation and Data Minimisation
25	Interviewer	Det blir mer specifikt var data finns och inte finns?	
26	Interviewee	Ja och då har vi gått från den delen till den delen och då finns inte datan längre i detta steget.	

27	Interviewer	Hur funkar det för er om en person en kund som vill se vad ni har för data hur kommer det gå till?	
28	Interviewee	Det kommer inte vara enkelt. Inte i alla system. Visa system är enkla vi har ju system som t.ex. där vi har posten för ett helt företag. Vi scannar in all post och då i den inscanningen tar vi visa fält och OCR och skickar in i en databas så den texten kan söka på. Och kan man söka på de personerna där då hittar du ju alla dokumenten som är relaterade men skulle det vara något i brödtexten då blir det problem. För det har vi inte inventerat är det fortfarande så att vi måste bevisa att vi har de här dokumenten angående dig? Egentligen om man läser i lagen så är det ju det, så där kanske vi måste göra mer. Eller snacka med juridiken hur kan vi göra detta?	The Right to be Forgotten, the Right to Access and the Right to Data Portability Storage Limitation and Data Minimisation
29	Interviewer	Men är det svårt att med definitionerna? Vad är persondata vad är inte persondata? Var gränserna går och sådär.	
30	Interviewee	Nä inte reellt. Det är rätt så solklart. men snackar vi t.ex. övervakningskameror ja det är ju persondata när man ser personer. Säger den personen att den ska ha all data vi har ju kundtjänst eller externa som behöver gå in, blir det övervakat? Behöver vi ha det övervakat? Det kanske blir att vi tar bort de kamerorna som är där allt är en balansgång över vad som är enkelt att göra. Skulle du vilja bli glömd på ett band ska vi då radera en person i banden? Jag har hört många titta på det, specifikt banker och sånt där de filmar allt som försiggår i lokalen där man har externa. Att man får ha kameror som går in och blurrar då visa ansikten. så att man inte behöver ta bort hela filmsnutten. För det vill man inte göra, eftersom man vill veta vad som hände där av en annan anledning.	
31	Interviewer	Men det blir egentligen att man får ha mer strikt kontroll på varje process. det bottnar i det?	
32	Interviewee	Ja man får skruva ner och se liksom vad är det vi har här och varför har vi det. Finns det fortfarande ett reellt behov av att ha det och sen jämföra det med kostnaden med att hantera det, kunna ta bort det och kunna leverera det till den personen som skulle vilja ha det i sådana fall.	
33	Interviewer	har ni några territoriella, reglerna påverkar utanför EU har ni några processor som skickar utanför EU?	
34	Interviewee	Det blir ju Norge men det har ju samma regelverk det är ju ESS land. Så ännålänge har vi inga externa men det tittas ju på cloudtjänster och då gäller det ju att titta på var ligger datan där? Är det fortfarande EU-land speciellt nu när England går ur, Irland är ju vanligt att man har cloudtjänster i. Kan vi säkra att de är flyttade till ett EU—land istället och så här men än så länge har vi inte det behovet så än så länge klarar vi oss men det är ju något som man måste ha i	Territorial Scope

		bakhuvudet.	
35	Interviewer	Ja precis för cloudtjänster blir ju ganska överlag, iden med cloudtjänster att det ska vara utspritt och tillgängligt överallt.	
36	Interviewee	Ja det är lite idén	Territorial Scope
37	Interviewer	så det är ganska hårda krav på det, och då kommer vi till DPO, kommer ni utse en sådan?	
38	Interviewee	Ja vi kommer att utse en sådan och det kommer bli jag. Vi har en på gruppnivå så på snurr gruppen är det SISON för hela snurr gruppen och vi, eftersom vi hanterar så mycket persondata så anser vi att vi behöver en också.	Data Privacy Officer
39	Interviewer	Är det pga vad lagen säger eller vad ni tycker själva?	
40	Interviewee	Pga lagen skulle jag säga. sen är ju frågan om vi ska ha någon ute i länderna som ska hjälpa dom mer näraliggande. Men där kommer vi nog inte ha någon som kommer vara DPO som den lagen säger utan vi kommer kanske ha en privacy advisor. SÅ kommer kanske inte ha rollen men som hjälper till med de frågeställningarna.	The Right to be Forgotten, the Right to Access and the Right to Data Portability Data Privacy Officer
41	Interviewer	Ja juste men kommer det här va specifikt det du gör eller kommer det vara en av dina roller?	
42	Interviewee	Det kommer vara en roll av flera. Vilket är lite si och så om man kollar på det i lagtexten för som jag ser på det så är det egentligen en juridisk person någon som kan lagen som ska vara DPOn inte någon som sitter i mer operationell IT position. Mer än jurist som ska ha den rollen. Men sen ska man kunna om våra tjänster och hela den här biten. Så det är väldigt svårt att hitta rätt person för att ha DPO hatten egentligen.	Territorial Scope Data Privacy Officer
43	Interviewer	Övervägde ni att ha någon extern?	
44	Interviewee	Jo vi tittade på det. och det kanske ändras också vi ser ju att i med att det är vi, alltså CISON som har haft bäst koll på var vi har datorn vara controller etc. att implementera själva GDPR att vi har oss i position som DPO i den rollen fram tills att vi har, GDPR kommer ge slagkraft i maj och att vi tar ett nytt beslut då att vi tar en extern eller att vi har en hel gruppering som är DPO som sitter i legal på ******. Men jag tror det kan ändras längs med vägen. I själva projektet nu ser vi det som att vi får mest momentum ifall vi har rollen.	Data Privacy Officer

45	Interviewer	när de mer tekniska aspekterna ska implementeras och så?	
46	Interviewee	Ja precis. Sen kan man flytta det.	Territorial Scope
47	Interviewer	Sen kommer det till det här med dokumentation att allt ska vara dokumenterat och kunna hämta ut specifika processer och sådär. Behöver ni ändra något där?	
48	Interviewee	Det vi mest har tittat på är själva loggkraven. Vi måste veta vem som har accessat vad och så så det är många fler system som vi har högre loggkrav planerat inför GDPR så där har vi fått utöka den miljön för att hantera alla dessa loggar. Sen så är det ju att hantera processer. för att få ut all data, ja jag vill ha ut all data men hur ska de här processerna se ut, var ska jag skicka in det, vad händer sen? Vem letar fram datan och vem levererar den. Sen är det ju att kunna dokumentera alla sina flöden i detalj. Och då tittar vi på var ligger datan och hur länge ligger den där? Behöver vi ha den här i tre månader temporärt? Nä det behöver vi inte vi behöver bara ha den tills vi levererat på dit. Okey det gör vi om det och beskriver hela den här processen så att vi vet var datan finns i alla lägen. Och vi vet när vi behöver ta bort den och här ligger den i tre månader och där ligger den i 10 år då vet vi vad vi har att göra. så det är mycket den dokumentationen vi jobbar på nu?	Transparency and Documentation
49	Interviewer	Är det högre krav på controllern? att vi måste ju veta var vi ska få den här och så?	
50	Interviewee	Ja det är mycket transparens dom är ute efter. Kunna se vad är det som händer här? Kan vi få någon insikt hur datan ligger där. Där är rätt mycket som dom vill ha. men också att sätta upp mycket mer regelbundna möten och så här att man går igenom såna frågeställningar att dom kommer närmare oss som partner.	
51	Interviewer	Kommer det krävas närmare samarbeten mellan controller och processor.?	
52	Interviewee	Ja iaf i början så att det ska känna sig trygga med det.	
53	Interviewer	Det är mycket som ska hanteras, mycket data.	
54	Interviewee	Japp det ser ju att risken ökar.	
55	Interviewer	Finns det någon skärningen där i vad ni vill och va de vill?	
56	Interviewee	Det är självklart att vi vill fokusera på att leverera och att leverera efter GDPR vi vill ju inte ha all	Transparency and Documentation

		overhead som relaterar kunder, att de ska gå in och göra review på vår miljö hela tiden, har vi hundra kunder och alla ska göra review på våran miljö ohh det kommer ta tid. SÅ hur gör vi för att de inte ska göra det? Vi måste vara transparenta, ge dom mycket information, inblick och möjligheter att kolla på våra system kanske ge dom loggsystem som kan visa dom hur mycket data dom skickat och var det ligger som dom får trygghet och inte behöver gå nästa steg och köra revision på oss för det tar väldigt mycket tid.	
57	Interviewer	kontrakt och så här ser de annorlunda ut?	
58	Interviewee	Japp alla kontrakt börjar skruva på det, det har ju tidigare varit lätta PUL kontrakt på 4-5 sidor nu är det 15 sidor där man går in i detalj kollar på den här delen i GDPR hur kommer ni göra där och hur kommer ni göra där? Problemet att vi gör olika i olika system. I ett system gör vi på ett sätt och i ett annat system gör vi lite annorlunda. Så det är det som är svårast. Att få en helhet i det. NU är det lite fragmenterat så det är mycket data vi behöver skicka över det är inte bara ett dokument. SÅ där håller vi på att sätta upp ett statement per tjänst. Så här kommer vi leverera GDPR i den här tjänsten och så här gör vi i denna tjänsten så här kommer ni att skicka processen med att få ut data och såhär så de får mer inblick i hur vi levererar de här tjänsterna.	
59	Interviewer	ÄR det främst straffen som har drivit denna ändringen?	
60	Interviewee	Jag tror att det är det som gjort att det kommit upp på ledningsnivå. och att det är så mycket snacka kring det alla börjar dra till sig öronen hur gör vi här? Vi har ju leverantörer och hur gör dom. Dom har vår data hur säkerställer vi detta och jag tror det är pga straffen som kommit igång för hade det inte funnits hade det ju varit samma som PUL för mycket av det här har vi ju redan idag det är inte jättestora skillnader egentligen. Och att man inte hur enkelt som helst kan skicka data ut ur europa man måste ha mer kontroll.	
61	Interviewer	Hur är det med att lagra datan om man pseudonymiserar och krypterar data? Pseudonymiserar ni data?	
62	Interviewee	Inte mycket än det är ju mer i testsystem där vi inte har persondata. Och om vi skulle flytta data in dit måste vi ju maskera data. Vi har ju visa system där vi kör med kundnummer men det är ju inte rätt heller för du kan ju härleda ett kundnummer till en kund så där kör vi mest kryptering. Och sen i testsystem har vi inte personnummer.	Pseudonymous Data

63	Interviewer	Blir det problematiskt eftersom det blir ett till led i processen?	
64	Interviewee	Ja vi måste göra om rätt mycket, så det kanske kommer i alla nya system. Att vi gör det men i de gamla kan vi inte. Det går inte att implementera i efterhand.	
65	Interviewer	Och kryptering gör ni det på all data?	
66	Interviewee	Inte i dagsläget men det kommer bli mycket mer, bara för att säkerställa att vi inte behöver lika mycket krav när det väl är krypterat. Sen ska man processa datan då behöver man läsa datan så måste du ha kontrollen över det.	Encrypted Data
67	Interviewer	Men är det samma sak där? Att det blir ytterligare ett steg i en process?	
68	Interviewee	Ja säkerställa det och när man gör förändringar är databasen krypterad? För det var den inte innan för det var mycket lättare att men nu går vi mot kryptering och nu ska det vara krypterat från början så det blir lite annat sätt att tänka när man designar men de är svårt att göra om allt från början när man har system som fungerar det får man ta när man gör en större förändring. Ny version ja då lägger vi på kryptering så det kommer gå steg för steg när man går mot kryptering.	
69	Interviewer	När de beskriv i GDPR är det saker man känner att man vet hur det funkar?	
70	Interviewee	Ja det är rätt så standard prylar egentligen men det är mer att göra alla införstådda med det och när man tittar på nya system att man har det i baktanken och frågar om det.	
71	Interviewer	Så det är mer en fråga om man är medveten om att det ska göras snarare än hur det ska göras?	
72	Interviewee	Ja	
73	Interviewer	Hur kommer ni hantera kravet att anmäla personuppgift incidenter?	
74	Interviewee	Ja där har vi både oss själva när vi måste rapportera till EU direkt, när vi tappar den, och samtidigt rapportera till våra kunder, men där har vi implementerat i vårt incident management system har vi en extra låda som säger att om en person är med i den här incidenten då checkas den i och då triggar vi hela data breach planen, då kollar vi vad är det för data som har blivit tappad ska vi då skicka till dom personerna specifikt dom medborgarna när ska vi skicka till kunden, så många olika steg som säger att antingen göra vi detta eller detta eller ska vi göra alla tre. Där är ju mycket som står i de nya avtalen med leve-	Breaches of Data

		rantören för de vill ha svar inom 24 timmar så det i sin tur kan gå 72 timmar till EU.	
75	Interviewer	Så man får helt enkelt ha en krisplan?	
76	Interviewee	Ja vi har ju en krisplan idag men då har vi inte tagit detta i beräkning så den kommer vi bygga ut till att också ta persondata frågan.	Breaches of Data
77	Interviewer	Det är väl ganska lätt att rapportera till myndigheter men när det kommer till personer kan det vara jobbigt att få kontakt då?	
78	Interviewee	Ja så det är frågan i dom olika systemen har vi direktkontakt till kunden eller måste vi gå genom vår kund för att ha dom uppgifterna vi kanske inte har dom uppgifterna på vår sida. I med att vi skickar väldigt mycket data så har vi ju oftast adresser och sånt så jag ser ju att jag ser att i de flesta fallen skulle vi lätt kunna göra det men då blir det en direkt fysisk.	
79	Interviewer	Det blir fler steg i processerna här också?	
80	Interviewee	Ja det blir fler steg i våra processor som vi har idag. Vi lägger till nya steg och nya kontroller	
81	Interviewer	Och då ökar ni säkerhetsåtgärderna?	
82	Interviewee	Ja och i med att vi ökar loggningen så kan vi se om data kommit på avvägar. Om någon har gjort en attack så vi kan se vad dom kommit åt och vi kan beskriva hur många persondata instanser har vi läckt ut. Så vi kan scopa den.	Breaches of Data
83	Interviewer	Hade ni inte loggar på allt innan?	
84	Interviewee	Vi hade på allt som berör personnummer hade vi alla dessa loggar, men bara det är en adress så måste vi ha det nu framöver och logga det också för det är persondata. Det behöver vi logga också. Så vi har utvidgat det och tidigare har vi bara haft det på känslig persondata.	
85	Interviewer	Har ni anpassat era dataprocesser för privacy by design?	
86	Interviewee	JA där är ju mycket med utvecklingsprocesserna där vi lägger till det. Vi ska inte ha persondata om vi inte behöver det t.ex. och vi ska ha kryptering by design istället för att försöka implementera det efterhand och hela alltet med va som kan ses när man loggar in behöver du se allting eller kanske du inte behöver du kanske bara ska se den här lilla datan allt anana ska vara maskerat så det är mycket sådana frågeställ-	Privacy by Design and Default

		ningar som vi har lyft upp i utvecklingsprocessen för att få det på plats. Mycket är ju standard det är saker som man behöver repetera och få på plats. men det är saker vi gjort förut.	
87	Interviewer	Så det är inte helt nytt och kommer som en chock?	
88	Interviewee	nä Privacy by default där kanske man göra lite andra beslut när man designar nånting istället för vi har data. Detta behöver dom inte se egentligen.	
89	Interviewer	Om man gjort det sen tidigare så är det inte ett så stort steg?	
90	Interviewee	Nä precis man vet var man brister så det är bara att ändra	
91	Interviewer	Om snackar om privacy by default hur relaterar ni till det?	
92	Interviewee	Ja det är i stort sett i alla projekt tittar i när man utvecklar något nytt att man tittar på vad man behöver förändra i den hära. Det kommer också lyftas upp när man gör sådana här DPIA assessments där man tittar på vad vi har för data här. Här har vi inte det per default och då kanske vi behöver förändra det. så det är också en process att få alla att tänka på det att vi ska försöka minimera det redan från början. Så det är mycket en träningssak att utbilda alla.	Privacy by Design and Default
93	Interviewer	Du nämnde innan det här med att ändra processen nu men att man ändrar det från början med nya system och processer. är det tanken att man lappar ihop dom nu inför gdpr och sen vill man byta ut dom helt och hållet nu framöver?	
94	Interviewee	Ja så ser man ju det. Det är också en process som man gör på sidan om att konsolidera alla systemen att få ett system istället för tre idag när man gör det gör man det till ett bättre system. Och lägger på alla dom här kontrollerna redan från början där man kan ha några legacysystem som va sådära fungerar inte riktigt bra. Dom har dom här bristerna redan från början när vi går och konsoliderar det så går vi till ett system som redan har dom här sakerna på plats redan från början.	
95	Interviewer	Tror du det är en vanlig approach att man på något sätt, nu gäller det bara att plåstra om så att allt funkar? Och att de flesta siktar på att göra en ändring över tid.	
96	Interviewee	Jag tror det flesta tänker så.	The Right to be Forgotten, the Right to Access and the Right to Data Portability

97	Interviewer	Det är väl svårt att kasta om sina dataprocesser som jämn?	
98	Interviewee	Ja det kommer vara mycket att jobba med det som redan idag är brister så det kommer inte finnas plats att göra allt redan från början. För man har bara en viss bandbredd att jobba med.	The Right to be Forgotten, the Right to Access and the Right to Data Port-ability
99	Interviewer	Så det kommer bli plåstra om och sen incremente-ellt?	
100	Interviewee	Ja tills man har en perfekt lösning	
101	Interviewer	Vad tycker du är den viktigaste eller svåraste aspekten av GDPR? Största förändringen kanske	
102	Interviewee	Det är mer ett mindset att man måste kontrollera något innan man gör det. T.ex. big data är en stor del. Big Data går inte att göra bara sådär, vi har massa flöden här och vi har en massa data wow om man sätter ihop de här två grejerna kan vi få det härа. Detta kan vi sälja det är jättebra! Det går ju även i GDPR men du måste vara klar med vad du tänker göra. Du måste tänka innan du gör saker,. DU kan inte bara testa och se nu fick vi detta det kan vi sälja utan du måste titta innan och se detta vill vi göra. Vi har data i de här två systemen nu vill vi kombinera detta och få den här datan. Men då måste vi gå till-baka och kolla samtycket, nä det kan vi inte göra jaha då får vi gå tillbaka och ändra samtycket. Och säga nu tar vi den här datan och kommer kombinera med den här datan och kommer leverera det här då är det okej. Du måste vara mer precis när du gör något. Du måste tänka innan du gör något.	
103	Interviewer	Du kan inte råka hitta något?	
104	Interviewee	Nä precis det är många som är i sin egna värld och tittar på det ”det här är skitbra kolla jag gör denna tekniska grejen” och det har man kunnat innan på ett lättare sätt nu måste man kolla kan vi göra detta? Har iv rätt samtycke? att verifiera samtycket med våra kunder för det är deras samtycke som vi levererar på så att vi har rätt där hela vägen ut. Och där måste vi säkerligen hjälpa dom och förstå det på ett helt annat sätt och när de vill förändra det att det går steg för steg på rätt sätt. Vi vill ha detta nu och då vill vi ha detta och då måste ni ha detta så det är mycket kom-munikation med kunder som jag ser det för att få allt på rätt plats.	
105	Interviewer	Så det är det ni som controller och processor, som processor blir det ett extra led om man vill jobba med sin data för då kan controllers säga ja men det är inte vi intresserad av. då faller det där liksom?	

106	Interviewee	Ja precis det kan vara en kund som vill göra detta. Då tänker vi att vi gör det för alla, men de andra kanske inte vill göra den här förändringen för de ser ingen business i det. Ska vi göra den för den kunden så måste vi ha en specifik lösning för dom och är det värt det? Kanske kanske inte. Det blir mer komplexa frågor på det sättet. Fler stakeholders som måste checkas av. Och sen blir det en förändring när man skriver avtal. Så fort vi tar in persondata så ökar vi vår risk. Och vi måste ju veta hur vi levererar på den här persondatan. Tidigare har vi bara sett ett nytt avtal som en, beroende på hur stort det här avtalet har varit pengamässigt in, har vi då haft steg då vem som skriver under. Kan det vara landschefen eller ska det upp till ledningsgruppen. Men nu är det baserat på persondatan, för det kan kosta oss väldigt mycket i risk så där måste vi göra om hela processen. När risken är så pass stor måste det gå upp till en viss nivå så där är också att man måste titta på de när man tittar på sina tjänster också. Och va mycket säkrare på det. Vi ser många avtal på kunder där de försöker trycka ner risken på oss, att vi skulle ta hela deras kostnad om något skulle hända. Det kanske vi inte är intresserad av risken blir för stor för oss, ICAs omsättning vi kan inte ta 4% av den, ska vi ta deras 4% och våra 4% det finns inte. Vem ska skriva under det? Kan vi göra det som ******? eller måste vi dra upp det med ledningen på ********.	
107	Interviewer	staketen är alltså högre?	
108	Interviewee	Ja allt blir ju så mycket mer.	
109	Interviewer	Har du märkt att det finns en sån här lite att kontrollera försöker bli av med ansvaret man måste förhandla om var det ligger?	
110	Interviewee	Ja tidigare har det varit väldigt låga summor i avtalen så att säga. Upp till vad kostnaden är på tjänsten så att största risken är att dom inte betalar något för tjänsten dom har kört. Nu är det ju till dom här nivåerna där de trycker över all kostnad på oss om det skulle hända något den risken kan vi inte skriva under det är ju omöjligt. Så det är mycket mer juridik med i avtalsskrivandet än det varit tidigare . Tidigare va det mer schabloner. Upp till den här nivån, fine!	
111	Interviewer	Har ni redan med jurister på möten som ni inte hade tidigare?	
112	Interviewee	Det har blivit mycket mer, processen är mycket längre i med att avtalen är mycket större redan direkt och man går ju mycket mer in på detaljer, hur gör man det hur gör man det hur gör man det. SÅ det tar ju mycket längre tid och vi måste ha lite med hela tiden. Det är mycket det här översätta mellan informationssäkerhet och juridik och tvärtom . Här är data	

		krypterat så det är inga problem, ja men vad händer om, ja det är inga problem det är ingen data längre det är bara en låda.	
113	Interviewer	Känner du att det finns ett kunskapsgap mellan det juridiska och folk som kan tekniken?	
114	Interviewee	Det har ju alltid funnit s men det blir ju mycket mer nu när man går in på detaljnivå innan har man kunnat skriva ett avtal som bara legal kört men det har varit fine. Nu är det mycket mer i detaljerna hur länge sparar vi datan hur gör vi detta och hur förser vi datan till dom och vilka format ska datan vara i. Och det är inget som dom riktigt förstår i detalj så man måste vara med och stötta dom. Och måste förstå det juridiska också.	
115	Interviewer	Det går på båda hållen?	
116	Interviewee	Japp jag tror det kommer fler hybrider på sikt, samma som man kunnat IT och affärskunskap tidigare kommer det finnas de kraven nu. I med att allt är avtal idag så är det nog framtiden.	
117	Interviewer	Tack det var nog allt vi hade.	

Appendix 3: Bob

Paragraph	Person Speaking	Text	Coding Reference
1	Interviewer	Din roll i organisationen?	
2	Interviewee	Jag jobbar som projektledare och portföljägare.	
3	Interviewer	Och hur länge har du varit det?	
4	Interviewee	Ungefär nio månader	
5	Interviewer	Hur skulle du beskriva en vanlig dag	
6	Interviewee	En vanlig dag… den börjar med att jag går igenom dem uppkomna punkterna, vad vi har, sen så har vi en liten snabb genomgång jag och systemarkitekten, vad som kommer komma upp under dagen, för tillfället sitter jag med mycket projekt i uppstartsfas, så det är mycket ee-jobb, vanligtvis under dagen har jag någon dialog med *****, vår säkerhetschef gällande någon av punkterna som har kommit upp, för det brukar vara några gemensamma beröringspunkter. Och sen så är ju den ena dagen inte den andra lik, hehe, det brukar bli mycket diskussioner kring en del saker.	
7	Interviewer	Men, du arbetar med någon process där persondata behandla	
8	Interviewee	Absolut, i alla projekt som vi sysslar med eller har på radarn nu, kommer vi ta hänsyn till persondata i någon form. Så är det. Eftersom jag jobbar inom IT och vi ansvarar för våra kärnsystem där vi har all kunddata liggande är det oundvikligt att transaktioner skulle innehålla persondata.	
9	Interviewer	Så att det är egentligen, ja , var dag är en…	
10	Interviewee	Absolut, på något sätt är vi berörda.	
11	Interviewer	Ja om vi dyker in lite mer i GDPR, lagar osv, när det kommer till samtycke, biten med att man måste godkänna, kommer det ändra någon process som du är med i? Det måste vara mer ändamålsriktig och mer informerat till personen som delar med sig av datan.	

12	Interviewee	Precis, det kommer ju att förändra de delar där vi jobbar mot customer facing applications, web gränssnitt, GUI, där slutkunder faktiskt agerar eller administrerar. Där kommer vi behöva ta hänsyn till det lösnings mässigt. Sen kommer inte jag fylla det innehållsmässigt, men lösning mässigt måste vi se till att det finns förutsättningar.	
13	Interviewer	Men ni agerar oftare processor, att ni hanterar data åt någon annan? Snarare än att ni samlar in data själva.	
14	Interviewee	Vi är ju en communication channel partner, så vi gör ju ofta precis som du säger, så utför vi det, och är deras omnikanal distributör av deras budskap, räkningar, whatever. så absolut, tanken är inte att vi ska buffra några data mängder för eget bruk. Absolut inte, tvärtom, vi lagrar ju åt kunden. så där är vi väldigt bundna av det.	Storage Limitation and Data Minimisation
15	Interviewer	Det finns en… Ni har en controller roll ibland? Ni har ju kunder som ni får data av, men ni kanske också samlar data om dem? Ni har båda aspekterna?	
16	Interviewee	Ja och det är ju en individuell dialog hur det sker. Men absolut finns det ställen där det i arkivformat, anpassat just för att generera information till kunden. Men det är fortfarande dem som har signat med sin användare. Den slutliga B2C kommunikationen har ju dem, och vi står för kanalen. Vi säkerställer såklart att vad de kommit överens om med sin slutkund. men vi initierar inte det.	
17	Interviewer	Nä precis, där blir ni processor	
18	Interviewee	Vi är transparenta.	
19	Interviewer	Men det där du pratade om hemsida, se till det här med samtycke, kommer ni ändra mycket med att det ska vara informerat samtycke? det är ju lite tydligare krav på att den som lämnat ut sina personuppgifter verkligen förstått vad som händer och aktivt då godkänner. Får ni ändra några processer där? Tex, det här måste vi verkligen ändra på eller ligger det mesta i linje med vad ni gör idag?	
20	Interviewee	Jag tror det är utökningar, sen är i vi i ett skede där vi ska förändra en hel eller de här delarna, bygga nytt och då blir det ju såklart, ett randvärde att vi måste ha med det från början, så på så sätt är det en god förutsättning att vi behöver inte titta så mycket på legacyn utan vi skapar nytt, vad de gör utifrån dessa förutsättningarna	
21	Interviewer	Kommer den här ändamålsbegränsningen, kommer det ändra något	

22	Interviewee	Där kommer det förmodligen att innebära vissa utmaningar, eftersom det är individuellt för varje kund, vi jobbar ju B2B, business to business. Men vi har kommunikationen B2C, så där måste vi ta hänsyn, vad har vår kund egentligen fått för krav eller överenskommelser med sina slutkunder? Och det kan bli individuella konfigurationer för varje kund, från mitt perspektiv blir det en stor del av utmaningen att vi har så generiska motor som möjligt, så vi inte behöver göra individuella flöden. vi håller oss så nära kunderna som möjligt med ändringarna som är unika.	Consent
23	Interviewer	Har det tidigare varit att man har haft generiska avtal? Eller snarare, har processerna varit generiska?	
24	Interviewee	Ja processerna i sig, men avtalet har skilt sig åt mycket. vi hanterar ju mycket myndigheter och då har de ju ett helt annat regelverk jämfört med privata intressen. Och när det gäller marknadsmässiga avtal så har de såklart kanske sina likheter, men det är ändå mer specifikt.	
25	Interviewer	Men, målet är att ha kvar generiska processerna som ni har idag? Fortsätta ha det generiskt även fast man är anpassad till GDPR.	
26	Interviewee	Precis, strukturera om så de anpassas till de här, exempelvis, att man inte cachar data på något onödigt ställe, behåller struktur och är bra på det generiska planet men samtidigt tar hänsyn till kundens unika krav	
27	Interviewer	Är det svårt med uppgiftminimering? Det här med att man hanterar den specifika data som är godkänd att processeras? Tidigare har man mer eller mindre kunnat ta allt, men att man måste begränsa det till de specifika punkterna som måste godkännas. Är det problematiskt?	
28	Interviewee	Jag tror det blir en utmaning ur den synvinkeln att vi måste ta en dialog med en och var av våra kunder. Vi kan inte ta ett gemensamt grepp på det, att säga nu begränsar vi CRM strukturen med det här och det här, och ERP så här. Utan kommer behöva ta en individuell dialog, hur har dem satt upp kontrakten med sina kundet så vi verkligen kan ta fram rätt produkt till dem. Det tror jag blir rätt mycket jobb.	Storage Limitation and Data Minimisation
29	Interviewer	Men mycket i dialog med kunden som samlat datan?	
30	Interviewee	Verkligen, verkligen, absolut.	
31	Interviewer	Kommunikations biten verkar vara återkommande	
32	Interviewee	Ja	

33	Interviewer	Sen har vi ju rätten till tillgång och rätten att bli bortglömd som slutanvändaren har. Hur kommer det påverka er?	
34	Interviewee	Där kommer vi behöva göra system mappningar på ett annat sätt. Där har vi arkivlösningar och sen så har vi löpande beställningar, som internetbankfakturor, som ligger buffrade några dagar innan de går ut till banken. Och sen så ligger det kanske en historik i valvet med fyra år för den här personen, så hör den här personen av sig till sin leverantör, säg mobiltjänster, och säger nu vill jag bli bortglömd. Dem kommer då lägga en beställning till oss som säger att den här personen ska anonymiseras, då kommer vi behöva en systemmappning för att vi effektivt ska kunna hålla de ganska tighta tidsramarna som krävs. Det kommer definitivt kräva arbete.	The Right of Access, the Right to be Forgotten and the Right to Data Portability
35	Interviewer	Men det är främst då rätten att bli bortglömd? Eller rätten till tillgång osv kanske är samma process?	
36	Interviewee	Exakt, i den mappningen som ligger till grund där. Vi kommer behöva mappa upp så vi kan identifiera brukar, dvs, users, i systemet, kundens grund. Samtidigt som vi inte identifierar den på toppnivå, som kan missbrukas, utan det måste ligga kvar där det ligger idag, men vi måste ändå kunna tråda det så vi kan hitta det enkelt. Där har vi ett jobb framför oss. Och det tror jag de flesta har, att sätta identifieringskoder och liknande. Hur bygger man en struktur på bästa sätt.	The Right of Access, the Right to be Forgotten and the Right to Data Portability
37	Interviewer	Så det svåra är egentligen att man på något sätt ska integrera legacysystemen med kommande GDPR, snarare än att gör rätt i framtiden?	
38	Interviewee	Anpassningen där är ju såklart en utmaning, men det tror jag ändå vi kan lösa. Men mycket är ju legacy data, alltså datan som vi byggt upp. Den måste ju nu då, på något sätt, struktureras och mappas.	
39	Interviewer	Nä just det för den har inte varit det när den en gång samlat?	
40	Interviewee	Nä, där är det ju så att man kan söka på ert namn, så hittar man det som ligger på er. För vi vet att vår kund med er att ni får vara kända som kund, och vår kund i sin tur då får lov att lägga det hos sin underleverantör som är oss. Vi får hantera det. Men så kommer det inte att vara.	The Right of Access, the Right to be Forgotten and the Right to Data Portability
41	Interviewer	Men kommer det vara svårt att säkerställa att nu är verkligen allt borta? Kommer det vara svårt eller har man ändå så pass bra kontroll på processerna att det kommer gå?	
42	Interviewee	Det kommer nog inte vara enkelt, men det kommer gå rättså bra, men jag kommer tillbaka till det att mappningen måste vara gjord, så vi inte glömmer bort att den här personen är kund i ett annat system	The Right of Access, the Right to be Forgotten and

		eller användare i ett annat system. Med en datapost iaf. Så det kommer tillbaka till den punkten.	the Right to Data Portability
43	Interviewer	Och dataportabilitet, det här med att man ska kunna leverera data i någon form så om man vill byta tjänst, så ska man ha rätt att hämta ut den i ett någorlunda smidigt format, är det samma sak där?	
44	Interviewee	Det kommer till samma grej, det är mappa, skapa den typen av strukturer, där ha vi jobbat mot generiska format, på vissa av systemen, men de är kanske inte helt harmoniserade. Det måste vi ju titta på, vi kan ju inte leverera åtta olika filer till en person, utan måste harmonisera det så vi får ut ett dataformat, exempelvis, eller en paketering.	The Right of Access, the Right to be Forgotten and the Right to Data Portability
45	Interviewer	När det kommer till territoriellt tillämpningsområde, asså att det är utanför EU, har ni några processer där, för där kommer ju lagar även att vara tillämpbara, men de kommer inte vara, lite problematiskt eftersom de inte befinner sig inom inom EU. Men lagarna ska ju följas....	
46	Interviewee	Nä vi ska vara inom EU. Vi ska vara ett nordisk bolag. Och egentligen ska all vår data ligga på nationell mark. Men inom EU, som regelverket styr, det kanske kan hända, men det ska vi tydligt reglera. Men utanför EU ska vi inte vara.	Territorial Scope
47	Interviewer	Men där har ni ingen process igång där ni håller på att skaffa en kontaktperson som befinner sig på rätt plats?	
48	Interviewee	Nej, gör vi det ska vi styra bort från det. ------ är väldigt tydlig med det så hehe	
49	Interviewer	Då kommer DPO-frågan, och det är ----- som är det? Men han sa också det skulle vara en person som CISO, som också skulle vara DPO?	
50	Interviewee	Ja, inom ----- (org.), de har ju en CISO och lite större organisation med security officers och någon av dem kommer också vara en DPO. Som jag har förstått det, men det är inte helt formerat än. Det är väl bilden, ------- var i Stockholm igår men vi har inte hunnit stämma av exakt var landet ligger. Men lite åt det hållet.	Data Privacy Officer
51	Interviewer	Och detta var för att lagen kräver det? Snarare än att ni känner att ni vill ha en DPO?	
52	Interviewee	Nä, jag tror diskussionen var att vi behövde en DPO, men inte riktigt hade headcounten för att formera en ny roll. Och kanske inte strukturen, men jag hoppas och tror att vi ska kunna styra det till sen att vi tar in en person till för att ----- inte ska behöva göra allting själv för det är helt orimligt i nuläget. Så att vi har en person som kan gå in och bli DPO, och ----- blir mer CISO eller så.	Data Privacy Officer

53	Interviewer	Men ser ni DPO som en extern person, den kan ju vara på arbetsplatsen men att den agerar mer som en revisor? Eller tänker ni ha en mer integrerad?	
54	Interviewee	Vi behöver ju ha en sån internt, vi hanterar så otroligt känsliga kunder och väldigt stora mängder data så är det en tjänst vi behöver ha. Nu när ----- både i den rollen och den strategiska säkerhetsrollen så blir det lite för mycket. Min bild, och den är helt subjektiv, jag bedömer det som att vi behöver en till person som sitter snett under -----, eller bredvid, beroende på hur man vill se det. Och att de bildar ett segme	Data Privacy Officer
55	Interviewer	Tror du att det är mer, inte bara tekniska kunskaper utan att det kommer behövas juridiska hållet ?	
56	Interviewee	Jag tror väl initialt att vi kommer behöva det. Det är jag rätt övertygad om, men där hoppas jag vi kan använda oss av ------ strukturen och nyttja deras funktioner där. Och eventuellt ta in consulting på lokalnivå om vi behöver det. Men, generellt sett, sen övertid så hoppas jag att vi ska kunna knyta upp oss mot det att ha en mer legal support från -------(högre upp i organisationen), men att ----------(lägre i org) inte behöver hålla den typen av kompetenser. Däremot att vi har en aktivt kommunikation mellan den som är DPO och den som sitter som legalförare på områd	Data Privacy Officer
57	Interviewer	Sen är det ju mycket transparens och dokumentation, det går ju igenom hela lagen, att ,man ska dokumentera och visa upp olika processer och så vidare. Är det något ni har fått förändra mycket för att kunna följa, den här dokumenteringen av processer?	
58	Interviewee	Det där kommer nog bli en hel del utmaningar att hantera det, så det tror jag nog att det kommer att vara. Sen kan jag inte säga vad det kommer innebära i detalj, men kommer innebära en hel del ändringar.	Transparency and Documentation
59	Interviewer	Så det finns ingen direkt plan, en strategi för; “så här ska vi dokumentera våra processer”, eller det kommer ske individuellt för varje specifik process?	
60	Interviewee	Nä, det kommer tas från toppen, men där håller vi på att titta på lite olika system, UML, baserat osv för att se vilket av dem som vi ska använda för att få en bra tydlighet, en generisk struktur.	
61	Interviewer	Är det för mycket processer för att man skulle kunna göra dem specifikt för varje, skulle det bli ett oändligt arbete?	
62	Interviewee	Nä det tror jag kanske inte i sig, men jag tror vi har mycket att vinna på att försöka hålla ihop det så mycket som möjligt. Men det är min bild. Sen så är där unika flöden som kommer behöva sin unika touch, härstans, så det är ingen diskussion där. Men jag tror vi kommer gynnas av att hålla ihop det så mycket som möjligt.	

63	Interviewer	Straffen, de har blivit rätt mycket hårdare, potentiellt hårdare, är det dem som har gjort att det har blivit ett sådant uppsving? Mycket snack om GDPR, motivering varför man vill ändra?	
64	Interviewee	Mycket är ju incitament drivet här i världen, det ligger säkert till grund till mycket. Men sen så tror jag det kuggar in rätt så bra i var vi är just nu. Det talas mycket om digitalisering, konstigt nog ska vi vara digitaliserade från ingenstans. Och då kommer ju detta naturlig som en addon som inte är så underlig att hantera. Men att det lyfts fram så otroligt mycket och får så mycket publicitet, JA, det tror jag definitivt handlar om penalties. Definitivt.	Penalties
65	Interviewer	Men märker du det också om du pratar med, nån som ni hanterar data åt, att de pratar om det, att det finns en dialog om GDPR?	
66	Interviewee	Absolut, det är håsat skulle jag nästan vilja säga, och det är inget fel, det betyder att vi har medvetenhet. Men det märker jag också med folk som är kunder men också folk i branchen, om jag talar med mina peers i olika nätverk. Det ät ju något som är på allas agenda, oavsett vilken bransch man är i. Hanterar man mobilnät, hanterar man hemlarm strukturer, hanterar man faktureringstjänster. Var man än sysslar med så påverkar detta oundvikligen.	
67	Interviewer	Men där du säger att det ligger i linje med vad man befinner sig som samhälle och som företag, tänker du att det egentligen är något positivt, bara positivt, att man får kontroll över sina processer och man hade gjort samma sak egentligen men över lite längre tid?	
68	Interviewee	Men jag tror att det är bra det här att man styr upp och får lite mer kontroll, och inblick, och jag inte något emot det. Jag är inte så mycket för integritetskränkning, jag tycker kanske inte att man ska få publicera folks uppgifter, alla har rätt till sitt privatliv, men under spårbarhet under kontrollerade former tycker jag inte är något negativt. Så det är bra att man får ett regelverk för det, för annars kan det vara att någon går alldeles för långt och någon inte startar ens, nu harmoniserar man förhoppningsvis det.	
69	Interviewer	Ja pseudonymisering av data, gör ni det nu	
70	Interviewee	Förlåt vad sa du?	
71	Interviewer	Pseudonyimisering	
72	Interviewee	Det kan jag inte riktigt säga faktiskt. Nä, Jag undrar det faktiskt. Delvis, delvis i vissa system. Men jag kan faktiskt inte detaljerna, om jag ska vara helt ärlig	

73	Interviewer	Men det finns inget, integrerat, vad ska man säga, standardiserat som hantera data som psuedonymiseras?	
74	Interviewee	Nä, det skulle jag inte säga	
75	Interviewer	Och sen kryptering, det blir lite mer kanske?	
76	Interviewee	Ja, kryptering, det klar att vi hanterar det dagligen. Med alla lösningar ska det finns krypterings steg, dekryptering och alla nycklarna ska vara konstruerade på rätt sätt. Det är en del av vår vardag.	
77	Interviewer	Pseudonymisering är kanske en nyare aspekt än va kryptering är?	
78	Interviewee	Ja, precis, kryptering har funnits så länge. Man har pratat om det och man vet vad det handlar om. Så jag tror det är därför det är etablerat.	Pseudonymous Data Encryption of Data
79	Interviewer	Men ser du det, det här är ju egentligen inga krav från GDPR, utan mer bara, vad ska man säga… nämnda förslag för att skydda.	
80	Interviewee	Exakt, men där tror jag kryptering är det vedertagna, som vi har använt, men den är kanske också lite mer riskfylld. Därför använder vi den. Pseudonymisering kanske kommer mer och mer, det gör det väl förmodligen. Men i nuläget ser jag inte att vi använder den i någon större utsträckning. Men jag vågar inte, vi har några inköpta system och där vet jag inte exakt hur det paketeras.	Encryption of Data
81	Interviewer	Och sen det här med data breaches, personuppgift incidenter, kommer det vara problematiskt, med att kunna rapportera, dels till myndigheter, dels till de personer som har lämnat sina uppgifter?	
82	Interviewee	Jag tror det, att det ser man om man tittar på de stora företag som haft det här att dröjt väldigt länge innan man har identifierat alla. Så det är nog en utmaning, men samtidigt har jag en tilltro till den tekniska utvecklingen att vi kommer få bättre verktyg. och jag vet att vi utvärderat några av dem med tämligen bra resultat. Så jag hoppas ju vi erbjuds det. Jag ser ju inte att vi rimligen ska utveckla det själva. Utan försöker hitta en bra lösning, någon slags log-bot hantering.	Breaches of Data
83	Interviewer	Men det är ändå, man måste investera för att kunna följa?	
84	Interviewee	Oh aboslut, definitivt. Vi kan inte stå som vi står idag, det kan nog ingen.	

85	Interviewer	Tror du en av det större svårigheterna med GDPR, att man ska kunna se vem som har varit drabbad, och sne kunna rapportera?	
86	Interviewee	Ja det tror jag nog, jag skulle gissa att vi kommer se en fantastisk bransch växa fram. Som håller på att växa fram just nu. För det handlar ju inte om aktivt skydd, utan om damage control. Och i det gränslandet är där väldigt mycket att göra.	
87	Interviewer	Vad hade vi mer på den….. Ja men precis, det blir lite samma där men, ni kommer öka säkerhetsåtgärderna? Ni kommer på någotsätt…	
88	Interviewee	Det kommer ske stora, eller hyfsat stora förändringar.	
89	Interviewer	Kommer de vara mer överliggande då, för hela organisationen, istället för specifika processer?	
90	Interviewee	Nä de kommer tryckas ner. Det kommer finnas generella riktlinjer, och sedan lkommer det finnas krav på att de implementeras i varje sub-system.	
91	Interviewer	Det blir lite både och?	
92	Interviewee	Ja, varje service manager, systemägare, måste ju säkerställa att de följer detta regelverket, vilket i princip betyder att de måste implementera det.	Data Privacy Officer
93	Interviewer	Men man kan ändå ha samma system?	
94	Interviewee	Absolut, det går förhoppningsvis att hitta en skalbar lösning	
95	Interviewer	Sen undrar vi om, ni anpassar era processer efter privacy by design, helt enkelt om ni räknar med säkerhet i skapandet av processer.	
96	Interviewee	Bra att du förklarar, det där privacy by design är lite flukturerande vad det innebär. Jo men det klart, som det ser ut nu så, vi har några saker som ska börja från scratch, vi ersätter gamla grejer och ska in med nått nytt, och då finns där ju som en grundtanke. Och ---- är ju en stark stakeholder som inte skräder orden att han vill ha in det, och jag efterfrågar det också, att vi behöver ha. Så det tror jag definitivt att vi kommer ha ett säkerhetsdrivet utvecklinngstänk långt framöver.	Data Privacy By Design and Default
97	Interviewer	Men är det på tidigare processer, fanns det tänket där?	
98	Interviewee	Nä det tror jag jag inte, det skulle jag inte säga	Data Privacy By Design and Default

99	Interviewer	Det är mer att man har byggt på de processerna?	
100	Interviewee	Då har man mer följt regelverk, tex med bankfakturor och liknande så finns det rätt strikta regelverk, och då följer man bara dem. Och thats it. Jag menar det är ju till och med en standard. På hur utbytesflöden (?) --- ser ut, så följer man dem.	Data Privacy By Design and Default
101	Interviewer	Men känner du att det är mycket som är helt nytt, och att man behöver göra om processer fullkomligt eller räcker det ofta att man tittar på den befintliga processer och lägger till någon aspekt, säg att det skulle vara psuedonymisering eller för data breaches eller sådär?	
102	Interviewee	Nä jag tror inte bara det är refinement, utan att det är refaktorering på mångt och mycket. Sen är det kanske inte att man river alltihopa och börjar om från scratch, men stora stycken kommer behövas skrivas om, i stor utsträckning.	Data Privacy By Design and Default
103	Interviewer	Tror du att man kommer lappa ihop det för att få det att funka när lagen träder i kraft och sen man efter det, inkrementellt…..	
104	Interviewee	Jag vet att -------- har gjort eller ledningen har genomdrivit ett GDPR arbete som är generiskt, så vi skapar de här förutsättningarna under det närmsta året, om vi lyskcas eller ej det får vi ju se. Men det är ju tanken att vi är fullt dedikerade från augusti efter sommaren, till att köra det här.	
105	Interviewer	Vad ser du som den viktigaste eller kanske den svåraste aspekten GDPR?	
106	Interviewee	Det är väl kanske en klassiker, man kan ju inte fånga alla kraven från dag ett, utan vara dynamiska i vårt tänkande. och sen så ha örat mot marken och höra vad som händer, eftersom vi inte vet hur tillämpningen kommer utformas i Sverige, men vi kan ju gissa att det kommer vara ganska nära ursprungs förslaget. Men, ifall om vi har en divergering i Norge, så måste vi se till att vi inte tappar det helt, utan att vi kan harmonisera det hyftsat väl, och inte har en unik Norgelösning och kör en Sverige/Danmark/Finland med någoting annat.	
107	Interviewer	Så det gäller att vara dynamisk i ändå en förändring?	
108	Interviewee	Det är ju ett agilt tänk i grund och botten att vi måste kunna förändra oss. Men vi måste ändå vara beredda på att det kan bli relativt stora förändringar mellan dessa länder, så det måste vi kunna hantera.	
109	Interviewer	Om vi vänder på det, finns det något du tänker, det här kommer inte vara några problem, det här tänket har vi redan från början eller den här lösningen hade vi från början?	

110	Interviewee	Ah, det vette sjutton om man ska vara så kaxig och säga egentligen. Utan jag tror snarare så att allt det vi bygger nytt det finns där från början, allt det som finns kvar av legacyn, det ska vi ta ett extra varv. Så ska man göra.	
111	Interviewer	Svårigheten med GDPR är egentligen hur omfattande den är?	
112	Interviewee	Ja vi ska inte ta något för givet, och det tror jag både är möjligheten och utmaningen. Vissa system så bra att det är en minimal twist så de där, medans andra saker, tyvärr, lite här får vi göra ett större jobb.	
113	Interviewer	Är det svårt att säga på rak arm, asså vet man ungefär vilka områden som kommer kommer vara mest drabbade eller är det verkligen att man tittar och inser att, herregud här är vi helt off, det trodde vi inte. Eller är det ganska lätt att estimera?	
114	Interviewee	Ah, hur långt är ett snöre? haha, Det vi har sett hitintills, vissa system, de visste om det, och har fått ta höjd för det, de måste göra ett rätt stort jobb med all kunddata hantering. Medans andra delar är att vi ska säkerställa att vi absolut inte ska hålla något vi inte ska göra. Samt att vi uppfyller de här kraven med mappning, så att, jag tror att det kommer vara väldigt omfattande, men samtidigt så får vi toppstruktur från ------ direktiv som gör att det ska vara genomförbart. Nått sånt.	
115	Interviewer	Ja det var väl egentligen det vi hade.	
116	Interviewee	Tack så mycket!	
117	Interviewer	Ja tack ska du ha!	

Appendix 4: Charlie

Paragraph	Person Speaking	Text	Coding Reference
1	Interviewer	Om vi börjar med mer allmänt och din roll i organisation?	
2	Interviewee	Jag är IT-säkerhet arkitekt på 50 %, Jag är ledare för it-säkerhetsgruppen så jag har hand om hands-on det som kallas för IRT-arbetete incident response och sånt där på halva tiden och 25 % jobbar jag för en organisation som heter SNIK(?) som är svenska superdata centrerna så dom akademiska superdata centrerna och är it-säkerhetsansvarig på dom. Så att det blir 125%	
3	Interviewer	Lite att stå i alltså. Hur länge har du gjort det här då?	
4	Interviewee	på **** har jag jobbat på i 30, på **** har jag jobbat i 30 år och sista 20+ har jag jobbat med it-säkerhet.	
5	Interviewer	okej och hur skulle du beskriva en vanlig dag?	
6	Interviewee	En vanlig dag börjar man med att titta efter vad som har hänt, man får en massa olika typer av larm och rätt mycket av det jobbar ju på natten och så får vi det på morgonen och då får man läsa igenom loggar och se efter om det är något som har hänt. Sen tittar vi på trafik registrering att allting funkar och att inget ser konstigt ut. Man läser in sig på nya buggar och lite sånt där. Är det något får man ju kontakta respektive avdelning och hittar vi något som är konstigt så utreder vi det.	
7	Interviewer	Men det är inte så att du är själv går in och ändrar saker utan du är mer övergripande?	
8	Interviewee	Vi är mer övergripande vi har haft en större bug som släpptes förra veckan som ligger i INTELs chip för fjärrstyrning av datorer asså autoband management av datorer vilket gör att även en maskin som står avstängd så kan man alltså nå den utifrån på ett trivialt sätt via vmc eller konsol inloggning. Och där fick vi ju leta rätt mycket här efter vilka finns det här och se till att dom försvinner från nätet eller fixas på olika sätt.	
9	Interviewer	Men det är mer en koordinerande roll, övergripande hålla koll?	
10	Interviewee	Ja vi har ju massor av kontaktpersoner som är ansvariga för datadriften ute på institutioner och fakulteter	

		och dom kontaktar ju vi så får de göra jobbet, vi är övergripande och göra inte så jättemycket hands-on förutom våra egna övervakningsgrejer dom sköter vi helt själv.	
11	Interviewer	Arbetar du med några processer där personuppgifter behandlas?	
12	Interviewee	Ja dels har vi vårt IRT-register alltså registret över incidenter och där står ju mycket personuppgifter. Förutom det har vi inte särskilt mycket personuppgifter i IT-säkerhetssidan. Vi har ett register över incidenter som sagt och vi har ett register över dom som är ansvariga för fakulteterna för IT-drift. Och det är i princip dom två registerna som jag och min lilla grupp har ansvar för.	
13	Interviewer	Men du känner inte till mer hur ***** Universitet kommer tackla GDPR osv. Har ni något ansvar i den frågan?	
14	Interviewee	Jag vet ju det på så sätt att jag suttit med i den utredningen som vi började i höstas som blev klar för 2 veckor sen. Det är ju en ganska gedigen utredning som är uppdelad i två bitar där den första biten som är klar nu den gick igenom hur vi organisatoriskt ska klara övergången till GDPR och den andra är mer hands-on hur ska vi göra det här. Nu övergår jag till referensgruppen så jag slutar i själva hands-on jobbet att skriva rapporter jag går över i lite mer referensgrupp rollen. men där har jag fått en ganska bra inblick för GDPR i universitetsvärlden.	
15	Interviewer	Alltså typ gemensamma riktlinjer för Universitetsvärlden?	
16	Interviewee	Ja först och främst måste du ju ha ett antal personella förändringar. Johanna som är PUL-ombud och jobbar på som PUL-ombud på 25% det räcker ju inte, det räcker ju inte idag, och det kommer definitivt inte räcka när GDPR är igång och då måste vi ha någon heltid för det. Informationssäkerhetsarbetet har vi inte utpekat hundra procent var det ska ligga. Utan informationssäkerhetsarbetet på **** är lite uppdelat på IT-kontoret på **** på säkerhetschefen, där finns inte någon nedskrivet exakt vad är det som ingår och var ligger ansvaret. Så det är en sak som måste åtgärdas också. Sen finns det andra styrleds dokument som måste skrivas. Så att i stora drag är det personella och organisatoriska förändringar som ska göras. Och klargöra var ansvar ligger och så här i den här utredningen. Ni kan gärna få den eftersom det är en allmän handling.	
17	Interviewer	Men om man går in mer specifikt på lagen och kollar på samtycke, det ändras ju där hur man får samla data, påverkar det er någonting?	

18	Interviewee	Ja det kommer det göra för vissa saker som vi har samtycke till kanske inte gäller, och för att få reda på det måste vi först inventera samtliga register vi har, de måste gås igenom och tittas på, på vilken grund har vi samlat den här informationen. Då kan vi dels som myndighet har vi tillåtelse att för register vi får föra register i vår myndighetsroll, alla statliga myndigheter har den rätten, om det faller utanför vår myndighetsroll kan det då vara stadsregister som vi har direkt informationsplikt på att samla och det är ***** t.ex. det är stadsregister. Så det måste vi ha och det finns ju några stycken det är den och det är spa och kriminalvård och polisen och lite så här. Sen så är det då samtycke och där kommer det vara lite mer problematiskt. Gäller det samtycket vi fått, måste vi fråga dom igen?	Consent
19	Interviewer	Så det svåra är lite grann legacyn som ligger kvar?	
20	Interviewee	Det fjärde sen är ju avtal vi får ju föra ett personregister för löneutbetalningar, närmaste anhöriga och lite såna saker som liksom universitetet behöver som arbetsgivare, och då anställningsavtal också ett avtal och då får vi rätt att föra visa register. Där måste vi se efter i vilken grupp hamnar de här personuppgifterna. I de tre varianterna där vi slipper fråga om lov är det helt okej. Men där vi måste ha samtycke måste vi se efter om det fortfarande gäller, har vi ens bett om samtycke? Det vet vi inte. Är det registrerat någonstans?, bara för man gett samtycke så måste man också veta, man måste spara det någonstans, att det finns ett samtycke. Och vad man gett samtycket till så där kommer vara ett litet problem. Sen får vi ju också föra personregister för forskning. För statliga myndigheter finns det tre stycken utredningar på gång. Den ena utredningen kommer i slutet på våren i början på sommaren och den gäller för GDPR för myndigheter. Sen kommer GDPR för utbildning och den kommer i början på hösten och sen kommer GDPR för forskning och den kommer inte förrän i December. Så att vi har ganska kort om tid från att den sista utredningen är klar till att vi måste vara färdiga.	Consent
21	Interviewer	Och ni påverkas av alla?	
22	Interviewee	Vi påverkas av alla ja. Sen kommer det vara massor av utbildningsinsatser. Så att alla får reda på vad de behöver veta. Gemene anställd behöver kanske inte i varje fall behöver få veta mer än ramverket och allmänt vad som gäller, är du forskare och har hand om personuppgifter har du rätt mycket att tänka på. Det kan ju vara inte bara personuppgifter utan det kan vara etikprövning och massa andra sådana här saker plus det att din finansiär kan kräva att den datan du samlar in ska göras allmänt tillgänglig. Under open data konceptet. Så där kommer det vara ett litet problem och universitet kommer antagligen lösa det så att universitetsbiblioteken får den här rollen som hjälp	

		och support central så att det ska finnas en one-stop shop som man kan gå till och fråga vad behöver jag veta? Jag ska samla in den här datan hur måste jag arkivera den? Hur måste jag spara den? Vad gäller för etikprövning vad gäller för GDPR. Så att det finns ett stället man kan gå och få reda på va behöver jag veta om det här datasetet jag behöver. Hur länge får jag spara det och under vilka premisser får jag använda det? Och det är också en sak som den här utredningen gör klart	
23	Interviewer	DÅ blir det nästan nationella riktlinjer som gör klart som sen kommer ner på universitetet som sen gör klart hur saker ska skötas?	
24	Interviewee	Sen när det gäller utbildning, och nu lämnar vi kanske pappret, men när det gäller utbildningssidan finns det just nu massor av diskussioner mellan de olika lärosätena i sverige som tar fram en gemensam utbildning. Att alla vi ska sitta och ta fram en likadan GDPR utbildning känns ju inte vettigt så det kommer antagligen göras i grunden, gemensamt.	
25	Interviewer	Och en gemensam tolkning av vad som måste göras och så här?	
26	Interviewee	Ja det bästa är ju om forskare som går från **** till **** eller *** till **** ser att vi använder oss av samma typ av grundinställning till hur man får använda data. Det gör ju saker väldigt mycket lättare för dom, de tar ju ofta med sig data i sin forskning. Det tar med sig det ifall dom går från göteborgs universitet hit. Då tar de ju med sig sin grunddata för att fortsätta forska på den om det är möjligt om det inte är så att de inte får lämna det lärosätet som den är gjord va, men mer och mer är öppen data idag. Mer och mer vill de ha med sig.	
27	Interviewer	Faller det under rätten till dataportabilitet? att ni är skyldiga-…	
28	Interviewee	Kan vara så, att när vi får pengar till ett forskningsprojekt så måste alla grunddata göras allmänt tillgänglig.	
29	Interviewer	Ni har inte, när det kommer till uppgiftsmininimering att man bara får hålla en viss mängd data under begränsade perioder?	
30	Interviewee	det är mer för vår egna administrativa databehandling. När det gäller forskningsdata, när det gäller medicinsk data så är det ganska tydligt, då är det etikprövningsnämnden som får berätta var är det du får använda den här datan till och hur mycket får du samla in, när det gäller forskningsdata så gäller inte den här minimerings principen du samlar ju in sociala data t.ex. över en population då vill du ju veta allt om den här personen, gruppen eller området för att kunna matcha saker mot varandra sen vill du ju samla in det över	Storage Limitations Data Minimisation

		lång tid så du kan jämföra det över tid. Då vet du ju inte riktigt behöver jag all den här datan, det är väldigt svårt att säga. För du försöker matcha olika saker mot varandra. Du kan ju inte gå tillbaka sen och samla in det speciellt inte om du samlar data över tid. Ett år senare kan du inte gå tillbaka och fråga för ett år sedan hur var det? Utan du måste ju samla in det då. SÅ då är det inte dataminimering som gäller, däremot om vi säger ett lönesystem eller om vi har såna enkla saker som när ni ska printa ut och ni ska ha ett eget konto med pengar på för att kunna printa ut. då kanske vi inte behöver adressuppgifter, det är ganska ointressant. Det är ju definitivt en dataminimering vi ska inte samla in data som inte behövs. Vi behöver inte ha närmsta anhörig i ett sånt register.	
31	Interviewer	Är det övergripande för hela organisationen, nu ska vi sätta oss ner och titta på liksom på alla dataprocesser och där vi håller persondata och liksom gå igenom eftersom det varit öppnare innan gissar jag på att man inte behövt ha samma koll?	
32	Interviewee	Innan har regeln varit att du ska rapportera det här, det finns fortfarande ett formulär på vår medarbetare webb , där ska du fylla i alltihop och där går det till ett mail till Johanna, som kollar, det här är personregister och det här ser okej ut och sätter det i pärmen. Men du kan inte sköta den organisationen över GDPR med en pärm, det funkar inte med ett ställe som är så här stort. Det måste finnas ett IT-baserat stöd för att föra de här registrens. Och det är ju också saker som vi måste titta på nu, sommar och höst så att det kommer finnas ett stöd så vi kan hålla en koll över vilka personregister finns det vem är ansvarig för det, vilken data finns det och i vilken rätt har vi att föra det här registret, var kommer data ifrån vart åker det ut från detta registret till andra register, hela den kedjan måste finnas. men det är inte designat än	
33	Interviewer	men man vill ändå kolla på helheten?	
34	Interviewee	Vi kommer titta på helheten	
35	Interviewer	sen typ mer få det mer strömlinjeformat göra det lite mer strikt?	
36	Interviewee	Ja	
37	Interviewer	Men jag gissar att det här går in lite på rätten till tillgång och rätten till att bli bortglömd, man måste veta var all data finns för att, det är egentligen samma sak där att man ska se över data processer för att se över var data hålls och var data sprids?	
38	Interviewee	Vi måste börja med att ta reda på var finns all vår persondata. Och när vi får reda på var all data finns	The Right of Access, the Right to

		får vi börja ta reda på i vilka system är det som behandlar all den här datan. Sen får ju de som äger systemet, så ansvaret kommer ligga på systemägaren, hela lagen är väldigt centrerad till ägandet av informationen det är alltid den som äger informationen som ska se till att den är säker att den behandlas på rätt sätt. Om den läggs i molnet måste de se till att molntjänsten har rätt att behandla datan först och främst sen att man skrivit ett datasäkerhets ombudsavtal så att den som behandlar data åt dig gör det på samma sätt som du har krav på dig att behandla data. När vi har kontrollerat att det är de här systemen får systemägaren en lista, det är det här som gäller för persondata, uppfyller ditt system det? om det inte uppfyller det, om det t.ex. inte finns möjlighet att plocka väck en person så måste man se till att det finns att ta en för möjligheten att ta väck en person, om det är så att det här registret ger dig rätt att bli glömd. Alla register ger dig inte rätten att bli glömd, du kan inte bli glömd i *****, du kan inte bli glömd i skattemyndighetens register, du kan inte bli glömd i kriminalvårdsregistret, du kan inte bli glömd i polisens register så du kan inte bli glömd överallt, men där du har rätt att bli glömd måste det finnas rutiner för att kunna plocka väck dig. Du måste kunna exportera din data det är också en rätt du har, alltså jag vill inte bli behandlad i ditt system jag tycker att ditt är mycket bättre, jag vill ha ut all min data i ett digitalt läsbart format från dig för att sätta in i ditt system istället och det måste vi kunna göra. Det kan vi inte idag. Därför kommer det finnas rutiner som måste byggas om och det är systemägarens ansvar, det kräver pengar det kräver tid och det kräver programmerare och det kommer vi inte vara färdiga den 25e det är bara att inse, men har vi en plan så, det kommer vara så många människor, så många organisationer som inte är klara men har du inte en plan kommer du kunna råka illa ut men har du en plan och säger vi gör det viktiga först och sen kanske rätten att bli glad eller rätten att exportera kanske inte är färdig den 25e, då klarar man sig.	be Forgotten and the Right to Data Portability Data Privacy Officer Transparency and Documentation
39	Interviewer	Tror du det är så att man kommer få bygga om saker från scratch, gå tillbaka och bygga om system helt och håller eller kommer det vara att man bygger på eller begränsar funktionalitet eller?	
40	Interviewee	Jag tror varken vi har tid eller pengar att bygga om från början, det gör man inte. vad man däremot måste tänka på redan nu och därför har jag gått ut och pratat med folk som sysslar med systemförvaltning och nyutveckling, här är då rätten att bli glömd, privacy by design som ni måste tänka in i systemet nu för de system ni bygger nu är klart någon gång i höst eller kanske nästa vår så att stå inte med skägget i brevlådan och bygga om systemet det första ni gör till Maj. Så när det är färdigt i januari ska ni inte behöva bygga om det i maj så ni måste tänka in GDPR redan från scratch. För utveckling av system är en ganska lång process, det tar ju månader även för ett litet system	Privacy by Design and by Default

		innan det är i drift.	
41	Interviewer	i tidigare system och de ni använder nu, har det funnits någon ide kring privacy by design och privacy by default?	
42	Interviewee	Nä man har nog byggt efter de principerna, vad behöver jag? och de är så att jag tror att jag behöver lite mer data så samlar jag in det också eftersom det inte är förbjudet är det tillåtet och om jag tror att jag kanske behöver det är det ju rätt korkat att inte se till att jag har möjlighet. så där är nog en hel del system som har lite för mycket data, det är jag relativt övertygad om. Sen kan det finnas en design, om du designar ditt system så designar du din databas och när projektet är färdigt så blir det inte exakt så som man tänkt det från början, det justeras ju lite efterhand. Så det kan vara sådana orsaker till att man har mer data än man behöver egentligen. För att verkligheten har förändrats och man behöver det inte längre och tanken var kanske god när man tänkte den ett halvår tidigare.	Storage Limitations Data Minimisation Privacy by Design and by Default
43	Interviewer	Är det mycket av den datan som man samlat sen tidigare som man måste mappa om eller vad man ska säga? Indexera så att säga?	
44	Interviewee	Än så länge har vi inte en aning om det, vi har ju inte ens börjat inventera än. Nu är det så här att alla centrala system, det vill säga det är lönesystem och det är **** och det är allt ner till parkerings kontorets försäljning av p-dekaler, allt sånt där som är förvaltningens system. De behandlas och sköts efter en modell som heter PM3. Det är en modell för system administration och där står klart och tydligt. vilken roll har Systemägaren vilken roll har systemförvaltaren, vilken roll har IT-systemägaren eller IT-systemförvaltaren. Så ska man ha möte vid vissa jämna mellanrum och vad ska diskuteras så det är ett väldigt formellt sätt att sköta systemen, och någon måste äga systemet någon måste äga driften någon måste sköta dagliga rutiner och allt det där står i den. Där är det ganska enkelt, där har vi koll på vilken data finns i systemet, vem äger den och vem ska du gå och prata med. Så att den biten är jag inte speciellt orolig för, går vi sen ut till institutioner och fakulteter som ligger utanför förvaltningen, det vill säga resten av universitetet vår verksamhet, där kan det vara både högt och lågt. Vissa är säkert duktiga och har bra koll på sina system och andra har säkert noll koll på sina system. går vi sen ner till forskare och forskningsdata som kan finnas med olika typer av tillstånd där har vi nog ingen koll alls, så där krävs nog väldigt mycket inventering. Men det kommer att anställas en person, ganska snart, som på i princip heltid kommer att inventera system, inventera data, så det är en stor organisatoriskt jobb där.	The Right of Access, the Right to be Forgotten and the Right to Data Portability Data Privacy Officer Penalties

45	Interviewer	Kommer det vara i egenskap av data protection officer?	
46	Interviewee	nä, inte den biten utan det är möjligt att den personen kommer bli DPO men det kommer anställas eller det kanske är någon som redan finns, det sista jag hörde var att ***** nog kunde fixa fram personal för att göra det. de är duktiga på att organiserar och registrera saker, det är deras jobb. De sitter och organiserar och registrerar böcker hela dagen så de vet precis hur man ska göra och sådär. Antagligen kommer själva inventerings biten att skötas av ****, men det får vi se det är inte bestämt än.	Data Privacy Officer
47	Interviewer	Behandlar ni någon data utanför data utanför EU?	
48	Interviewee	Ja vi har data utanför EU, vi har box, eller nä dom lovade att de skulle vara inom EU men vi var tvungna att ta box när vi skulle ta en molntjänst det är alltså SUnets avtal det är alltså en nivå upp som tog det avtalet, då var box det enda som hade safe harbour avtal det hade inte dropbox och de andra konkurrenterna därför var det ganska enkelt, då var det bara box vi kunde välja. Sen tror jag faktiskt att de var sagt så att de har all sin data rörande oss som kund liggande inom EU ändå även om företaget ligger i USA, har vi data i USA har vi data i …? Ja vi har data i hela världen! Universitetsförvaltningen har nog inte mycket data utanför europa, det tror jag inte, men forskarna har ju data precis var katten som helst. Och det har vi ju väldigt dålig koll på.	Territorial Scope
49	Interviewer	Men det är ert ansvar?	
50	Interviewee	Ja, det ligger på prefekten. Prefekten, tyvärr är en liten slasktratt för ansvar. Allt ansvar på en institution hamnar hos prefekten och det är lite taskigt för han eller hon har ju faktiskt, skulle jag säga, ingen möjlighet att hålla sig a jour med allt som ligger på prefektens ansvar men allt nytt är också prefektens ansvar. Men jag är fullständigt övertygad om att vi har data över hela världen, forskare byter data med varandra, det gör dom standardmässigt. De har troligtvis ganska låg kompetens om vad de får göra och inte.	Territorial Scope
51	Interviewer	Kommer man behöva intervenera så här får ni inte fortsätta, håll datan inom EU?	
52	Interviewee	Ja vi måste ju lyda regler och det var ju så här att när GDPR först kom på tapeten och man märkte dels, när det var PUL var det du gör fel då får en smäll på fingrarna du gör avbull med fullt puder och så kan du börja igen, nu är det du gör fel, då får böter i värsta fall och de kan bli höga böter, då gick det till att vara en administrativ fråga till att vara en ledningsfråga. När det gäller pengar eller stora pengar går det tre lönegrader upp och då märkte man att vi måste göra	Territorial Scope Penalties

		något. Och det var då man gjorde den här utredningen som startade i höstas. När utredningen hade gjort sin första fas märkte man att det är mycket mer att göra än vad vi trodde från början, det här kommer ta tid, det kommer var en jäkla massa jobb och det kommer vara massor av utbildning. Alla måste ha reda på och alla forskare måste ha reda på hur de får behandla sin data, jag tror inte vårt administrativa system kommer vara problemet utan jag tror problemet kommer vara ute hos institutioner som för register på alla möjliga sätt och det kan vara massa olika gamla filemaker system, eller spreadsheets eller vad som helst hur de för personregister och det har vi ingen koll på. Och de som gör de gör ju det i bästa välmening. Men de måste skaffa sig tillstånd för att köra det. Det är inte så att de inte får köra det, för det mesta, men de måste få tillstånd att köra de. Det måste registreras och de måste veta var datan finns och de måste få reda på vad är det jag får ha i mina register och vad finns det för krav på mig eftersom jag för dessa registren. Och kraven kanske blir större än nyttan och då kanske de får tänka om lite. Och sen är det då forskarna som måste tänka på med vilken rätt för jag detta registret och har jag rätt att föra detta registret överhuvudtaget, ska det till etiknämnden? är det känslig data? Sysslar jag med genome idag, all genetisk information är känslig eller blir då innan var det inte.	
53	Interviewer	Kommer alla de forskarna gå tillbaka och revidera datan de sitter på?	
54	Interviewee	Det vet vi inte, det får ta beslut , hur klassificerar de sin data, och i det stora hela, informationssäkerkhets-mässigt är detta ett jättebra arbete, för alla svenska myndigheter måste följa ISO27000 serien, den berät-tar hur man ska sköta informationssäkerheten och där i står ju att all data måste klassificeras, är det helt öppen data som kan användas hur som helst är den skyddad data, är det känslig data, ska det här hållas jättehemligt. Nu har vi helt plötsligt en jättebra möj-lighet att faktiskt föra in det tänket i all data. Nu måste vi faktiskt gå igenom i princip alla data vi har. Och berätta det här ni måste informations klassa den ni måste säkerhetsklassa den är det ett personregister måste det göras en riskanalys, så det kommer massa krav. Så det är perfekt, ur min synpunkt och jättejob-bigt.	
55	Interviewer	Kommer det vara mycket så här med dokumentation kring processer? med logging etc.	
56	Interviewee	Ja, om du vill veta varifrån får jag min data och var försvinner min data. Inom IT-arkitekturen här görs det ju jättemycket jobb mestadels för förvaltningens sy-stem för att ta reda på var används olika data och vart skickas de från system till system, var tar de vägen? Så där har varit rätt mycket jobb kring de, och där finns ett it-stöd där man kan modulerar och rita upp alla dessa system och egentligen så är det så att om vi	Transparency and Documentation

		gör förändringar här, vilka andra system kommer det här påverkar om vi vill bygga om det här systemet till någonting nytt vilka andra system kommer det här påverka, vilken data får jag in i systemen och vilken data lämnar. Allt det här med GDPR hakar ju i väldigt bra med det här så jag ser framför mig om det här blir bra, har vi väldigt mycket vunnet information säkerhetsmässigt. Även om det här bara gäller persondata så kommer ju tänket förhoppningsvis att spridas över till allt annat. Sen är det ju så att den mesta datan vi har är persondata på något sätt. Vår affärside är ju utbildning och forskning och extremt mycket av det är ju persondata på ett eller annat sätt. sen geologer är ju mindre intresserade av det men även en GIS databas kan innehålla saker som indirekt kan utpeka en person och då är det en personregister, en adress kan vara en personuppgift.	
57	Interviewer	Är det svårt att avgöra, göra den bedömningen, är det persondata eller ej?	
58	Interviewee	det är fullständigt omöjligt, det var en person, jag ville inte indirekt peka ut en person, kan någon annan säga att det är fullständigt omöjligt. Hur stor del av ett genome behövs för att peka ut en person?	
59	Interviewer	ingen aning…	
60	Interviewee	20%, jag har pratat med forskare de säger 20% av ett genome, krävs för att peka ut en person. Men då krävs det att du har en uppsättning av hela genomet, är det då en personuppgift och är det då en känslig personuppgift? Jag vet inte, det är en bedömnings sak	
61	Interviewer	Ska ni jobba med pseudonymisering?	
62	Interviewee	det gör forskare hela tiden. Men pseudonymiserad data är också personuppgifter, så att så länge det inte är helt anonymiserat får vi räkna det som personuppgifter. Väldigt mycket ligger i social forskning är ju pseudonymiserad data du jobbar med, medicinsk forskning. men eftersom dom oftare jobbar över tid måste man ju kunna matcha så när man får in ny data måste man pseudonymisera det med samma nyckel så att de kan matcha data över tid. SÅ jo vi använder väldigt mycket pseudonmyiserad data.	Pseudonymous Data
63	Interviewer	Så det finns redan ett tänk kring det?	
64	Interviewee	Ja medicinarna har ju sen jättelänge det tänket programmerat i sig det här är ju känslig data det måste vi skydda. Och även, man kanske blir förvånad, på sociologi och allt det där, genusvetenskap var ju uppe och snackade kryptering på så det är ju väldigt mycket där man inte tror så är de väldigt noggranna med att skydda sin persondata. Raoul Wallenberg institutet	Pseudonymous Data Encryption of Data

		sysslar ju med bl.a. folkrätt och sånt här de får ju uppgifter från personer som kan råka illa ut i hemländerna om de får reda på vem de är så de är väldigt noga med att skydda sina källor. Det dyker upp precis överallt, så det har jag lärt mig under mina 30 år man ska inte tro att man vet var saker och ting finns eller hur de jobbar på olika ställen, forskare slutar aldrig förvåna än, frågar man va de forskar om är det inom fält som man överhuvudtaget inte trodde att någon pillade inom mycket mycket större än vad man tror från början, jag är mycket övertygad om att vi kommer hitta personregister och känsliga persondata, det kommer finnas precis överallt.	
65	Interviewer	Men det finns någon ide om att jobba kring pseudonymisering och kryptering? SÅ det kommer inte komma som helt nya koncept.	
66	Interviewee	Jaja, kryptering tror jag inte det är så hemskt mycket, alltså organiserad kryptering så att säga, pseudonymisering Ja, kryptering, ja vi har haft frågor det finns dom som är intresserade av att kryptera sin data. Men det är alltid lite farligt att kryptera sin data, om det skiter sig kan du bli av med alltihopa, så att du måste backupa det på ett vettigt sätt och om du backar upp det på ett icke krypterat sätt så har du en backup som du måste skydda på ett speciellt sätt så du kan inte låta den sitta i bandarkivet som vilket band som helst. Skiter det sig kan du bli av med allt.	Encryption of Data
67	Interviewer	Det är inga krav från GDPR, det är ju mer förslag eller vad man ska säga?	
68	Interviewee	Ja asså, jag tror inte vi kommer ha väldigt mycket kryptering, men intresset för kryptering kommer öka det skulle jag tro. Jag ser mer kryptering, om jag skulle åka till USA idag skulle jag inte ta me min egen laptop, skulle jag ta med mig uppgifter vet jag att TSA har rätten att ta min laptop och läsa uppgifterna som finns i den, och min telefon utan att berätta varför och bara springa iväg med den och tömma den. Så att jag menar jag jobbar med IT säkerhet och jag har en del uppgifter som inte är helt så att jag vill spridda dom överallt, så jag tar med en lånedator från jobbet så att jag vet att den är tom från intressant innehåll.	Encryption of Data
69	Interviewer	Har de rätt att kräva, det här går lite utanför GDPR , men även om den där krypterad har de rätt att kräva den enheten och att kräva nyckeln till den?	
70	Interviewee	Ja, du har ju två val antingen lämnar du nyckeln eller så åker du hem, du har ju alltid ett val.	
71	Interviewer	Du var ju lite inne på det innan med straffen, inte straff men bötesbeloppen. Tror du att det är det största incitamentet för att man ändrar processerna?	

72	Interviewee	Ja, tyvärr tror jag det är så, det här kom upp på ledningens bord i stället för våra teknikers och juridisk fråga. Helt plötsligt kan du ställa pengar mot pengar, det här kan kosta si och så mycket. Om vi pratar universitet, 20 miljoner €, eller 4% av 6 miljarder SEK. Det är liksom de högsta straffen vi kan nå. Vi har väldigt hög omsättning. den ligger någonstans kring 6 miljarder. Det kan bli dryga böter men det är ju inte så att vi kommer hamna i väldigt dyra bötesbelopp om vi inte verkligen gör det riktigt jäkla illa, om vi behandlar känslig data som vi inte har rätt på ett flagrant och korkat sätt och blir av med det till ryska hackers och det hamnar på en dump på pastebin för alla att hämta. Då får vi dryga böter. Nej bötesbeloppen gjorde att det hamnade på ledningsnivå, helt plötsligt hamnade de tre lönegrader upp, här måste vi göra något. Annars hade det inte gett, det här jobbet hade inte gjorts annars. På så sätt tycker jag det är jättebra, det är ett nödvändigt MSB har ju då kraven att vi ska sköta vår säkerhet efter ISO27000 standard. Och i den finns det saker som vi inte lever upp till. Jag kan inte driva sådana projekt ensam det går inte med tanke på hur utspritt det är när en person säkerligen kommer jobba 9 månader heltid med alla system och persondata som vi har. Jag har ju inte i närheten av de resurser för att avsätta det, vilket gör att vi inte kan leva upp till informations klassningen som står i ISO27000. Vi kan uppmana folk, nu måste ni informations klassa era system, det händer ju bara inte. Utan det måste ju finnas både piska och morot. I en organisation som är så väldigt mycket större än vad jag eller it-säkerhetssidan eller information säkerhetsansvariga är vi kan inte prestera så mycket pengar att vi kan få en organisation igång att prestera det här. SÅ därför har det tidigare varit så att vi gör så mycket vi kan så gott vi kan och så hoppas vi på att det räcker.	Penalties
73	Interviewer	Så GDPR bidrar till de mål ni har?	
74	Interviewee	Ja det gör dom, och om man ska vara ärlig så ja det var piskan som gjorde att det kom igång.	Penalties
75	Interviewer	Du tycker också att det ligger i linje med tänket, hur man ska behandla data idag?	
76	Interviewee	Ja jag har inget emot GDPR, tvärtom det är ett alldeles utmärkt sätt att titta på data och just persondata idag är så på vissa ställen är det hanterat på sätt som jag tycker är väldigt felaktigt, om du tittar på sociala medier t.ex. där man uppmanar och matar bara på med, och alla dina vänner där du har ett sociogram över dig och alla dina vänner, om du tar Facebook och google och slår samman så vet du fan mer om dig än vad dina föräldrar vet om dig. Och är det data som du vill låta komma på drift? KNAPPAST. Nä, så att vi är påväg in i där personlig information är väldigt värdefull , där det köp och säljs, där jag lägger upp mina personliga uppgifter på ett ställe och kanske t.om.	

		läser det här 75 sidorna långa deklarationerna om hur de ska hantera min data och jag är nöjd med det. Sen säljs företaget 2 dagar senare, då gäller inte det längre. Då är min data på drift till ett annat företag som gör vad fan det vill med det, och det är ju det landets lagar, jag vet ju inte om den här servern, det kan se ut som den ligger i europa men den kan ju lika bra ligga i Indien eller Kina eller whatever. Om jag inte kollar det, det är ju bara en com adress, så om jag inte kollar var den ligger så har jag ingen aning om var min data tar vägen. Så att jag är allvarligt orolig över säkerheten i persondata så därför tycker jag det här är ett alldeles utmärkt sätt att kräva att allting inom europa följer samma lagar, och företag som vill göra affärer och ha europeiska kunder måste också följa den för den är inte territoriell.	
77	Interviewer	Tror du det kommer att bli effekter då, tror du det kommer fungera?	
78	Interviewee	Fungera och fungera, ja inom Europa kommer den nog fungera ganska hyfsat. Det har kommit upp på bordet, plötsligt pratar folk om persondata, pratar man persondata måste man ju fundera, vad vill jag med min egna persondata. Det har kommit upp på bordet på ett helt annat sätt än det gjort innan, så att för europeiska företag så tror jag nog de flesta, för de flesta gör det nog en förändring. Men för andra, amerikanska, kinesiska, indiska, ryska, bryr dom sig verkligen? Ja dom kan ju få böter, men hur kan dom driva igenom böter i ett annat land. Det vet jag ju inte, det får vi väl se. Så att mycket är väl det där, vi får vänta och se hur de yttre delarna av lagen hur de kommer funka. Kärnan i lagen kommer nog funka ganska väl för europeiska företag och myndigheter.	
79	Interviewer	Men du har märkt att det finns ett större intresse både uppifrån och nedifrån?	
80	Interviewee	Ja	
81	Interviewer	Det är en början iaf.	
82	Interviewee	Ja man ser ju mycket nu när man läser facktidskrifter man får mail från massor utav företag, GDPR har plötsligt kommit upp och diskuteras och personuppgifter och persondata. SÅ att ja vi får väl se, ett år framåt kommer det vara ganska hett men sen får vi se hur länge det håller sig hett, intresset försvinner ju, och det är samma sak för universitetet, så länge vi lägger pengar i det här, så länge det finns ett driv i arbetet kommer det vara på agendan. Om den sen, om finansiering blir mindre, om det försvinner och så här försvinner intresset. Man måste göra reklam, man måste visa att man finns och så länge man gör det kan man hålla intresset uppe. Problemet med ett universitet är ju att vi har en 48000 studenter och de byter vi	Privacy by Design and by Default

		ut var fjärde år, och vi har 7000 anställda och de byter vi ut med ganska hög hastighet eftersom forskare kommer och går. Och vi har en hierarkisk nivå där vi har doktorander och labbassistenter i bottnen och högst upp sitter professorn eller rektorn beroende på hur man ser det. Varje steg i den här pyramiden måste man slå ut folk och då börjar de på andra universitet och vi får in folk från andra universitet så det är ganska hög omsättning på folk. Och det ska alltså vara så, man måste se andra ställen inom forsknings-världen, så man berikar sig själv genom att jobba med andra och flytta till andra ställen. Dom måste också ha samma utbildning, alla våra studenter måste få den utbildning som de ska ha för att fungera på ett univer-sitet och veta hur det funkar, och alla anställda måste ju också få en utbildning över hur fungerar ****** universitet och hur hanterar vi data. Där kommer vara lite problem, vi kommer ha en puckel här, det kom-mer säkert gå jättebra i ett helt år efter GDPRs inför-ande sen kan jag vara lite rätt för att, vad händer sen när intresset har svalnat, kan vi fortfarande hålla uppe nivån?	
83	Interviewer	Så det är inte en lösning som man gör en gång och sen är det klart?	
84	Interviewee	Det här är en process så det måste in i de processer som universitetet har, och som jag sa alla våra cen-trala problem hanteras efter PM3 modellen där kan man bara skriva in det, alla system vi utvecklar här utvecklar vi efter en mall, där kan man också skriva in den, då kan man inte bara gå förbi den då måste man tänka på det. Men allting annat. Allt som inte är cen-tral förvaltning. Där måste vi på något sätt, och det talas om att den här PM3 modellen kommer gälla för hela universitetet, så du kan inte komma undan att använda den här modellen om du ska ha ett IT-system någonstans. Då kommer det står där i den, antingen är du flagrant och bara stryker den punkten, det är inte intressant och då får du stå för det eller så måste du faktiskt ta upp den och fundera på den. Jag har per-sonuppgifter, ja jag följer den lagen, det är de här sakerna som system måste kunna om de har person-uppgifter i sig och jag har gjort en riskanalys. Jag har följt allt jag ska göra för att få ha mitt system. Så det kan bli bättre ifall förvaltningschefen bestämmer att nu ska allt förvaltas efter samma modell. Och forsk-ningsdata där måste det vara naturligt att hantera sin data, typ som att alla medicinare vet att de måste gå till etikprövningsnämnden för att det här är medicinsk data och om inte etikprövningsnämnden säger ja så får jag inte lov att hantera den här datan och alla fors-kare måste ha det här om persondata. Jag måste gå till den här one-stop shop för att fråga hur ska jag göra med den hära. Det ska vara allt från hur samlar jag in det till hur arkiverar jag det och det ska få reda på hela kedjan av hur de ska göra för att hantera det. Och till slut blir det kanske en naturlig del att varje forsk-ningsprojekt gör det här. Så att man inte behöver	Privacy by Design and by Default

		springa runt och säga nu har du fått pengar, har du personuppgifter, man kan inte springa runt och jaga folk, det måste vara en naturlig del i sättet att hantera det.	
85	Interviewer	Du ser det mer som ett organisatoriskt problem snarare än processer?	
86	Interviewee	Data processerna kan vi lösa, det är lösbart, problemet är det organisatoriska, hur får vi organisationen att förstå vad som måste göras med persondata. Och att vi sen blir uthålliga efter tiden, att det här fortsätter vara intressant och att vi fortsätter med den här processen. Universitetets förvaltning, nu pratar jag väldigt mycket förvaltning men det är mycket enklare att genomskåda för den fungerar på mer eller mindre på samma sätt. Det har ett processkontor och allt som ska göras gör i en process där det finns ett start och ett slut om det nu råkar vara ***** eller lönesystem eller va det råkar vara, så finns det en så här ska man sköta det här. Så här ska det här arbetet skötas. DÅ kan man skriva in i det att man måste titta på personuppgifter och då är det mycket enklare. Men som sagt me det är för förvaltningen. Men det här process tänket måste också in på forsknings sidan och utbildningssidan.	Transparency and Documentation
87	Interviewer	Ja vi börjar nästan nå änden här men vad är den svåraste aspekten av GDPR, vad är viktigast? är det den här organisatoriska aspekten att få människor att förstå vikten?	
88	Interviewee	Ja, vårt största problem till att börja med kommer vara att inventera allt detta och se efter hur hänger vår data ihop. Och i bästa fall kommer vi göra en inventering av både forskningsdata och persondata och slå ihop detta. Det här är forskningsdata men det innehåller ingen persondata men det innehåller information om bergarter i skåne, jättebra. Det här är ett löneregister det innehåller bara personuppgifter. Att vi sen, det här är all data som universitet i '***** har. Det här är datan vi äger och det här är personerna som äger den här data. Det hade varit underbart, att veta precis det här är all information som ****** universitet äger och ah det registrerat. Men vi ska vara väldigt glada om vi kan registrera all persondata från början. Så det kommer vara det största problemet, att inventera det. Sen över tid kommer det vara ett organisatoriskt problem att underhålla det. Jag tror att vi kommer ha ett gott engagemang i början, det är ett gott engagemang när man börjar och nu ska vi göra något här både rätt och riktigt och att det sen sakta men säkert försvinner ut i dimman. Om vi inte avsätter tid, pengar och reklam för detta. Så både piska och morot att det blir uppföljning av det.	
89	Interviewer	Japp det var nog allt. Det var bra, jättebra! Tack.	

Appendix 5: Douglas

Paragraph	Person Speaking	Text	Coding Reference
1	Interviewer	Din roll i organisationen?	
2	Interviewee	Jag är förvaltningschef, så jag ansvarar för bankens alla processer, kontinuitetshantering, avtal med outsourcade leverantörer, it-utveckling och it-drift kort sagt.	
3	Interviewer	Hur länge har du jobbat med det?	
4	Interviewee	två år	
5	Interviewer	Hur skulle du beskriva en vanlig dag?	
6	Interviewee	Jag kan beskriva mer en vanlig vecka. Det kanske är lättare. Jag har 12 personer som jobbar på förvaltningen så dels är det mycket att hjälpa dom att planera sina dagar och vad dom ska göra i form av, vi har också compliance ansvar i form av banken, så dom jobbar med att planera och implementera nya regelverk. T.ex. GDPR vad är det som banken måste göra för att förhålla sig till regelverken? Vad måste vi göra så att alla förstår? Vi måste kravställa mot alla leverantörer så vi träffar jättemycket leverantörer, hur ska dom se till så att både vi får vårt behov tillgodosett men också hur följer dom de lagar vi står inför. Och där är ju GDPR en men det finns en uppsjö av andra som rör bank och finansiell verksamhet.	
7	Interviewer	Många regler för bankväsende överlag liksom?	
8	Interviewee	Ja jättemånga. sen är ju min roll väldigt mycket att se till att allting fungerar, både internt hos oss mot våra kontor och så mot bankledningen så att de vet vad vi gör och hur organisationen påverkas men också vad leverantörerna att de fullföljer de vi har kommit överens om och ser till att vi hela tiden utvecklas vidare och att de anpassar sig till regelverk. Så jag är väldigt mycket överallt.	
9	Interviewer	Du kombinerar?	
10	Interviewee	ja	

11	Interviewer	Men du har en övergripande roll så jag gissar på att du även jobbar med processer där personuppgifter behandlas?	
12	Interviewee	Ja jag har 5 processägare och de är ansvariga för sina områden och vi mappar ju in vilket regelverk och vem som är ansvarig för det, så ibland måste de alla jobba tillsammans t.ex. GDPR slår ju överallt men jag har fortfarande en person som är ansvarig för infrastruktur och de bitarna och han är ansvarig för GDPR implementationen hos oss.	
13	Interviewer	Om man går in på lagen specifikt samtycke kommer ändras lite med GDPR, hur man får samla data kommer det ändra era processer och ändra hur ni behandlar data?	
14	Interviewee	Ja dels måste vi ju börja i våra avtal att det framgår att kunden ger sitt samtycke. Sen har vi väldigt mycket , det finns massa annan lagstiftning som övertrumfar GDPR vi måste ju lagra all dokumentation i 10 år t.ex. då måste vi förklara för kunden att när du väl är kund så kommer vi ta in den här informationen om dig och vi behöver lagra den för att det finns lagar som står högre än GDPR. Men däremot kommer vi se över, det har vi redan börjat med, alla våra system. Var är det egentligen vi har personuppgifter.Där det inte behöver finnas personuppgifter där ska det inte finnas personuppgifter heller. Så t.ex. kommer vi nu styra ännu hårdare att det bara är i vissa system där man får lagra kundinformation man får inte göra det i dom som inte går lätt att gallra t.ex.. och härleda var har vi nu personuppgifter, vi måste lägga kundspecifika information i vissa system bara.	Consent Transparency and Documentation Storage Limitation and Data Minimisation
15	Interviewer	Men det blir lite kring det här uppgifts minimering då? Att man försöker hålla det strikt med var datan är.	
16	Interviewee	Ja precis.	
17	Interviewer	Tidigare har det varit lite slappare, man har tagit den datan man har tyckt vara bra att samla i det här fallet så har man gjort det så?	
18	Interviewee	Ja dels de sen också att lagen har ju nu blivit mycket hårdare jämfört med hur PUL var uppsatt innan så att många alla organisationer som har kontakt med privatpersoner har tidigare funkat så att ja men jag skriver ner att ”petter” han pluggar på LTH han bor i Lund för att det är bra att komma ihåg till nästa gång jag träffar honom. Men allt sånt det är egentligen personuppgifter och det får inte vi lagra utan att gallra det. Och sånt här finns, det är typiskt sånt som man lägger i ett excel eller onenote någonstans, och det kommer vi inte kunna få göra längre eftersom det är personuppgifter så då måste vi kunna ta bort det om dig sen. Jag tror man måste skaffa en medvetenhet för dom som jobbar både med kund - och personaldata att allt sånt	Consent

		får man inte skriva ner annat än i dom system där vi vet att vi faktiskt gallrat efter x antal månader om du inte blev kund eller om du slutat vara kund.	
19	Interviewer	Så det både handlar om dataprocesser som måste ändras, men även organisatoriskt tänk?	
20	Interviewee	Absolut för vår del handlar det mycket om att få alla anställda att förstå vad man får skriva om kunder eller personal och i vilka system man får göra det. Andra delen handlar om att vi måste gå till våra leverantörer som driftar de höra systemen där vi får lagra om data om personer att dom måste har rutiner för att gallra och allt det här. Det är de två delarna som jag ser det.	Consent
21	Interviewer	Hur tänker du på rätten att bli bortglömd eftersom ni är bank, i gdpr får man ju möjligheten att ta bort information om sig själv men den påverkar inte er på samma sätt eftersom ni måste lagra information i 10 år?	
22	Interviewee	Precis, jag utgår från att kunden ger sitt samtycke nu, dessutom måste vi ha denna informationen i x antal år eftersom vi har bokföringslagar, men jag vet inte hur vi kommer att formulera det men någonstans där måste vi få det att framgå.	Consent
23	Interviewer	Men där finns det andra lagar som.. .	
24	Interviewee	Triunfar över ja precis.	
25	Interviewer	Det finns en hel del inom GDPR det är en lång lag med många undantag så det är ju verkligen från bransch till bransch hur man får förhålla sig till det. ?	
26	Interviewee	Ja precis	
27	Interviewer	Men gäller det så här med ändamålsbegränsning? tidigare har det varit så att man kunnat samla data med ganska brett syfte nu famlar det under data minimering där man bara ska ha persondata när man verkligen behöver. Vet du något där typ syftet är att man ska ha ett bankkonto och då får man bara ha det till det och göra några ändringar där?	
28	Interviewee	Nä jag tror inte det vi är inte riktigt framme i den analysen än men jag tror inte det. Det finns massa med bolag som korskör. Men vi gör inte det så mycket så jag tror inte det kommer förändras. men visst alla vill väl väl veta vad har kunden idag och vad kan vi sälja extra. Men vad gäller lagring och samkörning är det nog väldigt tydligt varför vi lagrar personuppgifter. Sen finns det ju också inom bank, detta kan vara intressant för er att veta, inom bank finns det en annan lag som är väldigt strikt som handlar om penningtvätt och terrorism. Där är vi skyldiga att ta reda på ganska mycket om våra kunder. vi måste klassa om våran	Storage Limitation and Data Minimisation Privacy by Design and Default

		kund är en högrisk kund eller inte för bankerna får höga böter om man tillåter ett kundbeteende som kan ha syfte att tvätta pengar eller finansiera terrorism. Och lagen den säger att vi måste veta hur många utlandstransaktioner någon måste göra på ett år, om du har det vilka länder?, hur mycket kontantinsättningar kommer du göra, så ganska mycket sån information som vi måste känna till om kunden. därför finns det rätt mycket lagar som säger att vi måste känna till det här.	
29	Interviewer	Så det blir många undantag?	
30	Interviewee	Ja det blir väldigt många undantag, där vi också måste, vilket jag inte har klart för mig än, förklara för kunden: ja vi ska inte missbruka personuppgifter om dig men det här måste vi veta pg.a. de här och de här lagarna.	
31	Interviewer	Ja det måste vara svårt när vilken lag möter vilken och när vilken trumfar den andra eller?	
32	Interviewee	Ja fast det är ganska, det är inte helt omöjligt att reda ut, man har ju jurister, och man jobbar ju mycket, jag vet inte riktigt hur andra bolag jobbar med olika granskningar av organisationen där man diskuterar igenom det är det här som gäller.	
33	Interviewer	När det kommer till rätten till att bli bortglömd som blir lite annorlunda för er, men det finns ju också rätten till tillgång att man ska kunna hämta ut data och att man kan hämta ut datan i något slags behändigt format, t.ex. om man vill byta bank tänker jag. Kommer ni få ändra något där?	
34	Interviewee	Allt det här ligger outsourcat för oss, alla våra system är ju outsourcade och vi är inte riktigt framme där. Det kommer ske mer och mer under hösten gå igenom alla leverantörer, det är ganska många system, så hur kan man plocka ut kunddatan just härifrån dårå. så det håller leverantörerna på och kollar på just nu hur ska de sätta upp systemen så man lätt ska kunna hämta ut den här informationen. Och det är därför det gäller att få alla anställda att bara lägga upp kundinformationen i systemen så att man inte måste gå till 10 anställda och fråga om dom har ett excel?	Right of Access, Right to be forgotten and the right to Data Portability Storage Limitation and Data Minimisation
35	Interviewer	Du sa det här med outsourcing, är det inom EU ni har outsourcat?	
36	Interviewee	Ja det har vi, vi har avtal också där man har skrivit att den här leverantören är införstådd med att den hanterar personuppgifter. Och därmed följa de lagarna också.	
37	Interviewer	Så ni har tagit i åtanke det också? Att inte lämna eu	Territorial Scope

38	Interviewee	Ja precis.	
39	Interviewer	Så ni kommer hålla er helt inom EU?	
40	Interviewee	Japp	
41	Interviewer	När det kommer till data Privacy officer jag gissar att ni är skyldiga enligt lag att behöva utse en sådan?	
42	Interviewee	Ja	
43	Interviewer	Har ni utsett en?	
44	Interviewee	Ja vi är lite i limbo just nu för han som var har slutat, så vi måste anmäla en ny, vi måste ju anmäla också. Så det är helt rätt. Men jag vet inte heller om det måste upp högre i organisationen, det är ganska många lagar som kommer nu som inte nöjer sig med vem som helst det är faktiskt VD som är yttersta ansvarig och har man någon annan måste man ha olika rapporteringar till VD så att både VD och styrelse är uppdaterade på status.	Data Privacy Officer
45	Interviewer	Det är lite olika hur man tacklar det hela. Om man tacklar det som en juridisk fråga eller om man tacklar det lite mer tekniskt. Vilken väg har ni valt?	
46	Interviewee	Vi valde den juridiska men för vår del är det egentligen lättare för den som är DPO ska egentligen anmäla sina kollegor om dom inte gör sitt jobb och då är det bättre om vi har någon som är jurist som anmäler oss som har alla processer och all teknik än att vi ska ha oss själva asså det blir lite konflikt i den.	Data Privacy Officer
47	Interviewer	Ja precis den ska agera lite som en revisor?	
48	Interviewee	Ja som en polis eller revisor.	
49	Interviewer	Lite extern inom men ändå utanför?	
50	Interviewee	Precis	
51	Interviewer	Funderade ni inte på någon extern person?	
52	Interviewee	Jo det gjorde vi också, men vi valde inte det då men det är omöjligt att vi kommer göra det.	Data Privacy Officer
53	Interviewer	Tror ni att ni kommer behålla den här juridiska approachen även efter, det är ju en del nu när man ska an-	

		passa sig för GDPR men det är även en efter när GDPR har trätt i kraft. Tror du man kommer behöva byta anfallsvinkel för att förhålla sig till lagen då? Det är ett steg när man ska anpassa sig och ett när man ska upprätthålla en process.	
54	Interviewee	Nä men jag tror, nä det tror jag inte nu men man ska inte missförstå det, för den som är DPO kommer jobba aktivt med det och granska det men vi kommer jobba lika aktivt , det är vi som har ansvar för att vi följer lagen, och även om vi implementerar den nu så är ju inte vi färdiga med det sen vi kommer behöva jobba med detta varje dag, varje månad och så vidare och det kommer vi ändå fortsätta göra.	
55	Interviewer	Sen är det nytt i lagen runt om transparens, dokumentation allt ska ju loggas och så här, har ni behövt ändra mycket där eller fanns det från början? att man håller koll på, man har dokumenterat hur en data process ser ut man kan rapportera om någon skulle fråga men hur gör ni här så kan man säga, fanns det sen tidigare?	
56	Interviewee	Till viss del finns det men det behöver detaljeras vi har ju processkartor och register över alla våra system och på vilket sätt hanterar vi personuppgifter i de olika systemen de har vi. Sen kommer vi behöva se över det nu och vissa saker som behöver detaljeras ytterligare. Men ganska mycket har vi	Transparency and Documentation
57	Interviewer	ÄR det mycket det här med vad ska man säga gammal data. När det kommer till ny data vet man ju ofta va man ska göra med den man ska märka den på ett visst sätt och den ska bara finnas här?	
58	Interviewee	Den gamla kommer bli ett gissel en stor surdeg.	
59	Interviewer	Är det då att man ska instansiera, mappa, bara så man får koll på vad man har?	
60	Interviewee	Ja vi har ju gjort en första kartläggning eftersom vi har ett systemregister, med alla våra system och i följande system finns det då personuppgifteruppgifter och då vet vi lite grann vad för personuppgifter som finns men det här med att mappa att få tag på all gammal data som ligger på folks PC's, inte riktigt post it lappar men typ post it lappar som ligger på folks datorer. Det är en förfärlig uppgift att ta sig an.	Transparency and Documentation Penalties
61	Interviewer	Jag tänker ändå att er bransch är mer strukturerad här att den är mer anpassad andra har mer att anpassa sig för, det man kallar privacy by design att det redan finns ett säkerhetstänk redan från början.	
62	Interviewee	Grunden är ju att bank är väldigt säkert som du säger. Så i det perspektivet så finns det ju mycket mer att hämta ifrån me sen tror jag att som för alla organisationer oavsett vilken du är att man inte riktigt har tänkt det här som jag sa, jag skriver ner en notis här om vad	Privacy by Design and Default

		”petter” gör eller vad ”kalle” gör” till nästa gång jag träffar honom. Så blir det mer hur gick det nu köpte du någon hund eller sådär. Man skickar ut ett mail i all välmening från personalavdelningen skriver här är en lista på alla er som ska gå på företagshälsovården det här året. Så står det både namn och personnummer en sådan lista i mail är förbjuden att skicka. Och det gör man ju i all välmening. Och det är där jag menar det är där jag tror att alla organisationer, det här mörkertalet som kommer bli fruktansvärt att gräva i.	
63	Interviewer	Så det blir svårare organisatoriskt än sig data process-mässigt? att man ska lära folk	
64	Interviewee	Ja det tror jag, både kunder och personal information-en,	
65	Interviewer	Tror du det kommer bli lite kallare kommunikation i med GDPR? Att man inte kan skicka ut den här in-formationen?	
66	Interviewee	Nä jag tror bara man ska vara lite mer försiktig t.ex. om man ska skicka ut information så får man bli duk-tigare på att skicka kanske en länk, här ligger den här nu kom och titta, sen rensar man och gallrar i grundsy-stemet, man behöver inte maila ut alla namn, man kan säga här finns informationen ni får gå in och titta så gallrar man där, det är ett sätt att lösa det så det gäller bara att ge alla rätt verktyg på något sätt.	Transparency and Documentation
67	Interviewer	GDPR har ju kommit upp lite mer på ledningsnivå tror du det beror på den höga straffavgiften? eller tror du överlag att det alltid tas upp?	
68	Interviewee	Jag tror att den kommit upp lite högre på lednings agendan men jag tror inte den är så högt som den borde. Faktiskt. Visst har det att göra med att vitena är högre det tror jag absolut för nu tar du ju inte några reprimander alls. Så att den överhuvudtaget diskuteras nu är ju för att vittna finns, det tror jag.	Penalties
69	Interviewer	Ser du det som en positiv förändring eller ser du det som bökigt att behöva anpassa sig. Eller ser du det som att i slutändan är det en ganska bra grej man får ordning på sina processer?	
70	Interviewee	Jag tror nog att det är bra men jag tror problemet är, och det märker man med många trender, det är att vi inte vet var allt kommer sluta. PÅ ena sidan har vi alla appar, sociala media alla som är, jag ska inte säga under en viss ålder men ofta är det relaterat till ålder, som bara ”accept”, ”accept” jag klickar mig vidare, jag vet bara t.ex. min son, jag bara vad är det här för mail? då har han börjat prenumerera på något och accepterat en jävla massa villkor förmodligen och har inte en aning om det och det är liksom, vi vill ju ha tillgäng-lighet till appar, lösningar, mobilepay, allt sånt där. Vi skriver under massor av saker som vi egentligen inte vet vad vi skriver under och så var det ju inte förr, då fick man ett avtal. Då tog man in sin mamma sin	

		pappa sin advokat och läste igenom sitt avtal i lugn och ro innan man godkände något. så någonstans tror jag att, ja, det är ju bra att vi styr upp sådan här beteenden så att våra personuppgifter inte missbrukas fullständigt för det ligger extremt mycket information om oss på google och facebook, de kan kartlägga allt vi gör egentligen och det har vi bara godkänt utan att veta vad det handlar om. Sen att det måste drivas till absurdum att få ut all information om dig och så, det kanske blir lite jobbigt att hantera, men någonstans tycker jag det är bra att det stramas åt, det tror jag. Nu är vi lite de jag menar vi vet inte var det kommer ta vägen för alla de här sociala medier de har exploderat, och nu säger vi att vi ska strama åt det jättemycket. Ja vi får se vilken gyllene mellanväg vi kommer att hamna i.	
71	Interviewer	Ja om dom väljer att gå på facebook de första de gör liksom?	
72	Interviewee	Ja till viss del har väl både facebook och google råkat ut för såna här där de måste ta ut information om någon. Så vi får se var det slutar helt enkelt. Jag tror att det är i sin linda allt det här som vi vill ha men som vi inte riktigt förstår vad det kan användas till det är väl det.	
73	Interviewer	Det är ju ändå en tydligt mer bet. Det är det man läser om på hemsidor, varning varning vi kan ta 4% av omsättningen. Men det finns ju lite såhär olika tekniker som rekommenderas av lagen som inte är lagstadgat men de säger de här kan vara en lösning för att skydda persondata och gör man det tillräckligt väl faller det inte under lagen då blir det anonymiserat. Då är pseudonymersing en del, använder ni er av det? kommer ni använda er av det?	
74	Interviewee	Alla sådana här frågor kommer vi diskutera med våra leverantörer. Jag vet att de håller på att titta på massa olika teknik allt ifrån de till hur man ska kunna screena t.ex. email så det inte förekommer personnummer och allt sånt. SÅ det är jättemycket sånt och det här är också en annan sak som inte har med personuppgiftslagen att göra men som relaterar till den också är sån här screenscraping t.ex. om du använder tink då ger du ju dom godkänt att använda ditt bankID för att logga på alla dina system. det är ju en ID-handling det är som att du skulle ge mig ditt körkort och säga amen använd du det. Jag tror inte det är helt lagligt och det håller ju också de här leverantörerna på att titta på. Hur ska man stoppa screenscraping och det är också en fråga sen, vill du att vi ska stoppa det eller inte egentligen? Och det är också frågan det är egentligen folk medvetna om vad man gör? så det jobbar med leverantörerna också med och vi har inte landat alla de här frågorna så jag vet inte riktigt vilka metoder man kommer använda.	Pseudonymous Data Encryption of Data

75	Interviewer	Så det är egentligen samma sak med kryptering?	
76	Interviewee	Ja precis, de har dom redan på mycket, i bank är det otroligt många säkra system som går, där du har säkra tunnlar som du kommunicerar via, du får ju inte lägga ut saker hur som helst. I en molntjänst t.ex. allt är ju redan bakom lås och bom.	Privacy by Design and Default
77	Interviewer	Men det är för att inom bankvärlden finns det här ramverken som är väldigt tydliga om hur kommunikation får se ut och såhär och det gör kanske att det är enklare för er?	
78	Interviewee	Ja absolut eftersom det redan är innanför lås och bom liksom.	Encryption of Data
79	Interviewer	Jag antar att det redan finns lite idéer kring detta men, om det sker personuppgifts incidenter, en breach av persondata, hur hanterar ni detta? Hur kommer ni hantera detta? Alltså informera myndigheter och personer.	
80	Interviewee	Ja det får vi titta på, alla dessa rutiner. Men vi har ju redan idag, incidenter generellt som är av viktig karaktär får ju vi utav våra leverantörer och är det riktigt kritiska så måste vi ju rapportera de till finansinspektionen så vi har redan många rutiner på plats redan men sen gäller det att vi tittar på hur vi får in personuppgifter. Men oftast är det mer intrångsförsök eller andra incidenter. En incident för oss kan vara att våra betalkort, våra självbetjänings kanaler eller internetbank inte är tillgängliga under en längre tid. det kan räknas som en incident för att vi inte kan ge våra kunder möjlighet att fortsätta ett vanligt liv.	Breaches of Data
81	Interviewer	Så det finns redan på plats?	
82	Interviewee	Ja mycket finns redan på plats men vi måste bara anpassa det till om det blir en incident kring personuppgifter.	Breaches of Data
83	Interviewer	Skulle du säga att det mesta ligger i linje, alltså era dataprocesser redan ligger i linje med vad GDPR kräver och att man liksom får justera dom litegrann tweaks dom litegrann lägga på ett litet moment för att få dom att funka eller är det vissa saker saker måste man göra om helt och hållet?	
84	Interviewee	Visa saker måste man nog göra om helt och hållet det är bara det att jag inte har den detaljkunskaper för tillfället. Men just det här med säkerhetsbiten där är vi ganska hemma redan men det är säkert vissa bitar hur vi använder data och sådär vi måste göra om processerna helt och var vi skriver vad och sådär.	Breaches of Data
85	Interviewer	Vi har redan varit inne lite på det men privacy by design, ja precis, ni ligger väl lite i linje med det hur man skapar sina processer och vilket tänk som finns	

		där från början. SÅ jag tänker att från och med nu kommer väl alla nya data processer ni gör att ha det här GDPR tänket inbyggt från början, det är inget man lägger på efter ni kommer skapa processer som stämmer från början?	
86	Interviewee	Ja precis.	
87	Interviewer	Du svarade lite på det innan men säkerhetsbiten där det gäller kryptering och sådär där är ni hemma och där har tänket funnit från början men det är mer uppgiftsminimeringen när och var man hanterar persondatan.	
88	Interviewee	Ja det är stor del men sen måste vi också kolla med leverantör det här med gallring och hur tankar vi ur data om någon vill få tag på det. Där har vi det inte på det klara med och sen också den juridiska delen på det då alltså att det är tydligt mot våra kunder och anställda men framförallt kunder då, vad är det vi använder datan till hur arkiverar vi den osv. så det blir ju en del i alla avtal och sånt som vi måste få granskat.	Storage Limitation and Data Minimisation
89	Interviewer	Vilken del tycker du är viktigast eller svårast? Helt enkelt den viktigaste biten.	
90	Interviewee	Jag tror, att få ut all data kommer bli tuff. Om någon kommer och säger att den vill få ut all data om sig själv. Sen så är det nog att få alla att förstå vad får man och vad får man inte göra och varför det är viktigt.	Right of Access, Right to be forgotten and the right to Data Portability
91	Interviewer	Så det är snarare organisatoriskt än tekniskt? Den tekniska biten det löser man?	
92	Interviewee	Ja det tror jag, den tekniska biten att få ut uppgifter kommer bli en utmaning. Att liksom persondata finns på så många ställen, det beror ju på om du har konton, om du har lån, om du har fonder allt finns ju inte i ett bautasystem utan det ligger på olika ställen. Så det är ett att få ut den information att få ut den information vi har lagrat om dig. Sen så är det ju de andra att få folk att förstå, vad får jag och vad får jag inte göra.	Right of Access, Right to be forgotten and the right to Data Portability
93	Interviewer	Kommer ni ha några workshops och liknande?	
94	Interviewee	Absolut, redan nu har vi. Han som är informationssäkerhetsansvarig hos oss åker runt till alla, det här kommer komma vi kommer behöva göra ett jättestort jobb, sluta redan nu att göra så här. SÅ redan nu har det börjat göras att förbereda alla mentalt.	
95	Interviewer	Är det branschöverskridande, att man försöker kolla på det för er bransch. För att på något sätt komma som en enad front det kanske blir lite lättare att försvara ett visst sätt hur man hanterar?	

96	Interviewee	Det finns ju bankföreningen och andra organisationer. Det finns forum som pratar om just det här. Så finns det för alla lagar vi måste förhålla oss till. Hur förhåller vi oss till det här och man kan utbyta lite erfarenheter och de sätter upp riktlinjer, så här tänker vi i alla fall att man bör hantera och de här lagarna övertrumfar de här. Så det utbytet har man ju men sen hur vi väljer att implementera det är upp till oss i slutändan och det är bara vi som kommunicerar med våra. Sen kan det vara t.ex. vid sedelbytet eller penningtvätt går bankföreningen ut med visa såna här broschyrer och information till allmänheten det kan riksbanken också göra för att visa nu händer det här och att man stödjer bankerna, att de står bakom bankerna i det här. Det är mycket att det kommer ut sånt men då kommer det mer från dom så informerar man på olika sätt till allmänheten.	
97	Interviewer	Det var nog allt, stort tack!!	

Appendix 6: Eric

Paragraph	Person Speaking	Text	Coding Reference
1	Interviewer	Din roll i organisationen vad gör du för något?	
2	Interviewee	Jag jobbar med utvecklingen av våra produktionssystem och det är ju det mesta då som vi håller på med, digitalt och print. Och har en grupp som då jobbar med utvecklingen, det är webbutvecklare och andra roller för att vi ska kunna göra nya bra saker. Och det är allt från backend delarna då t.ex. integration mot kunddatabas, och sen är det också det man ser via våra webbsidor. Den presentationen man ser där.	
3	Interviewer	Så det är hela spannet eller vad man ska säga?	
4	Interviewee	Japp det är det.	
5	Interviewer	Hur skulle du beskriva en vanlig dag?	
6	Interviewee	Ja för mig, en vanlig dag består mycket av möten, olika företrädare, två olika delar av organisationen, ibland externt också. Vad vill vi ska hända i framtiden det är mycket där mitt fokus ligger. Vad gör vi om 12 månader och så. Det är mer där mitt fokus är egentligen. Sen ibland blir det väldigt konkret, något funkar inte som det ska, hur får vi det att funka. Det är allt mellan här och nu och var är vi om 3 år. Men mer ett framtidsfokus än dagligt fokus kan man säga.	
7	Interviewer	DÅ gissar jag att du har hand om processer, att ni diskuterar processer som har med personuppgifter att göra?	
8	Interviewee	Ja, det gör vi men den diskussionen i vårt fall är ganska tidig kan man säga.	
9	Interviewer	om vi går in lite mer specifikt på lagen, på GDPR? Så har vi ju samtycke, samtyckes biten kommer ändras, det kommer vara lite såhär informerat samtycke, det krävs lite mer för att faktiskt få samla uppgifter, kommer det ändras något för er? har ni varit tvungna att kolla på processer?	
10	Interviewee	Ja, det kommer ju ändra hur vi kommunicerar med våra kunder i allmänhet och i synerhet dp med våra nya kunder, dom som blir kunder. Vid själva övergången, nu vet jag inte, nu gissar jag lite, vi övergången nu gäller GDPR, då måste vi infomera våra	Consent

		kunder, nu är det nya avtal och dom ser ut såhär. Och sen knaske man som kund då bekräfta på flera punkter att man godkänner avtalet, så tror jag det blir. Det är avtal som måste godkännas, i synnerhet för dom som blir kunder efter 25 maj men även de som är befintliga kunder, ska ju bekräfta sitt godkännande.	
11	Interviewer	Ni har inte tittat på specifika saker på en hemsida som att, nu måste vi ändra den här så att man inte bara kan trycka ok utan att man kanske får mer information, ni har inte tittat på specifika grejer eller?	
12	Interviewee	Nä det har vi inte gjort än, men vi tror att vi måste t.ex. lite mer så här som apple eller Facebook, nu blir du kund, nu ser du avtalet och du måste godkänna det, och du måste kanske godkänna flera punkter i det var för sig, mer så. Så tänker jag mig, men det är lite mer av en personlig reflektion. Vi har faktiskt startmöte om det här den 7e juni. Just nu håller jag och någon till att formulera det här frågorna, vad tror vi att vi måste göra. Vi har väl känt oss ganska trygga eftersom vi är hemmastadda i PUL osv. Mycket som gäller den personliga integriteten och möjligheter att få ut uppgifter och så de har vi ju redan idag. Det blir mer kring det här, hur man kommunicerar med kunden att klargöra detta. Men vi kommer säkerligen behöva göra om, ha en bättre sida där avtalen finns så man kan komma åt dom. Och att man kanske ska kunna komma åt dom från sin kundbild, det vi kallar då nu går jag in på min sida här och nu ser jag mina uppgifter och jag kan redigera dom jag kan byta adress telefonnummer allt det här. Och att där finns då mitt avtal, alltid tillgängligt. Och där tror jag också där ska ju finnas en liten funktion som gör att man kan få ut sina uppgifter så att det blir både läsbart och möjligt att skicka vidare om nu kunden eller någon skulle vilja det.	Consent
13	Interviewer	Precis, man har ju den här rätten till dataportabilitet, ändras det någonting där, är det något specifikt där , vi måste se över, mappa om databaser, ibland kan det vara att man inte har tillräckligt indexerar, är det aktuellt för er?	
14	Interviewee	Det tror jag inte, i alla fall inte i någon stor utsträckning. Vi har en bra kunddatabas, där alla uppgifter finns väl strukturerade och så. Det är mer det här tillgängliga, om en kund hör av sig och vill ha ut all sin historik, jag vill ha alla uppgifter om mig, då kan dom få det. Men det är inte lika, man måste ringa idag och be om det, jag tror mer på det här att som kund ska det vara väldigt lätt att man som kund bara klickar någonstans och kanske med sitt lösenord kopplar loss sina uppgifter, eller kanske någon tvåstegsverifiering, men ändå att man väldigt enkelt på egen hand ska kunna få ut sina uppgifter.	The Right of Access, the Right to be Forgotten and the Right to Data Portability
15	Interviewer	Så sparar man också det att man slipper ta ett samtal, att man kan göra det själv liksom?	

16	Interviewee	Ja jag tror det självbetjäning är alltid bra, det gäller bara att kunna göra det säkert. Så att om vi säger att någon råkar komma över någons lösenord, det ska va lite svårare så någon slags tvåstegsverifiering. Det räcker inte med bara lösenordet man behöver även ha personens mobiltelefon eller något.	
17	Interviewer	Det finns ju även uppgift minimering, tidigare har man kunnat samla ganska mycket data utan att behöva reflektera över det, nu måste man strömlinjeforma nu tar vi bara den här datan för det är faktiskt det syftet vi har med insamling. Kommer ni få ändra något där?	
18	Interviewee	Det kommer vi säkert, men det är en sån här fråga som vi har och jag tror vi kommer få jobba med framöver, det är ju eftersom vi nu har digitala kunder numera, som loggar in, när man är inloggad har vi ju möjlighet att följa väldigt nära vad folk gör. Nu sparar vi inte den datan i en kunddatabas eller så men man skulle ju kunna tycka att det är värdefullt, vi följer x och vad han läser för något hela tiden. Då hade du kunnat höra av dig till oss, jag vill veta vad jag läst den senaste månaden. Då kan du få det av oss för det har vi sparat. Och då är frågan, hur långt sträcker sig det här, omfattas det här. Men vi sparar ju data, vi kan ju se vad ett specifikt ID-nummer läser, den datan är idag inte sammankopplad med en namngiven kund, de hålls isär.	Pseudonymised Data
19	Interviewer	Ni har alltså anonymiserat? Så man kan inte koppla det rakt av till? alright	
20	Interviewee	Nä, men när vi vill skulle vi kunna koppla ihop det.	Pseudonymised Data
21	Interviewer	Okej det finns information så man kan göra det men i samma stund som man tittar på ett ID-nummer så finns det inte en tydlig koppling till?	
22	Interviewee	Nä vi har inte tyckt att det är någon större poäng att koppla ihop dom, vi är inte så betjänta av att veta vad du läser, däremot är det viktigt för din upplevelse att webbsidan presenterar innehåll som är intressant för dig. men det behöver inte vi veta egentligen.	Pseudonymised Data
23	Interviewer	Man kan göra den processen anonym egentligen?	
24	Interviewee	Aa men det är en gråzon kan man säga, det kan ju va så att vi kommer på att vi vill veta vad en namngiven person läser, vi vill veta vilka annonser dom klickar på, vi vill veta om det köpt privatannonser eller inte och i så fall vad ville de sälj. Allt det där kan vi vilja veta och då tänker jag mig att allt det där omfattas av	

		den här lagstiftningen och då måste vi samla den datan också så att den är tillgänglig. Det är lite oklart för oss kan man säga, beroende på hur mycket information vi tycker är värdefullt att samla på oss, så blir ju, ju mer vi tycker är värdefullt att samla desto mer omfattande blir också arbetet.	
25	Interviewer	Är det många processer, det här ligger mer i framtiden om man ska samla det eller inte, men om man tittar på de processer som man har idag. Kommer man ändra något där och göra dom mer, amen vi behöver inte samla namnuppgifter på det här, det har vi gjort alltid men nu får vi kanske sluta med det det är onödigt, det blir bara mer lagar att förhålla sig till. Eller?	
26	Interviewee	Jag tror det blir mer tvärtom. Vi kommer samla mer information och i med det kommer tuffare krav på oss, när det gäller hur vi samlar information, hur vi säkerställer integriteten för folk, hur vi tillgängliggör den, allt det där. Behöver tänka mer på än vi gör idag. Data blir en allt viktigare del av den affär vi har. Mittmedia som har tidningar i mellersta och norra sverige dom labbar ju helt med personaliserade webbsidor, de har valt ut 1200 personer i dalarna som när de loggar in får startsidor som i ganska stor utsträckning är anpassade av den enskildes läsvanor. De testar om de får större djup i besöken, om folk blir mer lojala i sitt beteende om man får en personaliserad upplevelse. Det är inte otänkbart att det blir så och då lär de ju finnas i vår framtid också. Att man gör mer personaliserade upplevelser, och det ställer ju i sin tur ännu hårdare krav på datainsamling, eller vi kommer behöva ha mer datainsamling och därmed kommer kraven på oss gällande lagstiftningen.	
27	Interviewer	Det blir ändå så att man skapar nya dataflöden så att man kan designa dom i grunden på rätt sätt? Det är inte så mycket en fråga att gå tillbaka och titta på befintliga processer? Här får vi göra om här får vi lägga till eller så här för att det ska synkas.	
28	Interviewee	Ja det enda jag tror är, hur tillgängliggör vi datan och hur är vi tydliga med vad folk kommer få. Där tror jag att vi kommer behöva göra om utifrån vad vi har idag. Sen tillkommer det ju, det som tillkommer är ju nya behov hos oss, och med tanke på att vi jobbar mer och mer med användardata, vilka krav ställs då?	
29	Interviewer	Du pratar om rätten att bli bortglömd t.ex. Är det de du tänker där, att man ska?	
30	Interviewee	Det kan man ju, problemet för oss och den enskilde är att vi bygger ganska mycket av användarupplevelsen på att vi kommer ihåg dig. Dels är det här med att du ska kunna vara inloggad hela tiden och så här men vi sätter ju en cookie för att vi ska veta att det är du som kommer och såhär, om man inte tillåter det	Storage Limitations and Data Minimisation

		då blir ju användarupplevelsen mycket sämre. Man måste logga in varje gång. De delar av hemsidan som är personaliserade är inte det längre, då. Det kan bli en ganska full upplevelse, siten funkar inte riktigt som den ska om man inte använder cookies. Så det är ju dels det och sen såklart att bli helt borttagen, kunder som inte är kunder till oss längre, de rensas ju.	
31	Interviewer	Det har ni? Så att man kan ta bort en specifik? det är inga problem?	
32	Interviewee	Ja, det sker automatiskt, nu kommer jag inte ihåg exakt tiden men det sker 6 eller 12 månader efter att en kund inte är kund längre. Då måste vi så att säga för att uppfylla PUL. Under tiden då, om man har haft ett avtal med oss, så kan vi ju fortsätta efter att avtalet gått ut bearbeta kunden för att förlänga. men det kan man ju bara under en viss tid 6 eller 12 månader. Och efter de där månaderna så måste vi ta bort uppgifterna.	Storage Limitations and Data Minimisation
33	Interviewer	Då fanns det här redan i systemet. Som det funkar har det funnits det här är ingen teknisk utmaning så att säga?	
34	Interviewee	Nejnej det är ju jättelätt det är ju bara datum det där, den räknar dagar och sekunder från det att avtalet to slut och sen tickar den fram till 12 månader och på sekunden så försvinner du ur databasen.	
35	Interviewer	För det är ju andra som har upplevt att det är möjligt att få ut persondata ur ett av sina system men sen så kan man ha flera olika och man kan ha utspritt och det kan vara svårt att veta var all data ligger någonstans, har ni några problem med det? Att det kan vara många olika system och få en bild av var datan skulle kunna finnas och att det kan vara ett problem?	
36	Interviewee	Nä inte som det funkar nu i alla fall. Vi har en kunddatabas där personuppgifter finns. Den har vi bara på ett ställe sen har vi ju ett betallager eler vad man ska kalla det. Ett inlogg som betallager och där sker ju en viss autentisering baserad på id-nummer och där finns ju egentligen inga personuppgifter. Där vi har statistik alltså analytics systemet är också ID så jag tror inte det riktigt uppfyller kravet för.	Transparency and Documentation
37	Interviewer	Så ni använder er av, när ni ska skicka information emellan använder ni er då av det här anonymiserade datat?	
38	Interviewee	Ja, i det ena systemet som sköter autentisering och inloggning där är det ett ID-nummer som egentligen i realtid inte kommunicerar med kunddatabasen. Så att där sker mer läsningar med jämna mellanrum. Nä jag tror inte att det är så känsligt. Men det är ju en fråga vi måste ställa i vårt arbete, vad betyder det här? Det kan ju också landa i, amen vi vill nog koppla ihop det här och då måste vi isåfall tillgäng-	Pseudonymised Data

		lig göra det. Men en sak vi inte kommer ha, det är jag nästan 99% säker på, är ny betal information, vi kommer inte hantera kortnummer etc. den typen av information har vi inte hos oss det låter vi då PayEx eller motsvarande sköta.	
39	Interviewer	Det blir lite mer det här att man går igenom sina processer och sen överväger man, är det verkligen värt att hålla på den här informationen?	
40	Interviewee	Ja, men så är det ju. Och vi har ju ett tufft arbete framför oss här nu under hösten, vintern och våren det är jag säker på, om vi gör det här på ett sätt som uppfattas positivt av kunden, att det uppfattas som att det görs för kundens skull, det blir bättre för dig som kund för vi är tillgängliga till dig att du får ta del vad vi vet om dig, att vi också i det sammanhanget kan på något sätt erbjuda på något sätt en bättre användarupplevelse, jo men vi sparar den här datan för att du ska få en bättre användarupplevelse. så det är ju inte bara jobb, oj nu måste vi uppfylla vad en lagstiftare har hittat på utan det är också hur kan vi använda den här nya lagstiftningen som gör att vi blir bättre.	Storage Limitations and Data Minimisation
41	Interviewer	Det är många som har upplevt det så att det är ett jobbigt år framöver när man ska anpassa sig men det är på något sätt skönt att man ska komma tillrätta med många av de här processerna man kanske inte tittat på. Man får en ursäkt att nu måste vi göra det här för annars kan vi få böter?	
42	Interviewee	Så är det ju, ja. Där är det så vi har jobbat i några olika generationer sen 2009 har vi jobbat med kunddata på det här sättet som vi gör nu. Och på ett sätt så är det lite så att under de här 6-7 åren som har gått så har det blivit lite av ett lapptäcke och vi har ju det senate året i en helt annan synvinkel snackat om att vi behöver få ett mer strukturerat data så vi inser ju behovet själva att vi behöver mer strukturerad data men här är ju ytterligare ett skäl, gott skäl till att göra det då. Nu kan vi ta tag i det här, göra det, också på ett sätt så att det funkar för oss inte bara för att följa en lagstiftning. Hur kan det här bli till nytta för oss och vår kund. Den approachen ska vi försöka ha.	Transparency and Documentation
43	Interviewer	Tror du man fått upp det på bordet, är det förmält för att straffen har blivit högre?	
44	Interviewee	Äeeh, det känns nästan som skrönor x% av omsättning och sådär. Om man läser lite ser man ju att det beror på, det finns en avvägning mot den skada som sker och sådär eller som kan tänkas ske. Men det är klart att det, det är lite skrämmande om man skulle behöva betala 2-3% av sin omsättning, det blir rätt mycket pengar men jag tycker väl ändå inte så orolig när det gäller det, jag ser det mer som ett skäl för att göra något bra. Vi ska inte göra det för att vi är tvungna, eller det gör vi också såklart, men vi ska	Penalties

		göra det för att det ska bli bra.Inte för att vi är rädda för att få straff.	
45	Interviewer	Har ni data, det blir ju lite nya regler, man får ju lagra data utanför EU men det kan bli lite kladdigare, har ni data utanför EU?	
46	Interviewee	inte idag, men vi använder ju, det innehåll vi publicerar på våra webbar, det finns på amazon. Alltså artiklarna. Och just nu finns de i ett datacenter på irland och det är inom EU, och backupen är i frankfurt och det är inom EU men skulle båda dom där dö, tredje steget där det är ju USA, och då är man plötsligt utanför EU, nu är det jäkligt osannolikt att både irland och frankfurt ska gå ner och att vi då ska vara beroende av USA för att visa upp innehållet. Men det är som sagt bara innehåll, där finns ingen kunddata, kunddatan finns i Sverige.	Territorial Scope
47	Interviewer	Har ni, kommer ni anställa någon specifik DPO? I GDPR står det ju om en specifik person som ansvarar för datan egentligen.	
48	Interviewee	mm vi behöver veta mer om vilka krav som ställs på den funktionen, vad ska de va för slags person, vilka kvalifikationer vilken kompetenser ska den ha. Det tror jag vi behöver veta mer om.	Data Privacy Officer
49	Interviewer	Alltså om man ska gå mer åt ett juridiskt håll eller om man ska gå mer åt ett tekniskt håll eller sådär?	
50	Interviewee	Ja precis, eller nån kombo där i emellan..	
51	Interviewer	Kanske svårt att få tag på en jurist som är kunnig inom ?	
52	Interviewee	Aaeh det finns säkert lite IT-jursiter. Det är väl inte otänkbart.	
53	Interviewer	Tror ni att ni kommer landa, det finns ju krav ibland på att man måste ha men inte alltid, är det nödvändigt , att det kommer finnas en fördel med att ha någon som står som ansvarig för datahantering?	
54	Interviewee	Ja det tror jag, jag tror det skulle vara väldigt bra att ha en mycket kompetent person i en sådan roll, för jag tror att persondata kommer vara fortsatt viktigt och kommer kanske vara viktigare för oss i framtiden och då har någon som hela tiden ser till att vi gör rätt och uppfyller lagar och så tror jag är viktigt för oss men nu är det jag som tror det, vi vet inte än. Men det är en sån fråga vi ska ha upp på bordet då när vi ses i början av juni om just vilka krav som ställs på en sådan roll för det kan ju vara så att den typen av kvalifikationer är något som vi idag inte har. Vi har ju folk som jobbar med personuppgifter, det är ju dom som är ansvariga för vår persondatabas och dom hamnar ju ibland i lägen där de måste fråga	Data Privacy Officer

		jurister, men då har vi externa jurister som vi konsulterar. Men det här kanske betyder att vi måste ha mer egen kompetens för det sker ett mer löpande arbete.	
55	Interviewer	kommer ni få jobba mer med dokumentation av era processer och att man ska logga allt som händer och som gör att man kan dra ut och kolla vad hände på den här dagen och den här tidpunkten?	
56	Interviewee	Ja det gör det idag med. Vi har ju loggar på det mesta egentligen, som händer och har vi inte det kan vi begära ut det. VI jobbar ju ibland med leverantörer som driftar våra system och så. Dom loggar ju också det är avtal vi har med dom, att de ska kunna gå tillbaka och se om det sker t.ex. en incident då måste man kunna se varför det, så där har vi ganska bra rutiner för tycker jag.	
57	Interviewer	Det finns alltså implementerat idag en dokumentation över processer osv.?	
58	Interviewee	Ja det gör det	Transparency and Documentation
59	Interviewer	Sen har vi det här med pseudonymisering av data, det var vi inne på innan med ID. att ni på något sätt kopplar det mot ID. Krypterar ni data någonting?	
60	Interviewee	Aa, det gör vi. Just den här betalinfomrationen skickas ju krypterat. Och inloggningsuppgifter när man, vi kommunicerar med inloggningssystemet till kunddatabasen sker det krypterat. Samtidigt så säger vi att vi är ingen bank man behöver inte ha ett mobilt bankID för att logga in på en tidningssida. Och det är inte hela världen om någon annan använder, om du skulle använda mitt inlogg för att komma åt ystad allehanda, det gör ju egentligen ingenting.	Encryption of Data
61	Interviewer	Det finns inte så mycket man kan som förstör?	
62	Interviewee	Nä det gör inte det, det är inte den typen av inlogg där man kan orsaka skada det är inte. Så man måste få det här med säkerhet och sånt. Det ska alltid avvägas mot användarvänlighet, för den enskilda användaren ska det vara enkelt att komma åt det man ska komma åt. Men man vill ju inte heller att lösenord och så, ändå det är någonstans hel och ren fråga att man inte kommunicerar lösenord och andra uppgifter i klartext.	
63	Interviewer	När det kommer till personuppgifter och personuppgiftsincidenter? Då ska man rapportera ut när det hänt relativt snabbt, kommer ni få se över processer där?	
64	Interviewee	Ja det måste vi ju, för att se hur sker det och vad betyder snabbt, 72 timmar tror jag? och vad är det då	Breaches of Data

		man rapporterar och såhär. Där måste vi ju hitta våra rutiner för, det är ju såhär att det finns frågetecken där för vad är det vi måste göra där egentligen, vilka uppgifter är det som försklaras i sådana fall. Det vet vi inte riktigt än, det måste vi reda ut.	
65	Interviewer	Tror du det blir svårt att implementera in det i de processer ni har idag eller kommer det vara relativt lätt?	
66	Interviewee	Jag tror det blir lätt, asså för den enskilda kommer det ju, vi har ju e-post system som egentligen gör att när vi vill kan vi skicka e-post till våra användare och det kan vi ju, det är ett bra sätt där vi kan ta en matlap, nu har det skett ett data intrång här, det har vi kunnat kommunicera t.ex. Sen har vi, vi kan ju kommunicera via våra hemsidor med, tala om för våra kunder som en nyhet, det har skett ett datain-trång och på det sättet har vi många vägar att kom-municera. Det är ju mer kanske den formella nu ska vi tala om för datainspektionen vad som har hänt vad behöver de veta då? Det vet inte vi än, exakt vad det behöver veta, och hur vill de ha den information isåfall.	Breaches of Data
67	Interviewer	Men det finns möjlighet att liksom, med de befint-liga processerna som ni har så kan man relativt en-kelt hämta ut den informationen sen gäller det bara att vet vad det är man ska hämta.	
68	Interviewee	Ja precis.	
69	Interviewer	Så du tror inte det kommer vara ett större problem alltså?	
70	Interviewee	Nä bara vi vet vad man ska göra så gör vi det. Det är inte så mycket att be för, det är lagen, vi bara måste lösa det. Det är inte en sån här blocker, det fixar vi.	
71	Interviewer	Tror du det kommer handla mer om ett organisato-riskt problem alltså individen på, era anställda hante-rar data snarare än koden?	
72	Interviewee	Vi är rätt noga idag när det gäller kundhanteringen. Eftersom vi skulle prata här nu frågade jag kundcen-ter chefen, hur gör ni nu? Nu ringer x och är sur för att han inte fått tidningen för fjärde dagen i rad, skriver man då själva surgubbe i kundbilden där? Man har ju liksom en bild framför sig där det står vem jag är , var jag bor och hur länge jag prenume-rerat och allt det där. Sen finns det olika fält där man kan fylla i uppgifter och där kan man ju skriva vad man vill ”nu har surgubben inte fått sin tidning igen” men det är väldigt noga, man skriver inte så. Man använder ju koder för utebliven tidning etc. Nu har han fyra tidningar tillgodo sådär. Det är väldigt noga vad man skriver. Så jag känner mig rätt lugn när det gäller kundcenter. Däremot en sak som jag funderat på, det är mer den redaktionella delen av vår verk-	

		samhet, för på redaktionerna jobbar man ju mer och mer med databasjournalistik säg t.ex. nu gör vi en granskning av fällande domar i kalmarlän och så matar vi in en massa uppgifter, vi får en massa uppgifter och sen matar vi in dom som databas material sen börjar man sortera på det där, man börjar sortera på var folk bor och hur gamla dom är och vad de fick för straff oc etnicitet och vad det är för brott och allt det där kan man börja jobba med och det kan ju faktiskt vara så att man tycker det finns ett värde att ha med personnummer och namn på de här personerna hur omfattas det i sådana fall. Idag tror jag nog, att på redaktionerna, sånt gör man idag bara, man skickar in en massa uppgifter i excelark och så sorterar man och så försöker man bedöma om det är någon nyhet eller inte. Det där excelarken kan ju liggas på någons hårddisk och sne lånar någon den där datorn och där ligger det och skvalpar eller så nu ska datorn lämnas tillbaka för nu är leasing tiden över, oj vi glömde rensa den. Ja det är väldigt lätt att ett excelark, en excelfil kommer på vift.	
73	Interviewer	Så du tror snarare svårigheten, en svårighet är att få anställda att förstå hur man ska jobba med data?	
74	Interviewee	Aa och just i ett sånt fall om man gör en sån, om man tar databasjournalistik exemplet, är det att betrakta som, är det personuppgifter som ligger där helt enkelt? eller är det något annat? För en redaktion har ett annat skydd när det gäller uppgiftslämning och sådana saker, redaktionen har ju så att säga litegrann en särställning, grundlagsskydd och sådana här saker.	
75	Interviewer	Ja precis det finns ibland andra lagar som står emot.	
76	Interviewee	Ja och det hade kunnat betyda att, det vore jättekonstigt om, redaktionen har gjort en granskning här och så visar det sig att hela granskning måste göras tillgänglig för enskilda. OM vi tar krimexemplet t.ex. hörredu jag har ett nytt möte nu vid 10!	
77	Interviewer	Japp tack så jättemycket!	

Appendix 7: Fred

Paragraph	Person Speaking	Text	Coding Reference
1	Interviewer	If you could describe what position what you are doing,?	
2	Interviewee	So i am working for a consultancy firm where we are dealing with, working with GDPR towards different clients, because i noticed that a lot of these questions on different GDPR topics are related to implementing it in ”my” organization, but to make that clear i am not part of any GDPR implementing activities in this firm, we are helping other firms to become more mature in GDPR processes, if that makes sense.	
3	Interviewer	So you have a more abstract view of the law or?	
4	Interviewee	Yeah so we are basically supporting our clients in implementing the GDPR, but even before that we are making maturity assessments and GAP analysis towards the requirements.	
5	Interviewer	Do you work with any of these questions that we have in this form like consent, do you touch any specific parts of the law or are it always more of getting a better idea of how you could implement the law?	
6	Interviewee	We can go through the questions and i can see what i can answer, see what is relevant and what not.	
7	Interviewer	So just to start with the first question what position do you have in the company?	
8	Interviewee	I’m a senior consultant at a firm.	
9	Interviewer	How long have i been at this position?	
10	Interviewee	For 4 years now.	
11	Interviewer	Whats a regular day for you like?	
12	Interviewee	I’m having a lot of different clients, i reach out in context of GDPR only to one at the moment, i help the client to improve their privacy and GDPR and related process.	

13	Interviewer	If we only speak GDPR , then consent will propose specific consent and informed consent affect your work?	
14	Interviewee	I can't really answer that, do i have to look it through my firm's perspective or towards my client?	
15	Interviewer	I mean if you have any general ideas how companies go about and see this as an issue or not.	
16	Interviewee	Okey actually let me talk maybe not focus that much on the question and talk around the topic that will give you the most valuable information. So what we see at clients at the moment is that you need to record consent for all purposes of data collection. Indeed a lot of organization sees this as a real issue as they don't always know whether they do that right now. And that organization are trying to map that right now and we try to help them with that. For example a lot of clients are big big banks that have thousands and thousands of application and then you would need to know for each application if the consent is recorded for all the purposes of the data collection so it is very big and complex topic in all senses. For that reasons hat most organizations are trying to do is to move away from consent as such and base their data collection on other legal grounds. If that makes sense. You probably have background on GDPR since you are writing your thesis , so i dont need to go much in detail about the legal grounds. But indeed like consent, consent is something difficult especially if you are dealing with customer personal data and in particular for employee data there should not be consent because there are contractual basis. I think that is a way that organizations will handle consent, they will move away from consent and deal with it in other legal grounds.	Consent
17	Interviewer	Rather than making the information that you handle anonymized or pseudonymised you try to have another legal ground for collecting the data.	
18	Interviewee	Exactly let me just give you some examples, so i think you have other legal grounds e.g. the necessary for the performance of a contract that will be the case in particular for employee data, but i guess it depends in the way you interpret it. It can also be the contract between the customer or the client and the organization but it can also be legal obligations that can be another legal ground. It can be to protect the vital interest of the data subject, it can be to perform tasks in the public interest, necessary to riskful … between data controllers business interest and privacy of the data subject so there is a lot of these that come straight from the GDPR. So it is possible i know a lot who are trying to move away from consent otherwise you would need to have consent on all the purposes of the collection and that	Consent

		makes it a very cumbersome exercise.	
19	Interviewer	Alright, so it is rather to move away from the law, like avoiding rather than complying with it?	
20	Interviewee	No, i don't think so it is not really moving away, consent is just a way of having the data subject history with you processing the personal data i mean it have other legal grounds so it is more about making things easier, and not making things over-complicated.	
21	Interviewer	In some way switching approach how to collect data? it is still a matter that companies will have to look into.	
22	Interviewee	Yeah, no definitely i think all the companies will look into how do you get consent and how do you approach this in the context of the gdpr now we are only looking at customer data as this is usually the most content. The employee data is always covered by the contract which the employee have with the organization.	
23	Interviewer	Do you think for data minimization as well? not having more data than necessary at each process.	
24	Interviewee	Of course, data minimization its, its related, but companies need to make sure that they only borrow the personal data that they should that they need to fulfill the purpose of the collection, not more. They have to make sure that they look at data minimization in that perspective.	Storage Limitation and Data Minimisation
25	Interviewer	Do you think that will be technically hard to achieve?	
26	Interviewee	Well data minimization as such, maybe not, i think that is more of a matter of scoping rich data you wish to collect i think it will be very difficult, and of course that is not super specific in the legislation,that you actually completely anonymize the data, i think that will be very tricky because you can encrypt the data you can pseudonyms data but it is not because you pseudonyms the data or anonymize that necessary it wont be considered anymore personal data. There some explanation in the GDPR, only if it is completely anonymized and there are no ways of decrypting or being able to link it back and then identify an individual if there is no way of doing that then, Yes, then it is not even considered personal data anymore. So that is really tricky especially for organizations that have thousands and thousands of applications.	Storage Limitation and Data Minimisation
27	Interviewer	So would you say that this is technical landscape that makes it difficult to achieve compliance?	

28	Interviewee	Absolutely, i think that is probably the most, and that is why it makes this entire exercise difficult and that is also why a lot of companies use all these consultancy firms to support them in that.	
29	Interviewer	Do you think it is both, I'm guessing, distributed technologies but legacy systems as well? A lot of legacy systems that need to be mapped for instance is that a concern as well?	
30	Interviewee	Yeah exactly, you map the databases but, cause the requirement is to that you have some data inventory or some mapping and, were as a organization do you start? you start by mapping databases, the applications, the streams of data it's definitely a challenge i think probably the best way to kick of this kind of exercise is to use any existing, if any application register and then per application really confirm, whether it is personal data in which one and then for each application go through different, each GDPR requirement and find gaps where you don't have compliance for instance where information is not encrypted while transferring or where there are no functionality to delete data or export data for portability and so on.	
31	Interviewer	So you are saying you should start to somehow map up your entire system of technologies and applications and such and then you go in depth of this applications to see if the processes are compliant or not?	
32	Interviewee	Usually, first you have an assessment of the different GDPR topics. OR requirement. Then actually when you are trying to implement these you want to start mapping the entire IT landscape and really know where in the organization your personal information is, and customer data.	
33	Interviewer	So i guess this falls in line with the right of access the right to be forgotten and the right of data portability? all of these requirements are, you make this possible by mapping and systemizing your applications ?	
34	Interviewee	Yes exactly, so that is what we are doing for several clients, mapping different applications and for those applications finding out how mature they are in different areas of the GDPR	
35	Interviewer	Would you say it is a top down approach, you start from an almost abstract level and you work your way down to a more specific hands on processes?	
36	Interviewee	Ehm, well i think it's not, if you mention top down approach to me you are more looking at the business processes but i think that in a ideal world you would do that, and if a company is that mature that all their business processes are documented and where it is very supporting IT and applications and	Transparency and Documentation

		infrastructure that is behind those business processes all that is documented then definitely that would be a really good approach but i think in reality most companies have that inventory , or not even, those application registers with containing all their application, of course, and databases and that is more of the bottom up approach starting from all the applications containing personal data and i see that as more of a realistic way of seeing it the top down.	
37	Interviewer	when it comes to, the territorial scope, is it a lot of clients that have information or data outside of the european union?	
38	Interviewee	Not, i mean no maybe, i cannot say, but yes it happens but the clients need to be kind of engaged in their doing and it is usually entities here in sweden and they usually have their data center here in sweden, so they usually have their data here in sweden or at least in the nordics.	Territorial Scope
39	Interviewer	So the idea here is to have it more or less in the european union?	
40	Interviewee	well i don't really think there is a goal to keep data in the european union, i don't think you have to see it like that, but i think that organizations try to map out which applications transfer EU citizens data to other countries which applications transfer gets information outside of EU which applications get data through a third party processing data or actually going back to if data is transferred outside EU, on which legal grounds are companies trying to map out. And if they are doing certain things which is needed to look at from a GDPR point of view and if they do they need to make sure that they are compliant and if there are gaps or they are not compliant then they will start to make sure that they are	Territorial Scope
41	Interviewer	When it comes to a DPO is that a matter of how big a company are or are most companies aiming to have one to have responsibility of their data processes.	
42	Interviewee	No that is really a requirement and it is easy to appoint someone so that is definitely all the companies or if they do not have one yet they are looking for it now basically.	
43	Interviewer	Personally do you think it is a good step to have more control over your processes?	
44	Interviewee	Yeah i think someone needs to be responsible for this and also i think the person that will have that role will also be someone that is very independent from the rest of the organization so i definitely think it is a good thing.	

45	Interviewer	Working as an accountant almost?	
46	Interviewee	yeah something like that.	
47	Interviewer	Do you think, will companies get an external one? hiring someone from an consultancy firm or something or will they get an internal one, although they are quite independent in their work?	
48	Interviewee	I think of course the purpose is to find DPOs in house, or hire new people maybe a temporary solution is to get some consultants but i think it varies depending on how quick they can find a dependent person.	Data Privacy Officer
49	Interviewer	Alright, then there is a lot about transparency and documentation in the GDPR, it more or less characterizes the law, a lot of the processes must be transparent and documented, is this a problem? If you handle data you should be able to report that you comply with the gdpr	
50	Interviewee	Do you mean like generating policies and guidelines?	
51	Interviewer	Yeah and more into detail how you handle specific data in certain context as i have understood it, maybe this could be a policy or guideline for how you handle.	
52	Interviewee	No, that is one of the most important streams with a project like that, everyone need to have policies and frameworks and guidelines and communications towards the business that is definitely important that data processes are documented and communicated to all the stakeholders within the organization.	Transparency and Documentation
53	Interviewer	But, do you think this has been done before did you have some sort of an idea on privacy by design, was this to some extent implemented before or is this completely new?	
54	Interviewee	No i think in most cases privacy by default and privacy by design that its quite new for most organizations.	
55	Interviewer	So legacy systems will have to be redesigned or do you think they will be completely new?	
56	Interviewee	That is a good point, no i think the purpose of privacy by design and privacy by default are more focused towards new systems. Legacy systems i mean you cannot, it is impossible if you are dealing with thousands and thousands of applications to all of them implement privacy by default and privacy by design i think the approach more is to make sure that the data, the personal data you are processing is	Storage Limitation and Data Minimisation Privacy by Design and Default

		protected that you have processes around protection so it can be encryption it can be anonymisation so you have to have those mitigating configurations instead.	
57	Interviewer	So it is more, compliance by design is something for the future and then you just try to make your processes compliant with the GDPR in what ways are possible in the moment?	
58	Interviewee	Yeah the privacy by design and default are new and will be used for new applications or changes to old applications. It will not be applied to legacy systems that would be very, very expensive.	
59	Interviewer	Do you think when it comes to funding and so with this projects do you think the penalties are the main reasons why companies have put money in this?	
60	Interviewee	Its hard to say like that, i would guess so yes, i mean isn't that in general? If you wouldn't have a penalty why would you spend a lot of money fixing something if there aren't a penalty so. but at the same time i feel like people see and we try to communicate that as well, and that is the advantages that GDPR brings by itself. So it is not just being compliant it creates transparency and really just protecting personal data and i think that is more and more going forward in these types of projects you see that people actually concerned with it as well and is not only focusing on the 4%.	Penalties
61	Interviewer	The companies actually see the added value that comes with being compliant with the GDPR?	
62	Interviewee	I think so, yeah definitely, in the end it is personal data and it concerns everyone right.	
63	Interviewer	Pseudonyms data and encrypted data, we went through it a little bit this is used as you described earlier to comply with the law. is it common? i mean encryption are quite usual right?	
64	Interviewee	Yeah definitely, yeah of course not all the application but it is common maybe not when data is in a database but at least it would be when the data is transferred.	Encryption of Data
65	Interviewer	So communication overall encrypted but databases not always?	
66	Interviewee	No i mean like e.g. when you open an application and have data in front of you you don't it is not encrypted you don't need a key to deencrypt too see it it is usually, the encryption is more important when you actually are sending the data outside of the organization or outside of the network.	

67	Interviewer	Like you explained you need a key to access certain applications do you think this will increase? With GDPR?	
68	Interviewee	Yes but i just think in general it is a trend, with all cyber related that is happening in the world. So i just think in general there is a trend to a more important information security processes.	
69	Interviewer	Do you think, what would be preferred, pseudonymous data or encrypted data? or would companies use both? To ensure the safety of data.	
70	Interviewee	I think it will be a combination of the two of them. Encryption should always be applied and pseudonymisation is quite new. But for my clients i think they should use a combination of both of those.	Pseudonymous Data
71	Interviewer	When it comes to breaches of data will this be a difficulty to implement how to report back and see how many users are affected by a breach and so on?	
72	Interviewee	Yeah i think most companies just needs to make sure that they have a processes in place where the communication towards the authority and the data subject involved are properly communicated. But i mean i don't really think, that is one of the most easy things to implement to make sure that you notify authority and the data subjects when you have a breach it is not technically difficult to do, so i don't really se a issue there. This question is more about communication so i don't really see no requirements from the GDPR, i don't really see why they wouldn't notify the authorities within the timeframe.	Breaches of Data
73	Interviewer	Yes and my question is like technically it is not a difficult thing?	
74	Interviewee	I don't think so, you just have to make sure that the IT-department are know that they have to inform people when this happens and the DPO and the privacy department and they will make the necessary steps to make this happen.	
75	Interviewer	Overall when you say that complying with the GDPR are more of an organizational one then a technical one to programming specific stuff?	
76	Interviewee	I think no, i think the challenge from GDPR, i think it is really changing, depending of the size of the business and the amount of applications and dependency of IT in the organization i mean there is a lot of dependency there but i think for larger companies it will be mapping where the data is, understanding the different applications, databases, interface layers and we are not even touching on unstructured data so that really finding where personal data is residing, that is really the key issue and then processes around like breach notification, assigning	The Right of Access, the Right to be Forgotten and the Right to be Forgotten

		a DPO that is a lot more easy.	
77	Interviewer	So it's about more legacy system that did not have this in mind when they were developed and now you have to try to map them and like make them compliant? That is the main issue?	
78	Interviewee	Yeah make them compliant or at least find ways to mitigate the risks i would say. That maybe also be key, mitigating the risks you have, or at least the residual, the GDPR is not always specific and i think really that we have to have a risk based approach and when we are producing for different applications or at least new ones, we do privacy risk assessment, we actually look at those risks, and privacy risks as you can evidence those to authorities that you have those in place and maybe not all are compliant but we can use that to lower the risk so it all about mitigation in a lot of ways, and showing that you are at least trying to be compliant. Because it is gonna be very hard for bigger organizations to say i am 100% compliant by may 25th 2018.	
79	Interviewer	So you think the timescope here, with one year to go it's gonna be hard to be done completely?	
80	Interviewee	it is not possible for larger organisations i think i don't think that is possible, maybe for smaller companies. But i think the timeframe communicated from the authority is more, to put pressure, i don't believe all these large companies will start getting fines, i mean considering that hey have started millions of these kinds of projects already, it is all about to show that you are trying to work on the problems and trying to solve it so it is more the journey to being compliant.	
81	Interviewer	So i'm guessing this will be continuing work, this is nothing like okay we are compliant we are done.	
82	Interviewee	No this is definitely not a one off exercise, this is kind of privacy related problems and data security and privacy assessment and you know these are like that have to be overtime and it is kind of important when consultants come into organisations that they find ownership within the organization. And that the anchor these processes and anchor them deep in the organization trying to avoid a one off exercise really.	Data Privacy Officer Privacy by Design and Default
83	Interviewer	So responsibility comes back, it is good if someone hold responsibility for different processes?	
84	Interviewee	Yeah there should be ownership in everything in a organization definitely.	Data Privacy Officer

85	Interviewer	I think that was all thank you!	

References

Bhattacherjee, A. (2012). Social science research : principles, methods, and practices, Tampa, Fla. : A. Bhattacherjee, 2012 2. ed.

Bridge, P. (2014). EU puts pressure on businesses to erase data. *Network Security*, vol. 2014, no. 8, pp.5-8.

Brinkmann, S. & Kvale, S. (2005). Confronting the ethics of qualitative research, *Journal of Constructivist Psychology*, vol. 18, no. 2, pp.157-181.

Cavoukian, A., (2012). Privacy by design [leading edge]. *IEEE Technology and Society Magazine*, vol. 31, no. 4, pp.18-19.

Cavoukian, A., Taylor, S. & Abrams, M.E., (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society*, vol. 3, no. 2, pp.405-413.

ComputerWeekly. (2017). *EU data protection rules affect everyone, say legal experts*. [online] Available at: http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts[Accessed 15 Mar. 2017].

Consilium.europa.eu. (2017). *The general data protection regulation - Consilium*. [online] Available at: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/ [Accessed 15 Mar. 2017].

Cuijpers, C., Purtova, N. & Kosta, E., (2014). Data Protection Reform and the Internet: The Draft Data Protection Regulation. In A Savin & J Trzaskowski (Eds.), *Research Handbook on EU Internet Law* pp.543-568: Edward Elgar

European Commission. (2016). European Union Article 29 Data Protection Working Party (2016), *Guidelines on Data Protection Officers ('DPOs')* [pdf], Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 [Accessed April 13, 2017]

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Metayer, D.L., Tirtea, R. & Schiffner, S., (2015). Privacy and Data Protection by Design-from policy to engineering, preprint pp. 1-60, available online: https://arxiv.org/abs/1501.03726 [Accessed Mars 25, 2017

Eggert, M., Winkelmann, A., Lohmann, P & Knackstedt, R. " The Regulatory Infuence On Management Information Systems - A Contingency Perspective" (2013). ECIS 2013 Completed Research. 9. h p://aisel.aisnet.org/ecis2013_cr/9

Ehrlinger, J., Gilovich, T. & Ross, L., (2005). Peering into the bias blind spot: People's assessments of bias in themselves and others. *Personality and Social Psychology Bulletin*, vol. 31, no. 5, pp.680-692.

Eldred, M., Adams, C., & Good, A. (2015). Impact of EU Data Protection Laws on Cloud Computing: Capturing Cloud-Computing. Delivery and Adoption of Cloud Computing Services in Contemporary Organizations [e-book] Information science reference. Available at: Google Books: books.google.com [Accessed 17 Mars 2017]

EUR-Lex. (2017). Regulation (EU) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance, Available Online: http://eur-lex.europa.eu/legal-

con-
tent/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC [Accessed 2 February, 2017]

Financial Times. (2017). *When capitalism wants to data mine you*. [online] Available at: https://ftalphaville.ft.com/2017/03/09/2185767/when-capitalism-wants-to-data-mine-you/ [Accessed 14 Mar. 2017].

Forbes.com. (2017). *New Report Shows European Businesses Underprepared For Data Protection Regulation*. [online] Available at: https://www.forbes.com/sites/jenniferhicks/2016/10/27/new-report-shows-european-businesses-underprepared-for-data-protection-regulation/#37453c754c82 [Accessed 15 Mar. 2017].

Fuller, M (2015). BIG DATA: NEW SCIENCE, NEW CHALLENGES, NEW DIALOGICAL OPPORTUNITIES, *Zygon: Journal Of Religion & Science*, vol. 50, no. 3, pp.569-582

Gilbert, F. (2016). EU GENERAL DATA PROTECTION REGULATION: WHAT IMPACT FOR BUSINESSES ESTABLISHED OUTSIDE THE EUROPEAN UNION. *Journal Of Internet Law*, vol. 19, no. 11, pp.3-8

Hansen, M., (2016). Data Protection by Design and by Default à la European General Data Protection Regulation. In *Privacy and Identity Management. Facing up to Next Steps* pp.27-38

Heimes, R. (2016). Global InfoSec and Breach Standards, *IEEE Security & Privacy*, vol. 14, no. 5, pp.68-72

de Hert, P. & Czerniawski, M., (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, vol. 6, no. 3, pp.230-243

de Hert, P. & Papakonstantinou, V., (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?., *Computer Law & Security Review*, vol. 32, no. 2, pp.179-194.

Hintze, M., (2016). Viewing the GDPR through a De-Identification Lens: A Tool for Clarification and Compliance, preprint pp. 1-22, Available Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2909121, [Accessed 23 Mars 2017]

Hildebrandt, M. & Tielemans, L., (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, vol. 29, no. 5, pp.509-521

Hooson, S., (2015). Smarten your data security before new EU legislation or risk corporate loss. *Network Security*, vol. 2015, no. 6, pp.8-10.

Ifinedo, P (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, Computers & Security, vol. 31, no. 1, pp. 83-95, Available online: http://www.sciencedirect.com/science/article/pii/S0167404811001337/pdfft?md5=ea077ce4f20783a410e1e6fc92a8482d&pid=1-s2.0-S0167404811001337-main.pdf [Accessed 29 April 2017].

Jacobsen, D. I. (2002): Vad, hur och varför. Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Studentlitteratur, Lund

Kleindienst, D., Nüske, N., Rau, D & Schmied, F. (2017): Beyond Mere Compliance — Delighting Customers by Implementing Data Privacy Measures?, in Leimeister, J.M.; Brenner, W. (Hrsg.):13th International Conference on Wirtschaftsinformatik (WI 2017), Available Online: http://aisel.aisnet.org/wi2017/track08/paper/2/ [Accessed 17 April 2017]

Knackstedt, R., Braeuer, S., Heddier, M., & Becker, J. (2014). Integrating Regulatory Requirements into Information Systems Design and Implementation. Thirty Fifth International Conference on Information Systems, Auckland,

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*, vol. 28 no. 2, pp.159-171.

Koščík, M (2017), The Impact of General Data Protection Regulation on the grey literature, *Grey Journal (TGJ)*, vol. 13, special issue, pp.42-45

Kvale, S. (1996). The 1,000-page question. *Qualitative Inquiry*, vol 2 no. 3, pp.275-284.

Kvale, S. (2006). Dominance through interviews and dialogues. *Qualitative Inquiry* vol. 12 no. 3, pp.480-500

van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. *Government Information Quarterly*, vol. 33 no. 2, pp.338-345

Lohmann, N (2012).Compliance by design for artifact-centric business processes, Information Systems, vol. 38, no. 4, pp. 606-618, Available online: https://doi.org/10.1016/j.is.2012.07.003 [Accessed 4 May 2017]

Lynskey, O. (2015). The foundations of EU data protection law. 1st ed. Oxford: Oxford University Press.

Lyons, V. R., Van Der Werff, L., & Lynn, T. (2016). Ethics as Pacemaker-Regulating the Heart of the Privacy-Trust Relationship between Organisations, their Consumers and their Employees: A conceptual model, and future framework.

Myers, M. D. & M. Newman (2007). The qualitative interview in IS research: Examining the craft. *Information and organization* vol. 17, no. 1, pp.2-26

Norberg, P., Horne, D. and Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, vol. 41 no. 1, pp.100-126.

Norris, N., (1997). Error, bias and validity in qualitative research. *Educational action research*, vol. *5* no. 1, pp.172-176

Oprysk, L. (2016). The Forthcoming General Data Protection Regulation in the EU. *Juridica International*, vol. 24 pp.23-31

Panitz, J C., Wiener, M., & Amberg, M. (2011) "FACTORS FACILITATING COMPLIANCE IMPLEMENTATION – CASE STUDY RESULTS FROM MULTINATIONAL ENTERPRISES". ECIS 2011 Proceedings. 3. h p://aisel.aisnet.org/ecis2011/3

Poullet, Y., (2006). EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review*, vol. 22 no. 3, pp.206-217

Recker, J. (2013). Scientific research in information systems : a beginner's guide, Berlin ; New York : Springer, cop. 2013.

Ryz, L, & Grest, L (2016), Feature: A new era in data protection, Computer Fraud & Security, vol. 2016, no. 3 pp.18-20

Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling control objectives for business process compliance. In International conference on business process management, pp. 149-164. http://link.springer.com/chapter/10.1007/978-3-540-75183-0_12 [Accessed 4 May 2017]

Smith, H., Milberg, S. & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, vol. 20 no. 2, p.167

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, vol. 2016 no. 6, pp.5-8.

Tankard, C. (2017). Encryption as the cornerstone of big data security. *Network Security*, vol. 2017 no. 3, pp.5-7.

Turetken, O., Elgammal, A., van den Heuvel, W.J. & Papazoglou, M (2011). Enforcing compliance on business processes through the use of patterns.
ECIS 2011 Proceedings, vol. 5. Available online: http://aisel.aisnet.org/ecis2011/5 [Accessed 5 May 2017]

Walsham, G. (2006). Doing interpretive research. *European journal of information systems* vol. 15 no. 3, pp.320-330

Wong, R. (2012). The Data Protection Directive 95/46/EC: Idealisms and realisms. *International Review Of Law, Computers & Technology*, vol. 26 no. 2/3, pp.229-244.