A case study on managing customer data to comply with GDPR

Shahriar Hossain

Faculty: HS, Karlstad Business School

Subject: Information Systems

Points: 15

Examiner: Remigijus Gustas

Date: 2019-02-22
Abstract

This bachelor thesis paper presents a case study on the technical actions undertaken by a company in order to manage its customers’ personal information in compliance to GDPR (General data protection regulation), a law that was introduced on the 25th May of 2018. GDPR imposes strict responsibilities on the companies dealing with personal information. Therefore, companies located in EU or handling personal information of EU citizen have to review and update their information handling process to comply according to the law. Companies failing to comply with GDPR can be subject to heavy penalty.

This paper presents an in-depth picture of how a small company which is quite reliant on data processing adapts itself to the GDPR era when handling their customer’s personal data. The Order Department and the Technical Department within the case company, where most of the customer’s personal information is handled, were studied for this thesis. In conclusion, this case study identified seven different measures that the company undertook to comply with GDPR including periodical deletion of email letters, using separate email addresses for company internal messages, and tight restrictions on who can access what data. Moreover, two major challenges were identified: time and legacy. Time, because a small sized company cannot set off one staff to deal with everything related to GDPR but instead everyone has to take this regulation into consideration. The second challenge is legacy, because data routines before the GDPR were not strict.

Keywords:
“GDPR”, “Personal data”, “Data protection”, “Information system”
Contents

Chapter 1: Introduction
1.1 Problem Background 3
1.2 Purpose 4
1.3 Research question 5
1.4 Target Group 5
1.5 Limitation 5
1.6 Methods
  1.6.1 Case study method 5
  1.6.2 Case company 6
  1.6.3 Document analysis 6
  1.6.4 Interview 7

Chapter 2: Literature review
2.1 Principles of GDPR 9
2.2 Personal data 10
2.3 Data portability 11
2.4 Privacy by design and privacy by default 11
2.5 Data protection 15
2.6 Pseudonymization and anonymization 15
2.7 Data Encryption 16
2.8 Information System 16
2.9 Managing personal data in CRM 17
2.10 Database management system 17

Chapter 3 - Results
3.1 Result from Document analysis
  3.1.1 Result from process documents 19
  3.1.2 Result from customer documents 19
  3.1.3 Result from incident documents 20
3.2 Result from the interview 21

Chapter 4 - Analysis 24

Chapter 5 - Conclusion 29

References

Attachment
Chapter 1: Introduction

This chapter introduces the problem background and the research method.

1.1 Problem Background
The first European Union (EU) data protection directive was established and adopted in 1995 (European Data Protection Supervisor, 2018) when the internet and the mobile phone was still at its early stage. People did not do social networking, online banking or online shopping at that time when the regulation was first introduced. Technology has been changed drastically since then and a lot of reforms to the old laws and regulations were needed to be re-considered in order to keep up and address the issue of data privacy and personal data protection.

Today the personal data is collected and used by almost all types of industries. The world economic forum has termed personal data as a new economic “asset class” (World Economic forum, 2011). It states that the personal data is a valuable resource for the 21st century that will touch all aspects of society. Big companies like Amazon, Google and Walmart are constantly collecting personal data to create values for customers and businesses. The benefits for collecting and analyzing personal data is quite evident and visible for a large number of actors / organization, but at the same time, the protection of this new class of asset has to be guaranteed. There are numerous incidents where the organization failed to ensure protection of personal data, resulting in risks to individuals and organizations.

The General Data Protection regulation (GDPR) (2018) was introduced on the 25th may 2018 with a mission to providing clarity and consistency for the protection of the personal data. The GDPR imposes rules on organizations in the European Union (EU) and those that offers goods and services in the EU, or that collect and analyzed data tied to EU residents, no matter where they are geographically located (Datainspektionen, 2018).

The goal of the GDPR is to providing clarity and consistency for the protection of personal data. GDPR aims to enhance personal privacy rights and thus providing higher degree of data protection. It also imposes increased responsibilities on the people and organization for protecting personal data. Organization failing to comply with the GDPR will be charged with significant penalties as stated in “GDPR Key Changes” at EU GDPR Portal (2018).

Companies selling products and service may have multiple information system / platforms such as Customer Management System (CRM), Order management system, webshop etc through which data related to their customers, orders, sales, invoices and other operations are handled and managed on a regular basis. In general context, customers of these companies play the major role in generating most of the personal data. That is, if there is no customer, there is no personal data, no order data, no sales or invoice data. Even prior to the
introduction of the GDPR, popular commercial CRM Systems, Webshops, Email applications etc had good data security and protection methods inbuilt in the application. Technology like encryption and hashing had been used since long to protect personal data stored in these systems and companies had been reliably using them since then. GDPR has brought no massive changes in the technology these systems are built with. But after the GDPR law is imposed the companies using these systems now have to set protocols and rules on how the personal data are managed there according to the GDPR law.

In order to comply with GDPR, companies handling personal data (such as customer or employee data) may need to bring certain changes in their old way of managing this information. This may require to bring changes in their work process or upgrade their information system to ensure the privacy and security of personal data. If any issues related to handling of personal data are found either in the work process or in the information system, measures should be immediately taken to rectify those. The companies should pay high attention to it now that the personal information they are storing are handled in a careful way, according to a journalist at one of Sweden’s leading business newspapers, *Dagens Industri*. (Karlsson, 2018)

The overall goal of GDPR is well defined by the EU legislation body and the actual clauses and principles are quite straightforward. Small companies that do not have the necessary resource to have a full time GDPR expert may find it helpful to follow other companies who have already complied with GDPR in handling customers' information. But, as stated above, GDPR is young compared to many other technology based regulation that exists today and there are lack of examples and practical information on exactly how the companies should achieve GDPR compliance. Different companies may be from different domain and have different work process when it comes to handling personal data. The amount of researches on GDPR are also less than comparing to other areas of computing. Searching with the keyword ‘GDPR’ in google scholar yield a little over 10,000 result whereas the key word ‘Data Protection’ yielded over 100,000 result (both the searches are filtered with year 2018).

1.2 Purpose
This study was performed on a case company who are, at the time of writing this thesis paper, in the process to structure and formalize certain areas of the company to comply with the GDPR. Among these, one of the vital areas is the handling of customer’s data, which the case company is taking very seriously. The purpose of this bachelor thesis paper is to provide a case study example of how GDPR is dealt within a company selling products and services to its customer.
1.3 Research question
In regards to the purpose, this thesis paper aims to answer the following research questions:

1. How does the case company handle their customer’s data in the information system from order to delivery in compliance to GDPR?

2. What are the technical challenges faced by the case company in handling customer’s data to comply with GDPR?

1.4 Target Group
The target groups for this study are mainly those who want to get an overview on GDPR and get a real world scenario on how the customer’s information are stored and managed by the companies in accordance with GDPR. This group maybe researcher or student who may be interested in GDPR and working with GDPR. Another group such as employee who work in decision-making roles in the company or those who are in charge of data privacy and protection may also find this study quite interesting.

1.5 Limitation
It is important to note that the case company that was chosen to perform this study is located in Sweden and is small in size. It does not necessarily represent the mass or all companies in general. Other companies may have a different process for complying with GDPR. This thesis paper only covers the technical aspect of the GDPR and do not intend to interpret any legal (juridisk) concept. Moreover the focus of this thesis is handling of customer’s information from the time they place an order until the product is successfully delivered to them.

1.6 Methods
The empirical data for this study was collected through qualitative research. It is easy to investigate the problem area through qualitative research, which, gives an in-depth picture and covers a wide area into the problem. Interview in qualitative research uses verbal analysis method (Patel & Davidsson 2011) for data gathering. On the other hand Quantitative research method is highly dependent on obtaining data from previous researches, interviews and surveys.

1.6.1 Case study method
Qualitative research method is a big area and to narrow it down to answer the research question of this thesis paper, ‘case study’ approach is used. Case study is most often described as the part of the qualitative research (Merriam 1998, Starman 2013, Yin 2014). However in certain situation it may also be quantitative or contain a combination of qualitative and quantitative methods (Starman 2013).
The definition of case studies that best suits the context of this thesis paper is given by Yin (2014). According to the author, a case study is used in the situation where the main research question to answer is ‘how’ and ‘why’. He also states that case study method is relevant when the research question requires an extensive and in-depth description. In regards to Yin’s definition, this thesis paper aims to provide an overview on ‘how’ the case company handle its customer’s data in information system in compliance with the GDPR, ‘why’ and later ‘what’ are the technical challenges faced by the case companies. Therefore the case study method was most suitable to perform this research. However case study approach comes with some challenges as well, as Merriam (1998, p. xi) stated that the researcher can become confused as to what a case study is and how it can be distinguished from other types of qualitative research. Therefore careful planning is necessary while using case study approach.

1.6.2 Case company
The company Talk Telecom AB was chosen as the case company for conducting this study as it is a rather small company with around 10 employees. Talk Telecom AB was founded in 1996 and is currently located in Häggvik, Stockholm. It is a distributor of hardware and services for open SIP telephony products and leading brands in IP telephony. In most cases, the direct customers of Talk Telecom are companies and organizations rather than a person or an individual. Thus the amount of direct personal data collected and stored for sales and support purpose are not that huge. However, the company deals with personal data to some degree, for instance while storing the contact information for person who represents a company that has ordered service or product from Talk Telecom. At the time of conducting this study the company was in the process to comply with the GDPR.

1.6.3 Document analysis
Bowen (2009) defined document analysis as a systematic procedure for reviewing or evaluating documents, both printed and electronic material. The aim of document analysis, is to obtain a better understanding and develop empirical knowledge and often done in combination with other form of data gathering method. Therefore, rather than just depending on the interview as the only source of data, I chose to analyse the document at the case company for obtaining a more clear view and verifying the credibility of the empirical data used in this study.

To begin with this study, various types of documents were provided to me by the case company for analysing. The first step was to sort these document and select only those which are relevant for this study. My selection contains the documents related only to customers excluding any purchase or financial documents. No actual customer information from the case company has been used in this thesis paper.
1.6.4 Interview

For the case study, I designed an interview to gather empirical data for my research. While working on the interview I found that authors Bryman and Bell (2005) classified qualitative interview into four different categories; unstructured, semi structured, focus group and structured. Among these, the semi structured interview process is used to gather the qualitative data that are vital for addressing the research questions. My aim with the interview is to uncover descriptive data based on personal experience of my respondents.

In a semi structured interview the researcher prepares a list of questions or issue, in the form of an interview guide, which needs to be addressed by the respondent in an interview session. In the semi structured interview approach the respondent has the freedom to formulate the answer in his or her own way (Bryman & Bell 2005, p301). To dig deeper, the researcher can also ask further questions that is not present in the interview guide. In a semi structured interview the interview process is flexible but still follows the interview guide.

After analyzing several sources (Bernard 2000, Zorn 2010) I have designed the interview guide in the following way

1. Choice of respondents - Depending on the type of data I need I have chosen the respondents carefully. The details of the respondent are given in Table 1.

2. Following rules were maintained in developing the questions -
   a. I used open-ended questions to get descriptive answers rather than close-ended questions which can be just answered with "yes" or "no"
   b. I have avoid questions whose response may lead to another questions.
   c. I have kept the terms and the language simple.
   d. I have kept the questions short and specific.

3. The order in which the questions will be asked was set.

For this thesis work I reached to three respondents; see Table 1. Respondent 1, 2 and 3 are all employed by the case company who have different roles in the company. Multiple respondents from different department within the case company were involved for this qualitative interview to get a broader set of answer. The transcript of the interview (containing only the key points for this study) can be found in Attachment 1. The interview was conducted in two different session due to the shortage of time.
Table 1: Interview guide

<table>
<thead>
<tr>
<th>Respondent 1</th>
<th>Role</th>
<th>Type</th>
<th>Goal to conduct the interview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Dept</td>
<td>In Person</td>
<td>To get an overview of the current process regarding the handling of personal information in the company</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Respondent 2</th>
<th>Role</th>
<th>Type</th>
<th>Goal to conduct the interview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Dept</td>
<td>In Person</td>
<td>To understand what type of personal data are handled by the Order department.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Respondent 3</th>
<th>Role</th>
<th>Type</th>
<th>Goal to conduct the interview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Dept</td>
<td>In Person</td>
<td>To understand what type of personal data are handled by the Technical department.</td>
</tr>
</tbody>
</table>

Questionnaires to Respondent 1 (Admin Department)
1. When do you need to store data related to a person and how it is stored?
2. What type of personal data does your company deals with?
3. What software / platforms do you use to manage and access the personal data?
4. How is the access to these software / platform distributed and managed?
5. How long do you keep the personal data into the system that you used?
6. Do you have an up-to-date privacy policy that your customers can view?
7. How much you are compliance with GDPR in your company at present?
8. What issue is Talk Telecom facing when you are applying GDPR in your company?

Questionnaires to Respondent 2 (Order Department).
1. What is the process when a customer place an order?
2. What types of personal information do you store while processing Order from the customer?
3. What happens to the data when the orders are completed / shipped?
4. How much is your department complying with GDPR now?
5. What have been done at your department until now so far to comply with the GDPR

Questionnaires to Respondent 3. (Technical Department)
1. What is the work process in technical department?
2. What types of personal information (if any) do you store at your technical department
3. What happens to the data (if any) when the data is no longer needed?
4. How much is your department complying with GDPR now?
5. What have been done at your department until now so far to comply with the GDPR?

1.6.5 Ethical Consideration
I have strived to follow the principles of the Swedish Research Council (Vetenskapsrådet 2002). The respondents have agreed to my data collection and have also been given the opportunity to comment on my transcripts and general conclusions. No one has objected.
Chapter 2: Literature review

Reviewing literature, articles and existing research on GDPR was vital to obtain a good insight into the problem area and gain domain expertise. The literatures and articles that are used in this study are kept relevant to the technical side of the GDPR rather than the social or legal side. Google scholar and Diva portal (Digitala vetenskapliga arkivet, 2018) are used as the primary sources for accessing the literatures. While referencing the articles from website, special care has been taken to ensure the reliability and legitimacy of the sources as much as I could. Some examples of the keywords that were used to find the relevant articles and limit the number of the searches are, such as, “GDPR”, “Personal Data Protection”, “Information system security”, “GDPR compliant database design” etc. Being GDPR just few months old, I ignored any literature and articles that were published prior 2010.

2.1 Principles of GDPR
In the processing of personal data, six principles must be fulfilled to comply with GDPR. According to the Article 5 in GDPR these principles are,

1. Lawfulness, fairness and transparency of data collection
   The first principle of GDPR is about managing personal data in a fair and honest manner. Companies handling personal data need to make sure their data collection practices do not break the law and that they are not hiding anything from data subjects. There should be information available to the persons whose personal data is collected. This information should contain what type of data about the person is collected, why it is collected and how it is used.

2. Purpose limitation
   The companies should only collect personal data for a specific purpose, clearly stating the purpose of collection, and store them only as long as it is necessary to complete that purpose.

3. Data minimization
   Companies should store and process only the personal data that they need to achieve its processing purposes.

4. Accuracy of data
   The integrity of personal data is vital to data protection. GDPR states that the companies should take every possible step to erase or rectify data that is not accurate and complete. If a correction is requested by the data subject, action should be immediately taken by the companies to correct it.
5. Data Storage limitation
The companies need to erase personal data when it’s no longer necessary. GDPR demands that the companies have storage policies that clarify what type of data will be erased and after how long.

6. Data Integrity and confidentiality
GDPR states that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures". The GDPR is deliberately vague about what measures organizations should take, because technological and organizational best practices are constantly changing.

2.2 Personal data
Before diving deep, it is important to understand the concept of personal data in the context of GDPR. Point (1) in Article 4 in GDPR describes personal data as the information that can directly or indirectly identify a natural person. Personal data may be name, address, email, social security number, image, IP address or phone numbers. It may also be genetic data or biometric data such as fingerprints, facial recognition and iris scan data. For example, a company that collects information on people who visits their website might ask them to state their occupation. This does not directly fall under the GDPR's scope of personal data, as many people may have the same occupation. However, when the data on the person's occupation is collected together along with the other data such as name and location, it could be used to narrow down the number of people where in many cases the individual person could be identifiable.

Certain personal data can be sensitive by nature and therefore requires a higher degree of protection. These data are termed as 'sensitive' personal data. As a general rule, it is forbidden to handle sensitive personal data, but there are certain exceptions. Before dealing with sensitive personal data, the reason and the legal basis must be cleared up (GDPR, Article 9). A doctor for instance has the right to access sensitive information of his / her patient when the patient registers for a checkup. There may be legitimate reason to do so. On the other hand it is not required for an online store staff to handle any sensitive information about the customer such as the customer's ethnicity or sexual orientation. A person's Sensitive personal information may include his or race or ethnic origin, political opinions, religious or philosophical conviction. Sensitive health related data can include a person's psychological profile, sexual orientation, genetic data and biometric data that uniquely identifies a person. (GDPR Article 9, and recitals (51) and onward)

In many countries of the world, the citizen and resident receives a person identity number to uniquely identify them. For example in the United States this is called the Social Security number (SSN). Every person registered in Sweden also receive a personal identification
number. The personal number is obtained from the Swedish Tax Agency known as Skatteverket in Sweden. The personal number is composed of 10 digits and a hyphen symbol in the form of YYMMDD-NNNN. The first six digits indicate the person's date of birth in the format year-month-day order. The following three numbers are a serial number, where the third digit describes the person's gender, for female this digit is an even number and for male it is an odd number. In some cases when a visitor is visiting Sweden for a short term, he or she may not be eligible to receive a personal identification number rather receives a Coordination number (Samordningsnummer). The Coordination number is an identifier of persons who are not or have been registered in Sweden but still needs to be identified as a residence in Sweden (Skatteverket, 2018). Both of these numbers uniquely identifies each resident in Sweden and are considered as sensitive data due to the fact that they are revealing two critical pieces of information, first, the date of birth and second, the gender of the person.

GDPR put extra clauses when it comes to handling these unique numbers. The Swedish identification and coordination number may be processed if the registrants/person have given their consent. If there is no consent, personal identification numbers can only be processed when clearly motivated on the purpose of the handling this number. Article 9 in the GDPR law describes a set of rules and regulation in handling this sort of personal information.

2.3 Data portability
In Sweden GDPR has replaced the old PUL (Personuppgiftslagen) law, which implies that changes are required for organizations that process personal data with enhanced privacy protection. The Datainspektionen (Datainspektionen, 2018) describes what has changed from PUL to GDPR. One of these changes is the right to ‘data portability’. Right to data portability is described in the article 20 of GDPR. Data portability is the ability to obtain the personal information which they have provided to an organization, in a format that the person can keep in his/her device or share it with others. The article particularly mentions about two kinds of data that is subject to ‘right to portability’. These are,

1. The data that a person actively and knowingly shares with the organization such as name, address telephone etc.
2. The data that is collected by automated means or indirectly provided by the user when using a device or a service. This data may include the location of the person when accessing a mobile app, activity log or history gathered while accessing a website for instance.

2.4 Privacy by design and privacy by default
The introduction of the concepts ‘Privacy by Design’ and ‘Privacy by Default’ are two of the changes that GDPR introduces in EU data protection law. The aim of the Privacy by design (pbd) concept is to ensure the privacy issues of an individual is seriously taken into account in the initial phase of the design of an information system, instead of addressing them when
they occur and trying to build security mechanisms afterwards. (GDPR Privacy by Design, 2018)

Under the current directive as stated in the Article 25 in GDPR, data controllers or companies already need to implement appropriate technical and organizational measures to protect data against unlawful processing. The GDPR requires companies to consider privacy at the earliest stage while designing an information system that handles personal information. When the companies think upfront about what personal data they use, for what purpose and how they will do this legitimately, it reduces the chance of discovering at a later stage that implementing privacy into the system may be technologically challenging, expensive or even sometime impossible. (Data protection by design and by default, 2018).

Privacy by design (PbD) was originally developed by Dr. Ann Cavoukian, back in the’90s. (Cavoukian 2009). This concept has been used in designing and developing system and software application since then. The concept of PbD was already in place before the GDPR came into effect. What GDPR did was simply made this legally binding. The effect that the Data protection by design and by default (Regulation 2016, Chapter 4 Article 25) puts on the company is that the companies have to take proactive rather than reactive measures (Cavoukian 2009) aiming to prevent privacy related incident and malfunction in a software system before they happen.

While developing an information system such as a CRM (Customer relationship management) system, a typical system development life cycle (SDLC) according to Alexander & Maiden (2004, p40) is shown in Figure 1.

<table>
<thead>
<tr>
<th>Requirements Discovery</th>
<th>Requirements Validation</th>
<th>System Specification</th>
<th>System Design</th>
<th>Coding</th>
<th>Testing</th>
<th>Operation &amp; Maintenance</th>
</tr>
</thead>
</table>

Phases where PbD should be considered

**Figure 1: System development life cycle (SDLC)**

The first step of the SDLC is the requirements discovery where the actual requirement of the information system is gathered from the user or product owner. In the next phase this requirement is validated and a system specification is produced outlining how the system will work according to the requirement. After the specification is sorted out, the system designer produces a detail design on how to develop the system. Based on this design the coders and tester takes over the work to implement and deliver the system to the end user.

The first four phases of the SDLC mentioned in figure 1 are the critical phases where privacy by design has to be considered seriously. Several technical strategies can be taken in order to implement PbD while developing a system. These strategies often depends on usage or
goal of the system and what kind of technology (such as the choice of programming language, framework, library etc.) is being used to develop the system. Despite what technology or strategy is being used, using PbD strategies in the system development process should make privacy issues more concrete. The author in his paper ‘Making Privacy by Design Concrete’ (Hoepman 2018) has identified eight such PbD strategies. The first four strategies are data oriented and include minimizing, separating, hiding and abstracting data. The other four strategies are process oriented which include informing data subject, controlling, enforcing and demonstrating data.

GDPR states that “Privacy by default means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones” (Data protection by design and by default, 2018). Figure 2 shows the default privacy setting from the browser google chrome. From the figure we can see the options such as ‘Use a web service to help resolve spelling error’ is turned off by default. The reason behind it is the fact that, if the option is turned on, web service that helps with the spelling error will actually collect all the words that are typed by the user, check for spelling in the system google uses and send the correct spelling back to the user. In other word any word (sensitive or insensitive) typed by the user on the browser is being sent to an external web service. This may be considered as a lapse in the privacy protection by users and therefore it is turned off by default. If a user wants to enjoy this facilities for checking spelling mistake, he or she can always go to the settings and turn it on. On the other hand safe browsing is turned on by default to protect the user’s device from malicious websites flagged by google.
Figure 2: Default privacy and security settings of the Google Chrome browser
2.5 Data protection
In the paper, The Security Risks Associated with Cloud Computing (Agarwal & Agarwal, 2011), the two student authors mention three vital points for data protection:

Confidentiality of data - It ensures that the data is not or made available to unauthorized entities or disclosed to anyone who is not supposed to access the data.

Integrity of data - It is to ensure that the data remains in its original state, meaning that it has not been manipulated or tampered anyway by anybody.

Availability of data - It ensure that the data is available when needed and that the system hosting and managing the data is fully functional without any faults.

Even if the authors are students, this article has been cited 35 times according to Google Scholar so these three points do not seems controversial.

2.6 Pseudonymization and anonymization
Article 32 of the GDPR mentions about pseudonymization and encryption of personal data for providing data security. Both pseudonymization and anonymization are the two methods to hide identities and personal data but in different ways.

Pseudonymization in the IT system means replacing a part of the personal data with artificial identifier (Mourby 2018). In GDPR, pseudonymization is defined as 'processing of personal data in such a way that personal data can no longer be attributed to a specific registered without using additional information' [GDPR Article 4(5)]. After masking the Personal data is no longer recognizable and is coded, additional information (to break this code) is needed to recreate original information. This additional information is kept separately.
Pseudonymization makes the information less accessible to unauthorized users, and is a good way to achieve the security requirements of GDPR, in practice information such as personal identification can be pseudonymized.

In GDPR, it is written that anonymous data should be made anonymous in such a way that the registered person can no longer be identified (Mourby 2018). This can be achieved by simply removing the possibilities of identifying a person, and there are no additional information that can link the information to the registered person. Anonymization can be a difficult technique as it will completely lose the connection between data and the individual. If the data is made anonymous it is often safe to use for statistical or research purposes.

From the above description we can see a clear difference between the two concepts. Pseudonymization means that an individual can still be identified through indirect or additional information that was used for masking his / her data. This means that pseudonymized personal data are still covered by the GDPR regulation. Anonymization means that the original information cannot be restored, and such data are not covered by the regulation. There are different techniques that can be used to pseudonymized and anonymized personal data, such as data masking and data scrambling.
Masking means that some of the information in the original data is hidden using random characters or other data. One example is search pages like find.se, ratsit and eniro where the last four digits of the date of birth are replaced by characters. Masking is also widely used in online payment processing, masking parts of the card number. Scrambling means mixing / replacing the letters, and some examples of scrambling techniques are encryption and hashing.

2.7 Data Encryption
The GDPR law itself has taken a long time to compile and is intended to last for a long time. Laws and regulations do not usually mention any special technical solutions that must be fulfilled as the technology may change faster than laws. However, there is an exception and in the GDPR law where it is explicitly talks about the term ‘Encryption’, to provide technical solution for data privacy. It even says that if an organization has implemented encryption correctly, i.e. By implementing a proven encryption algorithm and that the encryption keys are kept inaccessible to third parties, they are not obliged to inform if any data breach occurs (Regulation EU 2016/679, 2016).

Encryption refers to the procedure that converts text data such as (name or personal identification number) into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key. Using encryption procedure minimizes the risk of an incident during data processing, as encrypted data are not-readable for third parties who do not have the correct key. Encryption is one of the best ways to secure stored personal data and protect data during transfer. It also reduces the risk of abuse within a company, as access is limited only to authorized people with the right key (Christina, Techworld 2018).

2.8 Information System
Valacich and Schneider (2010) defines information system as “Information systems (IS) are combinations of hardware, software, and telecommunications networks that people build and use to collect, create, and distribute useful data, typically in organizational settings.” From this definitions, it can be said that combination of the above component such as the hardware, software etc. collect, store, organize, and distribute data throughout the organization. Database are typically used as the backbone of any information system. An information system does not necessarily needs to be a complex software system rather any system that qualifies the above definition.

One of the information system that is widely used by the companies selling products and services to its consumers is the customer information system. It is a system that is used to manage customer data maintain the communication with the customers. This types of information system are also called as Customer relationship management (CRM) system which is used by the companies to improve relationship with its customer.
2.9 Managing personal data in CRM
A CRM is a business management tool used to manage the existing and prospective customers in the most efficient way possible with the goal to strengthen profitable relationships with customer (Foss, Stone, Ekinci 2008). The Customer data that are stored and processed in a CRM is therefore also personal data. The type of customer data that the company stores in a CRM caries according to the nature of the business. Some company may store only the customer’s name and contact information to deliver a product or service at the customer’s end whereas other companies may need to store sensitive data like personal identification number, id card, information about family members, financial data etc. There are lot of CRM system that can be bought off the shelf. One of the popular CRM system is Sweden is Visma.

2.10 Database management system
As stated in Section 2.8 that the heart of any information system is a database at the backend where all the data is stored. This data is managed by a set of software or tools collectively known as database management system (DBMS). Coronel and Morris (Coronel, Morris 2017) defined “A database management system (DBMS) is a collection of program that manages the database structure and control access to the data store in the database”. In order to explain the database in a general terms the author compared it to an organized electronic filing cabinet where the content of the cabinet (data) is managed by a software system (DBMS).
Chapter 3 - Results
This chapter presents the result from the empirical data that is collected.

3.1 Result from Document analysis
The result from analyzing the documents are presented in this section.

3.1.1 Result from process documents
The first document that was analyzed is powerpoint presentation that the case company may use in conferences and seminars. This presentation gives a good overview of the company and what its delivers and how it works. The most relevant information that I could extract from this document is details description on how the company works when it involves a customer. This would give a better picture for the reader of the thesis to interpret the rest of the result. The content of the document is summarized in Figure 3.

![Figure 3: Process of the case company. Source: The author](image)

The first step in the customer handling process for the case company to receive an order from the customer. Once the order is received for the products it is sent to the configuration department to configure according to the customer’s choice. After the configuration of the devices are complete, the products are sent to the customer’s delivery address which the customer mentions during the ordering. After the delivery the invoicing and billing process starts with the customer. After the products are purchased by the customers, they often come back to the case company for various support and services. The customers have also the option to subscribe for a premium support with additional cost. The company always strive to maintain a good long term relation with its customers and strongly looks forward to give the best possible service. Therefore maintaining customer’s up-to-date information is vital for the case company.

3.1.2 Result from customer documents
In usual case, the case company sells its product and services to other companies maintaining a b2b (business to business) sales model. The customer company can be for example a tele operator or retailer.

In order to maintain proper communication, the case company needs to store the personal information of a responsible person who represents the other company. In most situation this information contains the person’s name, contact and address. Figure 4 shows an application form for the retailers to fill in.
In addition to the retailer’s company information the case company needs to know a person’s first name, last name, email, phone and the role of the person in the company. In addition to this the case company are also provided with a list of the end customers of the retailers. The case company stores the contact information of all the end customers and is responsible for configuring the devices and send directly to the end customer on the behalf of the retailers. This increases the volume of the personal information collected by the case company, thus making the nature of the data sensitive, in contrast to collecting only the personal information of the retailer.

The case company is in the process of developing a privacy policy that will be added to the company website in order to make clear and transparent on how the company uses this personal information. The aim is to comply with the first principle of GDPR that is to follow, ‘Lawfulness, fairness and transparency of data collection’ as stated in Section 2.1. The draft of the privacy policy state the followings regarding how the case company may use the personal information it stores

1. When processing orders and handling returned products
2. For Support and service related issues
3. For SMS notifications about delivery status
4. For contacts regarding any problems with the delivery
5. In case of correspondence, questions and other information
6. When sending out offers in the form of newsletters, always with instructions on how it can be unsubscribed from further mailings
7. In case of any questionnaires to improve our services and offers.
8. In case of work that prevents abuse or other inappropriate use of our website

3.1.3 Result from incident documents

The case company takes any security breach very seriously and logs, report and take immediate action on any data breach. The case company has made a template where such breach and action will be recorded. The document is called ‘Incident plan’. One example of such incidents can be, compromised user id and password of the phones that the customers are using. The original template could not be shown here as it is in Swedish and contains certain confidential instructions to the employees of the case company, but looks similar to Figure 5.

![Incident Document Template](image)

*Figure 5: Incident Document Template, Source: The Author*

The template contains the incident date / time, description, action etc. If an incident concerning personal data management has taken place, an incident report (not shown here) should be completed by customer who are the victims of the incident. The case company has created a separate email address where all the incident related emails arrive. Once an incident report arrives in the email, one employee in the case company is responsible to immediately notify the victim of the incident. Then the employee review the report and fill up the form shown in Figure 5, store the documents in a specific directory in the company’s server and starts taking appropriate action.
3.2 Result from the interview

The interview was conducted in two sessions. The first session involved general questionnaires regarding the company, process and data policy. The empirical data was gathered mostly during the second session, which went much deeper into the problem area. For reader’s convenience, result from both the sessions are compiled into one and presented below.

It is found from the interview that the case company deals with customer’s personal information and the configuration information of the product they are buying from the company. Both of these type of information are personal and sensitive. Through personal information such as name and address can be identified and located directly. The configuration information is sensitive in the sense that each phone is loaded with credits of an amount the customer requests. Anyone who has the access to the configuration information such as the phone number, username and password can start using the phone and the customer will be credited or billed for the calls made through those phone. The order department (Respondent 2) deals with processing the order made by customer either through email or through the web shop. This department store and handles customer’s personal information. The technical department is responsible for handling phone or device’s configuration related information. If there is no configuration of the device is needed, the devices are sent directly to the customer from the order to delivery department.

The three places where the case company stores and process personal data are in their server, email application and a CRM application. In server the information is stored in doc, pdf or excel document in a proper directory structure. For security reason the configuration of the server and email application is not revealed and neither those are relevant for this study.

All the above mentioned customer information are handled primary through email. Respondent 1 has confirmed that during the interview and respondent 3 has explained how the order department sends an order to a special email to the technical department for configuring the phone. Thus it is confirmed that there are lot of interdepartmental email exchange happens on daily basis. Respondent 2 has mentioned about the information system Visma where the order and billing related information is stored and processed. The company do not store any information in the web shop. Any order that is made through the web shop is later stored in visma or handled through emails. The company do not manually encrypt any data and could not give any details if encryption is used in Visma or the webshop.

From the interview I found that all the departments of the case company has agreed upon a standard to keep the personal and configuration data for up to 6 months. All the respondents replied that if the customer request the data to be deleted earlier they would do that. If no such request comes from the customer, they data will be deleted after 6 months.
When asked about exactly how much the company is presently complying with the GDPR regulation, the first respondent replied in the form of percentage. According to the respondent 1, the company is complying approximately 80% with the GDPR law at present and the rest is under progress. The other two respondents did not present any number but replied that they are taking the compliance issue very seriously and soon they will try their best to comply with the GDPR. Respondent 1 and 2 replied that the major challenge for complete GDPR compliance is the time factor, respondent 3 answered that the change in the work process to comply with GDPR is a major challenge.

In order to comply with GDPR the case company has already taken up lot of actions over time and updated their work process. Respondent 3 has mentioned one such action in details. Respondent 3 mentioned that prior to the implementation of GDPR all the information was opened to all department. The order department could easily see the configuration related information at the technical department and vice versa. After the introduction of the GDPR, the company has put limitation on who can access what information. There are now two separate views of the customer, where the order department has access to the personal information and the technical department has access to the configuration information. Table 2 summarizes the findings from the interview that was conducted on the employee of the case company.

Table 2: Summary of the interview

<table>
<thead>
<tr>
<th>Area</th>
<th>Respondent 1</th>
<th>Respondent 2</th>
<th>Respondent 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Administration</td>
<td>Order</td>
<td>Technical</td>
</tr>
<tr>
<td>Types of data</td>
<td>Customer's personal and configuration related data</td>
<td>Personal data - Name, Address, Job title, company, personal contact number, email address</td>
<td>Phone's configuration data. Phone number, username, password</td>
</tr>
<tr>
<td>Information system</td>
<td>Server</td>
<td>Visma, Webshop</td>
<td>Email</td>
</tr>
<tr>
<td>Prior to GDPR</td>
<td>Information was open</td>
<td>Had access to configuration related information</td>
<td>Had Access to order information</td>
</tr>
<tr>
<td>After GDPR</td>
<td>Limiting access, so only the right person has the access to the data that he or she is responsible to handle.</td>
<td>Employee at the order department has access to the customer and order related information only.</td>
<td>The technical department can access only the configuration related information of the customer’s products.</td>
</tr>
<tr>
<td>How long data is stored</td>
<td>All data related to customer is deleted after 6 months.</td>
<td>The data is deleted after 6 months if the customer does not request to delete earlier</td>
<td>The configuration info is deleted after 6 month</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Compliance</td>
<td>80 %</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Challenge</td>
<td>Time and work process</td>
<td>Work process</td>
<td>Work process</td>
</tr>
</tbody>
</table>
Chapter 4 - Analysis

Reviewing the first principle of GDPR as stated in Section 2.1, it is known that, when collecting information about a person, the person must be informed. The company must mention that it collects personal information, what information is specifically collected and why would the company need to do it. If the company shares this personal information with others, it must be clearly stated in the policy and informed to the person whose data is being collected (GDPR Article 15). The case company is in the process of updating its privacy policy which will be published on its website giving a clear information what data is collected and how it is used. In addition to it the purpose of data collection is also clearly stated during the contract paper that is signed with the customer.

Clause C of article 5 in GDPR states that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed referred as data minimisation according to the GDPR. The result from the document and interview shows that the case company is complying with this principle by storing only the relevant information required to establish a business deal with its customer. The personal information that the case company is storing regarding its customer are, the first name, last name, phone, email, position of the person in the company and product delivery address. The email and delivery address do not necessarily have to be personal rather in most cases it is the work email of the employee provided by the company. A background and credit check on the customer’s company is made to ensure the safety and affordability state of the company for financial matters. When billing, the case company bills to the customer’s company. Therefore the case company do not need to store any additional personal information such as personal identification number, gender, home address etc. of the customer.

The first paragraph of Article 33 of GDPR states that “In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it”. The incident plan document, as shown in Section 3.1.3, describes how the case company is complying with Article 33 of GDPR by informing and storing any data related incident. From the interview Respondent 1 informed that the case company is interested in developing an incident database where all incidents will be stored. The template of this database will closely follow the incident document template that the company presently have. A incident database would give the company more efficiency in handling incidents compared to document based system.

Form the interview result in Section 3.2 it can be clearly establish that one of the major actions that the case company took in order to comply with GDPR is to limiting the access to the personal data. Clause (f) in Article 5 of GDPR states that the personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (integrity and
In section 2.5 I have also provided the definition of integrity and confidentiality. Thus it can be established from the result that the company has taken necessary steps to ensure the confidentiality of the data by giving the right access to the right person (employee) only. At the present scenario the case company designed the access limitation in the following ways as shown in Table 3.

Table 3: Limiting access to data in various information system. Source: The Author

<table>
<thead>
<tr>
<th>Information system</th>
<th>Description</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The documents stored in the server are stored in a proper directory structure.</td>
<td>Three level of password protection is implemented to secure the server and the documents. Access to the server’s login, the directory and the document itself is protected by user id and password</td>
</tr>
<tr>
<td>Email</td>
<td>The company has separate email addresses for handling separate areas where only the responsible person has access to the email</td>
<td>Only the company emails are used. For inter departmental email exchanges necessary care is taken so that personal information is not included in the email body if not required.</td>
</tr>
<tr>
<td>CRM System</td>
<td>The CRM system that the company uses have its own access settings that has been configured to give right access to the right user.</td>
<td>Access are granted according to the role of the employee and configured accordingly. To access the CRM the user has to log in to the system and system recognizes what action the user can perform in the system</td>
</tr>
<tr>
<td>Webshop</td>
<td>Orders can be placed in the webshop.</td>
<td>The articles can be browsed for description and images, but to place an order the customer need to log in using a id and password that is only provided once a contract is made with the customer.</td>
</tr>
</tbody>
</table>
During the interview Respondent 1 has expressed the interest to developing a cloud based software application for handling customer’s information in near future. As stated in section 2.7 any software system that stores and processes data, a database of some sort is used at the backend. In most of the DBMS the access to this data can be controlled by granting the appropriate privilege to the appropriate user of the database. The common access includes viewing, adding, editing and deleting data. If the case company decides to design a database for developing the software application, a role based access model as shown in Figure 6 can be implemented to limit the access to the data.

![Role based access model](image)

Figure 6: Role based access model. Source: The Author

As I suggested in figure 6 a role based access model that create all the necessary permissions that the user in that role will have. After the permission is set, one or multiple users are assigned to a role. In the above example the users with Technical Role will have access to all the permission for handling configuration related information, however they do not have the permission to completely view, add, edit and delete customer information in the database. On top of it techniques such as pseudonymisation and anonymization can be applied to increase the security. This model can be adapted as a part of privacy by design (pbd) when developing the software system the case company wish to develop.

Literature studies in Chapter 2 show that a person’s name and a company email address may clearly identify a particular individual and is therefore considered as personal data. If personal data is exchanges in emails, it should therefore be included in the company’s list of personal data processing and therefore should comply with GDPR. Therefore It is recommended by various sources not to use email to process personal data in the long run, in order to make it easier to comply with the GDPR. It may therefore be important to move certain information from the email to a more appropriate system, such as a CRM or an ERP.
The case company follows this procedure by moving the personal data from their email to appropriate document in their server or the customer management system they are using. During the intern departmental email exchanges the company sends personal information to only those who need the information for their work. In order to ensure security and privacy, the email are deleted on a regular interval. Most of the email application comes with the option to encrypt the content of the email. The case may use encrypted email (if they do not do it) to exchange privacy-sensitive data.

Clause (e) of article 5 in GDPR states that the personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In order to comply with this regulation the case company has decided to store the personal data for 6 months and remove it, unless requested by the customer to remove them earlier. The is done by removing

1. All the incoming emails
2. All outgoing email
3. Documents in the server
4. Personal information stored in Visma

According to Respondent 1, Time is the first challenge that the company faces to comply with GDPR. Respondent 1 thinks that the complete compliance will take a lot of time to achieve. The company is attracting customers and new data are generated on regular basis. The case company is small in size and do not have a full time employee who is in charge for implementing GDPR. Rather each employee has to take the GDPR into consideration for their daily activities. The company is getting help from Datainspektionen and conducting meetings to strengthening knowledge about GDPR among the employees.

The second challenge faced by the case company for compliance is the changes it made to its old way (prior to the introduction of GDPR) of work process. The company has now put a limit on the access to the data as a result the technical department has to sometime request the order department for additional data (if they require) to configure customer’s product and deliver them. It also takes some effort to erase the personal data completely from the system as it is spread over different places such as the server, email, CRM etc.

From the literature studies, document analysis and the interview, the following actions can be established as a proper guideline towards managing personal data in information system in compliance to GDPR.

1. Customized settings in the operating system, email and CRM system so that the amount of personal data collected or processed is minimized.
2. Features to delete data that can no longer be processed.
3. Limiting access so that only those who need the tasks to perform their work have access.
4. Strong authentication to access an information system to process personal data.
5. Protection of personal data through encryption.
Chapter 5 - Conclusion

GDPR requires organizations to protect personal data through relevant organizational, administrative and technical measures. In order to comply with the regulation, organizations that process personal data must always have a legal basis for handling the data. GDPR imposes strict requirements on transparency. In general it can be said that personal data privacy is desired by everyone and even though it could take some effort and time to comply with the GDPR, companies handling personal data should take all possible and relevant measures.

5.1 Case company’s technical measures to comply with GDPR

To answer my first research question, that is, ‘How does the case company handle their customer’s data in the information system from order to delivery in compliance to GDPR?’ I have presented the technical actions and measures the case companies undertook in Chapter 3 and the result was analyzed in Chapter 4. In conclusion, the case company took the following technical measures to handle their customer’s data in the information system in compliance to GDPR,

1. The CRM system that the company uses is customized so that the personal information is only accessible to the person it is required to. This separation of ‘who’ has access to ‘what’ is strictly maintained by the case company after the introduction of the GDPR.
2. The company maintains a local server to store all documents that can be accessed only from within the company. Employees need authorization to access the directories in the server which is protected by user id and password.
3. The company has created specific email address for inter-departmental email exchanges. The inbox, outbox and sent folders are periodically erased to remove any personal data that can persist in the body of the email.
4. In order to minimize the handling of personal data, the company gives access to its webshop only to the regular customers and retailers. Once a contract is finalized with a customer, he or she gets to create an account and order the products from the webshop. Regular visitors can see product description but cannot place any order.
5. Any data related incident is recorded in a word document and kept in a specific directory in their local server. This word document will be replaced by a custom incident database so any incident can be tracked and responded faster.
6. The company is in the process of updating their data privacy policy (at the time of writing this thesis paper), clearly mentioning what personal data they collect and how they use this data. The policy will be put as a new page in the website and a link will be given in the footer area.
7. All personal data is periodically deleted when it is no longer required. This includes deleting document from server, deleting record from the CRM system, deleting user account in the webshop and deleting of email.
5.2 Challenges faced by the case company to comply with GDPR

The answer to my second research question, that is, “What are the technical challenges faced by the case company in handling customer’s data to comply with GDPR.” can be found partly in the interview summary in Section 3.2 and the latter part of the Analysis chapter. In conclusion, the two major challenges are time and legacy. The first challenge is time, because a small sized company cannot set off one staff to deal with everything related to GDPR but instead everyone has to take this regulation into consideration. It takes time to improve the knowledge among the staff and gain the skill. It also takes time to convert this skill into practice.

The second challenge is legacy, because data routines before the GDPR were not strict, as a result, personal data were scattered across different hardware and software within an organization. Lack of protection and maintenance posed security risk to these personal data.
References:


Skatteverket (2018) Personnummer och samordningsnummer https://www.skatteverket.se/privat/folkbokforing/personnummerochsamordningsnummer.4.3810a01c150939e893f18c29.html

Starman A. B. (2013) The case study as a type of qualitative research, Journal of Contemporary Educational Studies 1/2013, 28–43


World Economic forum (2011) Personal Data: The Emergence of a New Asset Class, Online, Accessed 2018-10-21


http://home.utah.edu/~u0326119/Comm4170-01/resources/Interviewguidelines.pdf
Questionnaires to Respondent 1 (Manager of Talk Telecom)

1. When do you need to store data related to a person and how is it stored?
   “A part of the personal information that we often handle is stored in the customer management system. Then there are handling of personal information involved during the configuration process (of the actual device) and delivery process.”

2. What type of personal data does your company deals with?
   “We mainly store customer’s personal information and product’s configuration information in our company”

3. What software / platforms do you use to manage and access the personal data?
   “Mostly the data is managed and handled in information system like Visma, during the order process and in CRM system for customer relation management. Also we use Email a lot to communicate and transfer personal data.”

4. How is the access to these software / platform distributed and managed?
   “We have already set up a process where we have defined the rules on who can access what. The goal is to give the necessary permission only to the people in charge”

5. How long do you keep the personal data into the system that you used?
   “If the customer do not place any request to delete the data we will save it for 6 months into our system”

6. Do you have an up-to-date privacy policy that your customers can view?
   “It is under progress, we have come almost finished two third of our privacy policy.”

7. How much you are compliance with GDPR in your company at present?
   “We have completed around 80% done, it is taking finish up the rest. I believe that we may never be 100% compliance with GDPR, as the big companies we work with have very big and custom requirements on GDPR.”

8. What issue is Talk Telekom facing when you are applying GDPR in your company?
   “We are a small company and it is taking a lot of time for us to apply GDPR. Time is the biggest issue here.”
Questionnaires to Respondent 2 (Order Department)

1. What is the process when a customer place an order?
“The customer can place an order through email and webshop. Two people in the order department are authorized to handle the order.”

2. What types of personal information do you store while processing Order from the customer?
“In order to process an order our department needs to know customer’s name, job title, company name, organization number, product delivery address, email and phone number.”

3. What happens to the data when the orders are completed / shipped?
“The order information are stored in files at the special folder for 6 months if the customer do not request to delete it. We blocked our webshop for visitors to place an order and is accessed only by the retailers and regular customers who have a login id and password. All the email inbox are emptied everyday as a result any order placed through email is not stored for a long time. We use visma to handle customer information and the customer name, reseller name, order number, articles and delivery address are stored this this system.”

4. How much is your department complying with GDPR now?
“We are trying our best to comply according to the GDPR regulation”

5. What have been done until now so far to comply with the GDPR
“Now we are more confined within the information related to only processing order. For example now, we cannot see the configuration related information of a customer’s phone such as user name, password etc.”

Questionnaires to Respondent 3 (Technical Department)

1. What is the work process in technical department?
“One of the work process at technical department is that we configure customer’s IP telephone which they are using for their daily work. First the order department receives an order on what hardware customer want. And together with this order they also send sensitive information like user credential and password for configuring the phone. We receive a work order from the order department to configure the customer's phone through email to a special email address which only the technical department has access to. The configuration information involves phone number, username and password which is very sensitive and if the wrong person has access to this information, he or she can use this information to make calls and the bill will be sent to the customer it is registered to.”
2. What types of personal information (if any) do you store at your department
   “In our department we deal with the configuration related data. Each phone is configuration
   credential bound to specific user, which personal from user perspective. The configuration
   data involves the phone number, user name, and password. Once the phone is configured
   we send it directly from our department to the customer’s delivery address, therefore we
   need to know the name of the customer and the delivery address”

3. What happens to the data (if any) when the data is no longer needed?
   “There is no rule on how long we will keep the data. But we usually keep the data for 6
   months and then delete it. If the customer requests it to delete earlier, we would do it right
   away.”

4. How much is your department complying with GDPR now?
   “We are not finished yet complying completely with the GDPR but we are on a good way and
   have done quite a lot. It is still a work in progress."

5. What have been done until now so far to comply with the GDPR
   “The primary action that we have taken to comply with the GDPR is to limit access to the
   information. Before the information was open and everyone in the company could access the
   customer’s personal and configuration related information. Now we have limited to only the
   person or people who are responsible to deal with it. For instance now the finance
   department cannot see the technical and configuration related information of a customer’s
   phone.”