GDPR in practice

A guide that is primarily aimed at those who will practically carry out the work

Richard Frank
richard.frank@infotrust.se

Content

1 SUMMARY 5
1.1 Keyword 5

2 ABSTRACT 6
2.1 Keywords 6

3 PREFACE 7

4 DICTIONARY 8

5 INTRODUCTION 9
5.1 Problem statement 9
5.2 Objective 9
5.3 Boundaries 10

6 BACKGROUND 11

7 THEORY 12
7.1 The Archives Act 12
7.2 The Accounting Act 12
7.3 ASSA Abloy and Kommers Advertisement 12
7.4 Personal data 12
7.5 JavaScript 12
7.6 The abuse rule 13
7.7 Privacy by design 13
7.8 RSA – Encryption 13
7.9 C# 13

8 RELATED WORKS 14

9 ANALYSIS OF THE GDPR 15
9.1 General provisions 15
9.2 Principles 15
9.3 Rights of the data subject 16
9.4 Data Controller and Data Processor 17
9.5 Transfer of personal data to third countries or international organisations 18
9.6 Independent regulators 18
9.7 Cooperation and consistency 18
9.8 Remedies, Liability and Sanctions 18
9.9 Provisions on special processing situations 19
9.10 Delegated acts and pace of implementation 19

10 METHOD 20
10.1 Strategy for the survey 20
10.2 Interviews 20
10.3 Technical implementation 20
10.4 Economic analysis 20

11 SUPPLIER REGISTRATION IN KOMMERS 21

12 RESULT 22
12.1 Definition of personal data 22
12.2 Interviews 22
12.2.1 Training, awareness, personal data identification and consent 22
12.2.2 Risks, incident management and backup 23
12.3 General plan for implementation of GDPR 23

12.3.1 Phase I - Preliminary investigation 24
12.3.2 Features and processes 24
12.3.3 Personal data 24
12.3.4 Consent 24
12.3.5 PHASE II – Risk analysis 24
12.3.6 PHASE III – Implementation content 25
12.3.7 Appoint a Data Protection Officer 25
12.3.8 Appoint a data processor 25
12.3.9 New data protection practices 25
12.3.10 Documents that need to be produced/updated 25
12.3.11 Request for a register extract 26
12.3.12 Education 26
12.3.13 Deletion routines 26
12.3.14 Transparency towards the customer (create a transparent user interface) 26
12.4 Implementation checklist 26
12.5 Implementation of solution proposals in Kommers 27
12.5.1 Phase I – Preliminary investigation 27
12.5.2 Phase II – Risk analysis 27
12.5.3 Phase III – Content of implementation 27
12.6 Technical implementation in a test environment 28
12.6.1 Vendor User Registration 28
12.6.2 Technical solution 28
12.6.3 Storage of personal data 28
12.7 Investigation of the economic impact of an implementation 29
12.8 Cost calculation company X 30

13 ANALYSIS AND DISCUSSION 33
13.1 Definition of personal data 33
13.2 Interviews 33
13.3 General plan for implementation 33
13.3.1 Phase I 33
13.3.2 Phase II 34
13.3.3 Phase III 34
13.3.4 Technical solution 34
13.3.5 Encryption 35
13.4 Financial calculation 35
13.4.1 Scenarios 36
13.4.2 Scenario 1 - Implementation of encryption features only 36
13.4.3 Scenario 2 - Only implementation of change for the Terms of Service acceptance 36
13.4.4 Scenario 3 - Implementation of both solutions 36
13.4.5 Cost comparison with cost calculation for companies X and Y 37
13.5 Durability 37

14 CONCLUSION AND RECOMMENDATIONS 38

15 REFERENCES 39
15.1 List of references 40

16 ATTACHMENTS 42
16.1 Appendix A - Checklist for implementation of GDPR 42
16.2 Appendix B – Create supplier account (before implementation) 44
16.3 Appendix C – Database structure for registering new supplier account 45
16.4 Appendix D – Results of implementation for approval of contract terms 0
16.5 Appendix E – RSA Encryption 0

1 Summary

With the new General Data Protection Regulation (GDPR) in the EU, there are higher requirements for the handling of personal data and for the first time, companies risk sanctions if they do not handle personal data correctly, which means that all organizations must take a position on how personal data should be handled within the organization. In the IT sector, an analysis must be carried out on what data will be affected with the introduction of GDPR and how data should be handled in current IT systems.

The new GDPR and related work have been studied together with interviews conducted at various companies to produce a solution proposal. The proposed solution has then been used in an implementation test in ASSA Abloy's system to show that it works. The survey also includes a financial analysis to determine the importance of managing and prioritizing implementation.

The solution proposal that the survey developed has had a proven effect in the system and can be reused with relatively few resources to ensure that an organization takes sufficient measures when implementing GDPR.

1.1 Keyword

Personal data, Privacy, GDPR, General Data Protection Regulation, Information management

2 Abstract

As a result of the new General Data Protection Regulation (GDPR) in the EU, there are stricter requirements for handling personal data. For the first time, companies risk sanctions if they fail to handle personal data properly, giving rise to a wide spectrum of impacts. In the IT sector, an analysis must be undertaken to determine which data will be affected by the introduction of GDPR and how this data can be managed in current IT systems in order to meet the new requirements. Against this backdrop, this study was con- ducted at ASSA Abloy, a purchasing and electronic trade company located in Stockholm.

A proposed solution was developed by studying the GDPR, related works and the results from the interviews which was conducted in this study. The proposed solution was then tested on a selected part of one of the company's systems. Furthermore, this study presents an economic analysis to determine the significance of implementing of this solution, which points to a need for such a solution to be prioritized by the company.

Overall, the proposed solution proves to have a positive effect with respect to complying with GDPR and can be reused with relatively few resources.

2.1 Keywords

Personal data, Integrity, GDPR, General data protection regulation, Information management

3 Preface

The work has been carried out at the company ASSA Abloy AB. The purpose of this document was to create a better understanding of the causes and implementation in the business sector.

A big thank you to Christian Hilbertsson who has been a sounding board along the way.
An equally big thank you to my wife who has insistently read the document 100's of times

4 Dictionary

Kommers – Kommers ad is a procurement portal that ASSA Abloy AB has tried to handle, among other things, procurements and tenders.

Directive - A directive is a binding provision that requires the underlying authorities to comply with it.

GDPR - General Data Protection Regulation

Regulation - The regulation refers in this survey to the new data protection regulation, also called GDPR.

Organization - In this survey, which is aimed at both companies and organizations, organization will be used to designate both of these.

Personal data - Data that can directly or indirectly identify a living person. In this survey, personal data is used instead of personal data.

Pseudonymization - "A technology that makes it easier to handle personal data in terms of security. Pseudonymisation means that identifying personal data is stored separately from other personal data. By storing identified personal data from other data, it becomes a regulation of security"[1].

(The) Data Subject – The person who has their personal data registered

Data portability – The right to receive an extract of one's personal data for use elsewhere, for example in another media service.

Natural person – An individual and not a legal person.

Big Data – A large amount of stored digital information that it is difficult to process.

Structural capital – Already invested capital in the current organization, e.g. already implemented technical systems that handle personal data.

5 Introduction

The chapter begins with a problem statement that explains the problems that organizations face with the new regulation. The objective of the study is then described, followed by the delimitations of this study.

5.1 Problem statement

On May 25, 2018, the new General Data Protection Regulation will be introduced, the new regulation replaces the old Personal Data Act (PUL), which means a big change for most organizations and companies that must then be ready for this change. The change will include all IT systems, the various files in the file systems and the documents that are on the desktops that contain personal data, in other words all processes where personal data is handled. The new regulation has been created to strengthen the privacy of all private individuals in the EU. The GDPR has been interpreted differently depending on which country has interpreted it, and this has led to the processing of personal data differing greatly depending on the country that made the interpretation. This is a result of the enormous technological development that has taken place since the Personal Data Directive was introduced in 19952. As it looks today, organizations save personal data by users agreeing to long user agreements that are often very unclear, for what purpose and how the personal data will be used is not clear to the data subject. It is not uncommon for the data to be stored insecurely and sold on to other players in the market without the data subject having any control over it.
As mentioned, companies are faced with the challenges of handling private individuals' personal data correctly according to the regulation, how this should be carried out and what the cost will be financially for the companies concerned for implementation and possible sanctions, these will be the big questions in this survey.

5.2 Objective

- What is personal data
- The goal is to be able to demonstrate this and whether this personal data can be divided into different types or risk groups.
- Develop a general plan for how data should be handled to meet the requirements of the regulation
- Produce a general plan on how an implementation of the regulation can be carried out. Describe this in a process with phases and an explanatory text on what will happen in the different phases.
- A general specification for how an implementation can be carried out
- To develop a checklist as a complement to the general plan in the point above, which can then be followed when implementing the regulation.
- Show in a test environment that the implementation is working
- ASSA Abloy AB provides a test environment in their procurement system Kommers, in this test system the goal is to prove that an implementation can be done in a real environment.
- Examine the financial impact that an implementation creates
- The goal is to make an analysis that shows what the cost of a technical implementation that takes place in connection with this investigation would amount to. Then make a comparison against not implementing these changes and through this evaluate whether the financial aspect can show what is best for the organization to do.

5.3 Boundaries

Implementing GDPR throughout ASSA Abloy's organization is too extensive for this survey. The delimitation will therefore be to discuss how the solution proposal developed in this survey can be adapted to their organization, but also to analyze one of their processes and to implement technical measures to ensure that the process meets the requirements that come with GDPR. The process to be analyzed is "create new account" in the system Kommers. The delimitation also applies to the financial analysis that will be done on the cost of implementing the technical aspects of the process of creating new accounts. That cost will be compared with what the cost may be as a consequence of not taking sufficient measures to ensure the personal integrity of customers.

The survey has been carried out at a smaller organization within the group, because of this, the proposed solution is aimed at smaller organizations, which does not mean that the solution in this survey cannot be used for authorities, hospitals and companies that engage in research.

6 Background

GDPR is the new General Data Protection Regulation that as of May 25, 2018 replaces the current Personal Data Act. Unlike the Personal Data Act, the GDPR is a regulation and not a directive. A regulation means that everyone who is part of it must comply with the new rules and implement them in the manner set out in the regulation3. The GDPR is introduced, among other things, because the members of the EU want the free information to flow freely but controlled between companies, organizations and authorities, but at the same time protect the data subject's personal integrity [1].

The new regulation has been developed together between the member states to have a common regulation that will look the same in all countries. The current directive is not only old, it is also only a directive, which has led to all member states implementing it in different ways, which has created a big difference in how personal data is processed. The Personal Data Act was introduced in 1995 and since then the world has changed enormously with technological advances and the internet's entry into the lives of private individuals. This has caused the law to lose both power and function, and according to Colin Tankard, as little as one percent of the world's population used the internet in 1995 [1]. This figure compares to figures from Unstats which say that 43.75% used the internet in 2015 [4].

7 Theory

This chapter presents areas that this survey touches on in addition to the new General Data Protection Regulation. Each sub-chapter contains a general explanation of the topic to create an insight into what this means in order for the reader to gain an understanding of this when it is mentioned in later parts of the report.

7.1 The Archives Act

The Archives Act deals with, among other things, how long procurements need to be saved after a contract has been procured. If a person requests deletion of their personal data under the right from the GDPR, the company still has the obligation to deny this deletion if the Archives Act states that the information must be retained5.

7.2 The Accounting Act

According to the Accounting Act, accounts must be kept for seven years after the calendar year in which the financial year ended6. This means that much of the personal data that is stored must be stored for the same period of time as this data is needed for the accounts to be complete.

7.3 ASSA Abloy and Kommers Advertisement

ASSA Abloy has been developing solutions in purchasing and electronic commerce since 1998. With Kommers, a turnkey solution is offered for procurement, purchasing, contract management and e-commerce. Kommers Annons is a portal for suppliers who want to find ongoing procurements, submit tenders and manage e-commerce7.

7.4 Personal data

The Swedish Data Protection Authority has defined personal data as follows: "All kinds of information that can be directly or indirectly attributed to a natural person who is alive is counted as personal data according to the Personal Data Act. Images (photos) and sound recordings of individuals processed in computers may also be personal data, even if no names are mentioned. Encrypted data and various types of electronic identities, such as IP numbers, are considered personal data if they can be linked to natural persons"[8]. The Swedish Data Protection Authority has also listed what is considered sensitive personal data according to the General Data Protection Regulation9:

- Racial or ethnic origin
- Political views
- Religious or philosophical beliefs
- Membership in a trade union
- Health
- A person's sex life or sexual orientation
- Genetic and biometric data that uniquely identifies a person

7.5 JavaScript

JavaScript is a cross-platform and object-oriented language, it is mainly used to develop web pages. JavaScript can be used, among other things, to create iterative and dynamic content for web pages, such as toggling ads or hiding certain parts of a web page10.

7.6 The abuse rule

At the time of writing, the processing of personal data is regulated by the Personal Data Act. The Personal Data Act protects individuals from their personal data not being used or disseminated without permission. In this Act, there are exceptions on how personal data can be used for certain purposes such as publications, which are protected by the Freedom of the Press Act or the Fundamental Law on Freedom of Expression, i.e. radio, newspapers, television, films, books and websites with a responsible publisher do not need to apply the Personal Data Act11 [12]. But they must comply with the Freedom of the Press Act and the Fundamental Law on Freedom of Expression13. Another exception is the abuse rule, which states that personal data in unstructured form (in liquid text) may occur as long as they do not violate personal integrity.

7.7 Privacy by design

Privacy protection refers to the principle of taking in only the information that is needed and nothing more, not storing data longer than necessary and not using the data for more than the purpose for which it was collected. It is also about obtaining consent from the data subject to process the personal data for the purpose for which it has been collected and being transparent about how the processing of the personal data will take place.

Privacy by design is based on the principle of highlighting privacy issues at the beginning of the process when developing an IT system or an IT solution. By highlighting the issue of privacy protection early in the process, you can take into account the laws and requirements that are set to protect personal privacy and thus eliminate the risk of ending up in expensive pitfalls, examples of privacy issues that can be addressed early and integrated into the system can be[14]:

- Minimize the amount of personal data processed
- Access to personal data is restricted
- Transparent user interface for the registered customers so that it gives the data subject visibility into how their personal data is handled
- Protect personal data from unauthorized persons

7.8 RSA – Encryption

RSA encryption is a secure and proven encryption algorithm that is easy to understand and relatively simple to apply. It uses an asymmetric encryption, which means that it uses a public key to encrypt a text and this text can only be decrypted with a private key. This allows the encrypted text to be signed to guarantee that it is decrypted by the correct recipient[15 16].

7.9 C#

C# (pronounced C-Sharp) is a programming language developed by Microsoft to run on the .NET framework17 [18]. C# is a cross-platform programming language, which means it can run on multiple operating systems. Some different types of programs developed with C# can be console programs, Windows applications, and web applications.

8 Related Works

Some reports and articles that touch on the topic in this report have been studied to get additional perspectives on how the GDPR has been interpreted, by others to develop a general solution for how companies should handle the GDPR. Initially, the question of what challenges the organization faces with the introduction of GDPR is addressed, it then goes on to study other perspectives on how the problem of the removal of the abuse rule can be handled. The chapter concludes with related work on how companies perceive the changes, how these changes should take place and what preparations are required for these.

Colin Tankar writes an article about GDPR and its implications for organizations [1]. He writes about how GDPR imposes stricter rules on the organization to protect personal privacy. That this was a necessary change as the previous law for handling personal data is different depending on which country interpreted the law. He also writes that this places higher demands on data protection for the organizations and gives a brief guide on what the organizations need to look at in order to adapt to GDPR. This is something that Steve Mansfield-Devine also writes about in the article "Meeting the needs of GDPR with encryption", Steve writes about how companies are thinking about adapting to GDPR and possible solutions to this [2]. Henrik Månsson and Joey Erichsen write in the report "Compliance with GDPR" about the biggest technical challenges companies face with the introduction of GDPR, they also write about the challenges that arise when developing new technical functionality and implementing this in current systems [3].

An article written by Lawrence Ryz and Lauren Grets "A new era in data protection" is more focused on how a person is identified through data and what exceptions there are to sharing this data with a third party [4]. Since the article is based on how GDPR will affect e-discovery, they also write that handling data in liquid text will be a tough task as there are no exceptions in GDPR for this. Paula Lundholm and Sandra Adolfson also write in their case study "Retail's preparations for GDPR" about data in liquid text, they have interviewed different companies where they asked about how they should solve this issue [5]. It shows that there is a lot of concern about data in floating text and how to solve this, only one of the interviewed companies had an idea of how to handle this. In the article "The GDPR and Big Data: Leading the way for Big Genetic Data?", Kärt Pormeister writes that the risk of collecting large amounts of personal data was identified long before the directives with GDPR were developed. He also writes about how GDPR will affect Big Data [6].

In a report written by Maja Brädefors and Julia Petterson, they examine the question "How do companies perceive the changes that GDPR entails and how do they proceed with the preparations for the new law?" [7]. They write about what GDPR means and what change processes can look like in companies. They have also interviewed companies about this, analyzed and compared their answers to see how the different companies solve the issue of GDPR. It is also written about preparations for GDPR in the article "The Year of the GDPR" written by Kim Smouter, in that article Kim mentions three important steps that should be taken into account when adapting to GDPR and complements this with a checklist for adapting to GDPR [8] [9].

Another measure that is talked about a lot is privacy by design, to highlight the issue of privacy protection early in the process. This is something that Harald Gjermundrod, Ioanna Dionysiou and Kyriakos Costa write about in an article where they also write that there is no clear framework for implementing this [10].

9 Analysis of the GDPR

A survey on the General Data Protection Regulation in its entirety, the survey has been divided into chapters in the same order as the text of the regulation is divided. The parts of the GDPR that are considered most important for the project are shown and explained here. The references are to linked parts of the regulation, but specific chapters and articles will be mentioned if necessary [11].

9.1 General provisions

This chapter of the GDPR explains briefly how the regulation is intended to be used and how it should be used depending on the type of person, company or organization that the issue concerns. Article 1 states that the regulation is intended to lay down rules for how the processing of personal data is to be carried out and how the free flow of personal data is to take place. The first chapter of the Regulation, Article 1, states, inter alia, that, "This Regulation protects the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data"[20]. The remaining parts of the Regulation explain the scope and definitions.

Conclusion: Explains how the Regulation is to be used by stakeholders and for what purpose it has been introduced.

9.2 Principles

Personal data collected for specific purposes shall be processed in a lawful, correct and transparent manner vis-à-vis the data subject concerned and the purpose expressly stated. It is the defined purposes that set the framework for the processing of personal data. If the personal data is also to be processed for archiving purposes that comply with the Archives Act or the Accounting Act, this is the case for archiving of personal data21

[22.] The personal data collected must be up-to-date, relevant and consistent with the purpose for which it is to be processed. To ensure that the data is accurate, reasonable measures shall be used to ensure that it is not inaccurate. The data subject's data must be stored in such a way that the data subject cannot be identified for a longer period than necessary for the purpose for which the personal data is processed.

The personal data must be processed in a secure manner that protects against unauthorized processing, unauthorized access, loss, destruction or damage by accident. This should be addressed by using appropriate technical or organisational measures. In order for the processing of personal data to be lawful, the person concerned must give their consent and that the data subject's personal data is processed for one or more specific purposes.

According to the regulation, the processing may be necessary if:

- The parties must enter into an agreement or perform certain actions at the request of the person in question before an agreement is concluded.
- Comply with a legal obligation incumbent on the controller (to be determined in accordance with Union law or the national law of a Member State to which the controller is subject).
- protect the interests of the data subject or of another natural person;
- Perform a task carried out in the public interest or in the exercise of official authority vested in the controller (to be determined in accordance with Union law or the law of a Member State's national to which the controller is subject).
- purposes relating to the legitimate interests of the controller or of a third party, unless the interests or fundamental rights and freedoms of the data subject override and require the protection of personal data, in particular where the data subject is a child.

When collecting personal data for information society services directly from a child under the age of 16, the consent must be approved by a person who has parental responsibility for the child. Data controllers must verify that the consent is approved by the person with parental responsibility for the child.

where personal data are processed for purposes other than the specific purpose for which they were collected which constitute a necessary and proportionate measure to protect the objectives referred to in Article 23(1). Data controllers must prove how the processing for other purposes is consistent with the purposes for which the personal data was collected.

- They shall consider links between the purposes for which the personal data has been collected and the purposes for which they have been further used.
- the context in which the personal data have been collected, in particular the relationship between the data subjects and the controller;
- the nature of the personal data, in particular whether special categories of personal data are processed in accordance with Article 9 or whether personal data
- on criminal convictions and offences are dealt with in accordance with Article 10.
- Any consequences for data subjects of the planned further processing.
- the existence of appropriate safeguards, which may include encryption or pseudonymisation;

The controller must be able to demonstrate that the personal data collected is based on consent and that the person has consented to the processing of personal data. If consent is given in a written declaration, the consent must be explained in a clear and intelligible manner using clear and unambiguous language. The person must be able to withdraw their consent at any time at their own request. This does not affect processing that has already been carried out under the consent of the person.

The processing of personal data revealing race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biothermal data for the purpose of identifying a natural person, data concerning health, or about a natural person's sex life or sexual orientation shall be prohibited unless consent has been given to the processing of these data23.

Conclusion: Personal data may only be collected when there is a need for this and consent has been obtained from the data subject to protect personal privacy. It is the obligation of the collecting party to process the data lawfully, correctly and transparently in relation to the data subject.

9.3 Rights of the data subject

The rights of the data subject have increased with the introduction of the GDPR. The main part is that the natural person must be informed in a simple and easy-to-understand way about how the various personal data is stored, why, how long it is to be stored, who is responsible for the processing of the personal data and what opportunities and rights the data subject has in the handling of the personal data provided. The data subject also has the right to access the personal data the organisation has about the data subject, rectification and deletion, the right to restrict the processing of the personal data and the right to data portability. In addition to these rights, there are several additions on how the natural person's data is to be handled and in which cases these are applicable24 [25] [26] [27] [28].

Conclusion: The data collecting actor must clearly and simply demonstrate that the data subject knows how and why the personal data is stored. The data subject must also be informed of the possibilities available to them for the processing of personal data.

9.4 Data Controller and Data Processor

According to the Regulation, a controller is 'a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'[29]. The data controller is responsible for ensuring that all personal data is handled in accordance with the regulation that exists. It is responsible for ensuring that the technical and organisational changes are required and that the organisation and the employees understand the importance of the processing being carried out in the manner decided by the data controller. The controller is also responsible for ensuring that this is continued to be followed and updated as necessary. In order for the controller to be able to demonstrate that it has fulfilled its tasks, there are various codes of conduct and certification mechanisms that may be used to demonstrate compliance with the applicable rules, according to Articles 40 and 42.

If the organization meets any of these requirements, it is the data controller that is obliged to establish a register of the personal data processing carried out:

- The company has more than 250 employees
- Is there a risk to the rights and freedoms of the data subject
- That the treatment is not temporary.

The Data Processor is a natural or legal person appointed by the Data Controller to handle the Data Controller's data in accordance with the given guidelines. This must be regulated in the agreement and be well specified. In order to be appointed, a processor must be able to guarantee the technical and organisational security required for the type of personal data to be processed30.

The Data Protection Officer is appointed by the Data Controller and the Data Processor if any of these three issues apply to the organisation31:

1. Are you a government agency or an elected assembly, i.e. a public body?
2. Do you have as your core activity the regular, systematic and extensive monitoring of individuals?
3. Do you have as your core business to process sensitive personal data or information about crime on a large scale?

The Data Protection Officer's task is to monitor the organisation's full compliance with the GDPR. To be available to the controller and processor to advise on data protection impact assessment. The Data Protection Officer cooperates with the supervisory authority and acts as a contact when the supervisory authority needs information from the organisation.

Conclusion: The controller is obliged to prove compliance with the Regulation even if it has signed an agreement with a processor that handles the actual processing of personal data. To be able to explain to the data subject what personal data is being processed and the purpose of the processing, and that these are secured against infringement. A data processor handles the data controller's data in accordance with the regulation and the agreement between the two parties. The Data Protection Officer on the occasions when such a regulation is required monitors that the organisation complies with the Regulation and acts as a communication link between the Data Protection Authority and the Data Controller or Data Processor

9.5 Transfer of personal data to third countries or international organisations

In order for personal data to be transferred to a third country or an international organisation, the European Commission must decide that they have ensured an equivalent level of protection in the matter, in which case the transfer should not require any special authorisation32. The Commission will also monitor developments in third countries and international organisations, which may affect decisions taken in the past. In the following situations, the transfer of personal data to third countries or international organisations may take place on the condition that the rules in the Regulation are complied with.

- Appropriate safeguards
- Special permission from the Swedish Data Protection Authority
- Consent or in other specified situations
- Occasional transfer

Conclusion: For the transfer of personal data to a third country, consent does not need to be obtained if there is an equivalent level of protection or the requirements for one of the four exceptions above are met.

9.6 Independent regulators

Each Member State shall designate one or more independent authorities responsible for the application of the Regulation in order to protect the rights of the individual by supervising those who process the personal data and that they do so in accordance with the GDPR. The supervisory authority must communicate risks, rules, protective measures and rights about how processing is to be carried out. They must also warn and order organizations to take action when processing personal data, they can also restrict or prohibit the processing of personal data by organizations and decide on sanction fees. The supervisory authority may also provide individuals with information about their rights under the Regulation.

Conclusion: Each Member State must designate one or more authorities that are obliged to enforce the Regulation by communicating the Regulation and monitoring its compliance.

9.7 Cooperation and consistency

Cooperation refers to most types of cooperation, but above all it is about the supervisory authority cooperating together with other countries' supervisory authorities in a quick and smooth manner and with the organisations or persons who have some form of contact with the supervisory authority. The supervisory authority must assist with communication between the supervisory authorities of the different countries and they must also communicate with the organisations or persons who have opinions on the handling of personal data.

Conclusion: The supervisory authority is obliged to handle communication between supervisory authorities and organizations or persons, they must act as an intermediary.

9.8 Remedies, Liability and Sanctions

According to Chapter VIII, Article 77, any natural or legal person who considers that his or her personal data has been wrongly processed has the right to lodge a complaint with the supervisory authority responsible for the Member State where the complaint relates, usually the supervisory authority located in the person's country of residence. Communication between the supervisory authority and the person in question regarding the ongoing case shall be handled by the supervisory

authority on the progress of the case. The supervisory authority is responsible for the type of sanction that a controller or processor can be imposed depending on the type of violation that has occurred. This is particularly in accordance with Article 83 in conjunction with Article 58(2). Sanctions can range from warnings in advance that a violation of the regulation is likely to occur in view of some kind of change, to penalties of up to €20,000,000 or 4% of global annual turnover. There are both lower sanction fees and only reprimands in the penalty scale. It depends entirely on the nature of the infringement, the magnitude of the infringement, the measures taken in advance to prevent it and a number of other assessments that can be made under Article 83 of the Regulation, both aggravating and mitigating.

A person who has suffered harm in any way due to an organization's handling is entitled to compensation according to Article 82 depending on the situation and event, this from the data controller or the data processor or both.

Conclusion: The supervisory authority has an obligation to ensure that reported complaints are handled and controlled. If errors in the processing have occurred on the part of the controller, the supervisory authority shall punish the controller in accordance with the Regulation.

9.9 Provisions on special processing situations

Certain situations require special processing of personal data for the performance of certain purposes, Member States must develop special provisions, i.e. exceptions or deviations depending on the situation. These processing situations have been divided into the following areas and they have their own specific exceptions that must be achieved for the processing of personal data33.

- Freedom of expression and information
- Public access to public documents
- National identification numbers
- Employment relationships
- Safeguards and exceptions to processing for archival purposes in the public interest, scientific or historical research purposes or statistical purposes
- Professional secrecy
- Existing rules on data protection in churches and religious communities

Conclusion: The regulation has some exceptions as there are laws that are stronger, these exceptions are extremely important to handle and control.

9.10 Delegated acts and pace of implementation

The right to receive delegated acts referred to in Article 12(8) and (8) shall be conferred on the Commission from 24 May 2016. When the Commission receives a delegated act, they shall inform the European Parliament and the Council. That power may also be revoked by the European Parliament or by the Council, which means that the power ceases to apply on the day following its publication in the Official Journal of the European Union or on a given date.

10 Method

This chapter describes the different steps of the investigation to provide a deeper explanation of how the work has progressed and what methods have been used throughout the investigation. The chapter starts by explaining the type of method that has been chosen for the study and then continues and describes the interview method and finally describes the implementation of the technical implementation in the study.

10.1 Strategy for the survey

The chosen method for this study is a qualitative case study that Alan Bryman writes about in Social Research Methods [12]. This method makes use of several data collection methods such as interviews, observations, and document analysis to collect data to be analyzed in order to gain a deep understanding of the topic of the survey. Based on this, interviews, literature surveys and participating in seminars were chosen as methods to collect data for this study. The methods for collecting data were chosen as the largest source for this survey is the Swedish Data Protection Authority and the regulation text for the new data protection regulation. After careful analysis of the new regulation and various interpretations of it, a proposed solution was developed as a result of the study. Then two different organizations were interviewed and then compared the solution proposal with the results from the interviews, which were based on how other organizations have solved the same issue in their fields. Finally, part of the solution was implemented in Kommer's system, which is shown in chapter 8 and discussed in chapter 9.

10.2 Interviews

The interviews were intended to be used as research material in the survey and to compare solutions at other organizations with the results of this survey. It was then important to gain a deep understanding of how other organizations have interpreted GDPR and what solutions they have to implement it in the organization [13]. The chosen interview method for this study then became a semi-structured interview methodology that involves preparing questions before the interview and follow-up questions being adapted depending on the answer the interviewee gives. By using a semi-structured technique, it opens up for the interview to be a more natural conversation and the follow-up questions that are adapted to the answer given provide a more in-depth answer to the original question asked. This provides a certain structure so as not to end up in the wrong direction during the interview, while at the same time giving the interviewee the opportunity to speak freely about the questions that are asked.

10.3 Technical implementation

The process in Kommers that the study deals with was carefully analyzed and a model of this process was created together with ASSA Abloy. This was done to create an understanding of what happens in the process and how personal data is handled in the organization and in the system. Alternative solutions for how GDPR can be implemented in this process were then discussed, and then when a decision was made regarding a solution, it was implemented in the system.

10.4 Economic analysis

Cost calculation for the implementation and a cost calculation where an implementation has not been made. A comparative analysis has been made on these two cost calculations. Tables have been created to be able to show a result that has later been freely discussed depending on which scenarios could have been predicted through a workshop together with ASSA Abloy.

A comparison of this cost calculation has been carried out with a company, hereinafter referred to as company X, which is significantly more established in the market and larger in the number of employees. The cost calculation used from company X is not on the entire implementation of GDPR

at the company, but it is limited to a similar implementation that this report handles. Company X has several projects running in parallel and the costs of these projects are very similar.

An interview with company Y has also been carried out where a comparison was more difficult to make as they had taken a larger approach and not divided it into equally small systems. Company Y talked more about how the cost of GDPR is extremely individual as the already invested structural capital differs greatly between companies. According to company Y, a company that has handled the Personal Data Act in a good way already has a lot of the administration and most of the systems ready for GDPR. This entails a lower cost for the introduction of the changes to the GDPR. This makes it difficult to compare the costs of different companies.

11 Supplier registration in Kommers

This chapter explains the process in Kommers that this study analyzes. It describes how a registration of a supplier account in Kommers is done before the implementation of GDPR has been implemented.

Registration

When a supplier wants to join Kommers, they use a registration function on the website. This function is illustrated below in Figure 7.1 and Appendix B shows how it looks in the system. A user enters the homepage and chooses to start a registration process. The three different steps in the process are "Receive request", here the user enters their details and then clicks register. The next step is "Accept terms & conditions" which checks that the user has accepted the current agreement, which is a requirement for the user to be allowed to register. When this step is completed, the data subject's personal information is stored in the database, see Appendix C, here it is shown that only the password is encrypted in the database. The third and final step in the process is "E-mail confirmation" which handles an activation email that the user must approve, this step is performed to check that it is the right person trying to create the user account.

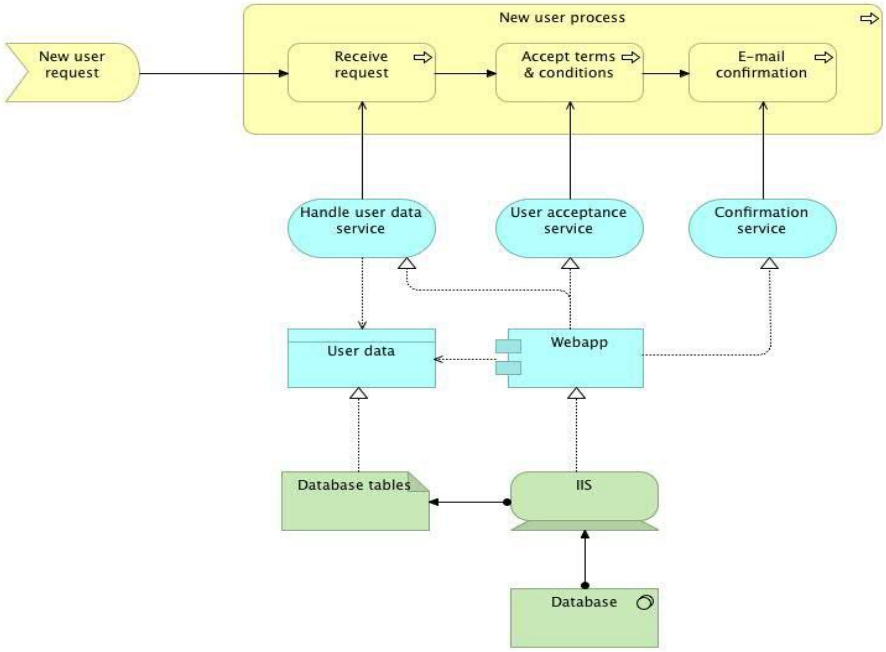


Figure 7.1 - Shows the process of how a new supplier registers in Kommers and gets access to a user account.

12 Result

In this chapter, the results of the survey are presented, the chapter answers the questions presented in the objective and the results of the interviews conducted for this study. The chapter is divided into sub-chapters and begins by presenting the definition of personal data and then presents the results of the interviews. The chapter then continues to present the general plan produced by this study and the results that have emerged from the use of this general plan in a limited part of the system Kommers. The chapter concludes by presenting the financial aspects for the use of the general plan and the implementation of the technical parts of Kommers that this study dealt with.

12.1 Definition of personal data

Earlier in the report, personal data is described under heading 3.4 where the Swedish Data Protection Authority has interpreted the General Data Protection Regulation and describes what is considered personal data and what is considered sensitive personal data under the Regulation. This is considered a good and clear description of what personal data is, which is later analyzed and discussed from a GDPR perspective during discussion in the report.

12.2 Interviews

The interviews were conducted according to the method in chapter 6, which created slightly different answers from the interviewees who will be referred to as company A and company B. Company A is a very small company with few employees, company B is just the opposite, a large company. Both companies handle a lot of personal data in their operations.

12.2.1 Training, awareness, personal data identification and consent

To create awareness of GDPR, both companies have trained their staff, although in slightly different ways, company A has used the Swedish Data Protection Authority's training courses where the entire company participated, company B has brought in consultancy help to handle the transition and has its own compliance department that handles the training for the employees[34]. This department chooses who receives what type of training and they put together the working method to be used, all to ensure that the work is done in the same way regardless of whether there are several people doing the same work. In company B, it has also been concluded that more types of roles will be needed in their CRM system to prevent personal data breaches.

After the training, Company A has developed what type of personal data they process, later they have made a division in what classification the identified data should be given, they state that they do not have any direct form of external unstructured data as they themselves handle their customer data in a database and not in files but that they have some internal unstructured data. Then this part is not considered a problem, the challenge they have instead is to manage the unstructured data that they have in a common file area which at this time is about five million files that are completely uncontrolled. They intend to handle this by setting read access to the entire file area for all employees who have to go through the file area and retrieve the files that the employee thinks they need. This must be done before a specific date that falls before 25 May. The files that the employee is allowed to save in order to carry out his or her work according to the company's governing documents must be placed in the correct place that is assigned. Then the entire file area will be locked for everyone except for a management group that can give access if someone is missing something. This file area will then be locked for a predetermined time before it is completely deleted as it can be considered information that is outdated. The company does not know if this is an approved method according to the regulation, but they believe that it is justifiable to handle it in this way. Both companies discussed consent and had slightly different thoughts about this. Company A needs to handle consent both for people older than 13 but also younger, this creates a need to be

able to identify both guardians and the person to be registered. Company A sees this as a pretty big problem as it is both expensive and difficult to identify who it is that consents to their registration for marketing. Company B wants to respond to this by avoiding consent as far as possible as it can be withdrawn from the data subject at any time. They want customers to enter into contracts for the services they provide so that the company can consider itself to need the personal data to be able to perform its tasks for the customer. They say that such agreements cannot be broken in the same way as there are other laws that require that the processing of the data subject's personal data is saved for e.g. bookkeeping.

12.2.2 Risks, incident management and backup

The management of risks and incidents has been handled in slightly different ways by the two companies, Company A has seen that the biggest risk is that they could be inundated with requests for register extracts as they are in an industry where their customers' users may want to know this. As the company is small, this can take up a lot of their resources unless an automatic function for this is created. Company B, on the other hand, has only had a single request for a register extract over a period of seven years. They believe that they do not need to prepare for such a scenario with an automatic function, but they choose to only create a control document for manual handling. Company A has also identified a risk regarding their storage of data, their database and web server are located on the same server. In other words, if they were to experience a breach in the server, the attackers would gain access to both the web application and the entire database. This has meant that Company A does not encrypt anything more than the passwords of the users as a breach gives access to the decryption keys for the database as well. Company B believes that they do not have any increased risks regarding data security with the new regulation as they already have high requirements for security in their systems.

In particular, company A discussed backups as both a risk and a problem as there are no clear guidelines for how backups and especially deletion in backups should be handled. They say that technically, it is a huge job to remove specific things from a backup in the event of a deletion. They themselves believe that it should be enough for all backups to be removed at regular intervals and to inform about this when the data subject's personal data is collected. Company B had no views on this.

12.3 General plan for implementation of GDPR

By analysing the GDPR as a whole, a general recommendation has been developed in the form of a solution proposal that has been divided into three phases: feasibility study, risk analysis and content of implementation (see figure 8.1), these followed by a checklist of what an organisation should take into account in order to implement the GDPR.

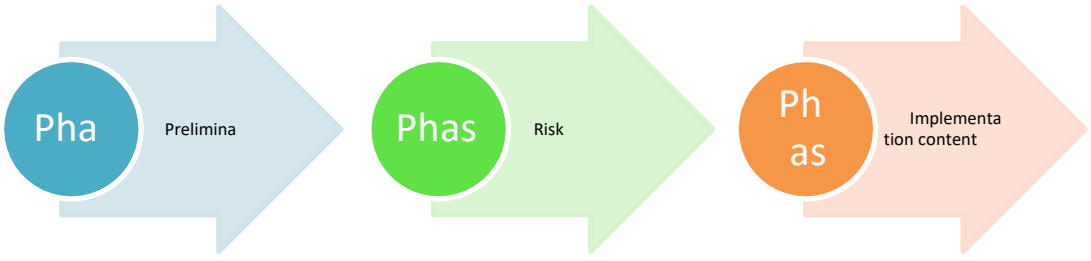


Figure 8.1 - Illustration of Phasing

12.3.1 Phase I - Preliminary investigation

A detailed preliminary investigation should be carried out to read up on whether the GDPR is and understand how the organization must relate to the requirements of the General Data Protection Regulation. By doing this, knowledge is created that will then be used to identify parts of the organization where the processing of personal data needs to be handled. It is important that it is not just one person or a small group who learns about what the regulation says, but that the information is also passed on to the entire company.

12.3.2 Features and processes

Identify which processes in the organization handle personal data, then analyze these processes to assess whether measures need to be taken to meet the requirements of the regulation. Finding out whether these processes send data to third parties for processing is very central to protecting personal privacy. Identifying all the security measures that exist in these processes is central to being able to make a good risk analysis.

12.3.3 Personal data

Map and create a register of all personal data the organisation processes and divide these into direct and indirect identifying data. Here, data that is processed in unstructured form must also be identified, i.e. whether the organization uses the misuse rule. This facilitates at a later date when a risk analysis of this personal data must also be carried out. As the personal data controller must submit a register of the personal data processing carried out in the organisation to the Swedish Data Protection Authority, this is a good support for creating the register at a later stage. Personal data is any kind of data that can be related to a living natural person. Examples of personal data can be name, e-mail address, audio recording, pictures, IP address. How this data is collected must also be identified in order to analyze what information the data subject receives and how it is stored, data can be collected, for example, in the following ways: forms (online/offline), quotes, email correspondence and health data through pedometers.

Which people in the organization handle personal data should also be identified as they must be informed about what applies with the new regulation in order to handle personal data in a correct way. This step is also important as not all persons should have access to personal data that is processed.

12.3.4 Consent

How you currently obtain consent for the processing of personal data must also be analysed, as this is an important point in the new regulation. How are the terms of use structured, is it legal text or is it easy to understand even for someone without this knowledge? How clear is it for the person who registers about how and why storage takes place, but also for what purpose personal data is collected?

12.3.5 PHASE II – Risk analysis

A risk analysis must be carried out to identify the risks that both the company faces with the new regulation and the risks that the company's customers face. The risk analysis must be carried out immediately after the preliminary investigation, as the company has the most control over what personal data they handle. How can the company be affected if the regulation is not followed. Although the Checklist in Appendix A is not specific to a company, it gives a good idea of the type of questions that need to be asked.

12.3.6 PHASE III – Implementation content

To implement all the content, the data controller organization needs to appoint a manager who puts together a competent team to handle the implementation and together with them compile a schedule. This group must compile what needs to be managed, by using Phases I and II together with the recommendations in Phase III, then the entire content will be able to handle the company's transition to being GDPR-Ready.

12.3.7 Appoint a Data Protection Officer

A personal data officer is the person who is responsible for ensuring that the data controller handles personal data in accordance with the regulations that have been developed. A data protection officer should not be a person in a key position when the data protection officer's judgment can be questioned. The regulation has some guidelines that are intended to help in this procedure, see chapter 5.4.

12.3.8 Appoint a data processor

A Data Processor may be appointed but will probably be identified. Since many companies have outsourced their entire data management to a data center, this data center acts as a data processor. Here it is important for the data controller to develop clear agreements with straightforward requirements on how the data processor is to handle and secure the personal data that is stored, this is described in chapter 5.4.

The company itself can be both the data controller and the data processor, it is then important to analyse whether there is any customer where the company acts as a data processor and these agreements must also be handled, in the manner described above. If the company has many customers where personal data is stored, it is important to offer a good service with good handling of the new regulation to try to make all agreements with customers be similar to each other.

12.3.9 New data protection practices

The processes identified in Phase I that do not comply with the technical security measures for data protection must be updated/changed to meet the requirements set for technical data protection in the GDPR. New data protection practices or system access restrictions may be options for this.

12.3.10 Documents that need to be produced/updated

Legal documents: Drafting the new agreements regarding the handling of personal data both between their own organization and their data processor is of enormous importance. These agreements must be GDPR secured. If you as an organization have several data processors, it is important that you develop an agreement that is used for all data processors to ensure that the data processing takes place in accordance with the organization's interpretation of the GDPR.

Customer/User Consent: According to the GDPR's specifications, update the information provided to the customer when collecting data, provide them with information regarding how their personal data will be processed and for what purpose this data is collected. Developing a standard text that can be used in several situations is a good solution for this.

Establish procedures for following up on the implementation of the GDPR: It must be monitored that the rules from the GDPR are followed and insufficient measures or in case of deficiencies must be reported. Establishing procedures on how this is to be monitored and reported should be done to follow up on compliance with the GDPR.

Steering documents: Establish routines in the form of steering documents on how staff should act in different scenarios that are added with GDPR, these different scenarios are explained in more detail in chapter 5.3:

12.3.11 Request for a register extract

- How staff should act in the event of incidents or suspected incidents has been identified
- Processing of personal data for those in the organisation who process personal data
- Request for deletion, modification and restriction of personal data that is registered
- Data portability procedures

12.3.12 Education

The employees in the organisation that processes personal data need knowledge of the GDPR to handle personal data correctly, ensuring that the right people have the right training is the responsibility of the data controller35. Some roles may also require in-depth knowledge, such as the data protection officer, department heads, the IT department or HR.

12.3.13 Deletion routines

Establish instructions regarding the company's own deletion procedures. How long and for what purpose does data need to be stored after the case has been closed where the case involves the processing of personal data. This must be established and included in the consent that the customer approves when the organization collects personal data in the first step as set out in chapter 5.2.

12.3.14 Transparency towards the customer (create a transparent user interface)

With the new regulation, it is a requirement to be transparent towards the data subject, this can be solved in several ways such as governing documents and the like. If you as an organization have a user interface where the registered person can log in, then it is possible to create a function on e.g. "My pages" where the organization continuously shows what personal data they have about the registered user.

12.4 Implementation checklist

Table 8.1 below is an excerpt from the checklist which can be found in its entirety in Appendix A. It has been prepared using information and points from the Swedish Data Protection Authority together with this study's interpretations and comparisons from the interviews conducted at companies A and B. In the table, the left column explains who is involved in each point.

Table 8.1 - S = The survey, D = The Swedish Data Protection Authority.

Phase I - Preliminary investigation		**Results of analysis**
S	Read up on what GDPR is and understand how you must relate to the requirements of the General Data Protection Regulation.	
S	What functions and where do you handle personal data (processes)	
S	Internal processes that deal with personal data	

D	Third-party processing of personal data	

12.5 Implementation of solution proposals in Kommers

12.5.1 Phase I – Preliminary investigation

In the preliminary investigation, the process of registering new supplier accounts in Kommers was identified, which is described in chapter 7. Upon registration, the personal data is obtained through a web form that is filled in by the creator (user) of the account. The creator is given the opportunity to give consent for the personal data to be used for marketing purposes, the creator is also given the opportunity to read the user agreement by clicking on a link before accepting it. Personal data processed in this process are those listed in Table 8.2

Table 8.2 – Personal data processed

Direct personal data	**Indirect personal data**
First name, last name and email	Company name and corporate identity number

This data is then stored in a database where it is not encrypted and all employees in the organization handle the personal data from the suppliers. They also use the misuse rule when they process data in unstructured form. They do not process personal data about children.

12.5.2 Phase II – Risk analysis

A risk analysis was made on what it could mean for ASSA Abloy not to take action in the process of creating new accounts in the supplier portal. The consequences of this will of course be sanctions mentioned in Chapter 5.8. Whether there will be full sanctions or whether they will receive mild sanctions cannot be determined at the moment, so different scenarios are discussed in later chapters. These scenarios address different levels of sanctions as a result of the actions taken in the organization. Another aspect of this is that they lose trust from customers if they do not live up to the requirements of GDPR. By not protecting customers' personal privacy, the consequence may be that current and future customers choose to turn to another player in the market. Taking measures should therefore be seen as an investment instead of avoiding the cost of these measures.

12.5.3 Phase III – Content of implementation

The content of the implementation has been decided after consideration of the delimitation, the results of the preliminary investigation and the risk analysis. In the process of creating new supplier accounts, measures must be taken to protect the personal data stored in the database, this must be done by encrypting the direct personal data before it is stored in the database, which means that it becomes unreadable in the event of a database attack. Furthermore, changes must be made regarding how the user takes part in the user agreement and gives their consent for the processing of the personal data they provide. The solutions to these are described below in chapter 8.6. An analysis of what ASSA Abloy as an organization needs to take for other measures to achieve the requirements of the GDPR is to appoint a person responsible for implementation, identify the data processor and write an agreement for the handling of the personal data that the data processor is to handle, update the user agreement and information for obtained consent, a plan for follow-up to

check that the GDPR is complied with after completion of the implementation and produce various governing documents.

12.6 Technical implementation in a test environment

12.6.1 Vendor User Registration

By changing the checkboxes at the time of registration and creating a feature that forces the user to read the user agreement that is clearly and simply structured before they can register the account. These measures have been taken to force the user to take part in how their personal data is to be processed and for what purpose. The user is first allowed to enter their personal data and give consent for the various processing operations described in the checkboxes before proceeding to register the account. At this step in the process, the user gets the user agreement on the screen that they have to read through and at the bottom of the user agreement they have to approve this before the account is registered.

12.6.2 Technical solution

Below in Figure 8.2 are the functions that were created to force the user to read the terms and conditions of the agreement before registration. The function brings up a pop-up box with the user agreement and consent that the user must read through (scroll through the agreements) before they can approve this and then be registered as a new user in the portal. The result of the function is shown in Appendix D.

```
$(document).ready(function () {
        $(".close").click(function () {
                $('.termsModal').fadeOut('fast');
                $('.overlay').fadeOut('fast');
});

$("#<%=bAcceptTermsAndConditions.ClientID%>").prop("disabled", true)
$('.textBoxHolder').on('scroll', function () {
        if ($(this).scrollTop() +$(this)[0].inner) >= $(this)[0].scrollHeight) {

                $('#<%= bAcceptTermsAndConditions.ClientID %>').prop("disabled", false)
```

Figure 8.2 - JavaScript Acceptance User Agreement Feature

12.6.3 Storage of personal data

The personal data that the supplier provides when registering a new account is managed in the system and stored in the database. In order to protect personal privacy according to the General Data Protection Regulation, the solution has been developed to encrypt this data before it is saved in the database, see Appendix C. The data that has been chosen to encrypt is a result of the analysis of personal data processed by this function in the system, encryption of first name, last name and e-mail prevents the remaining data from being related to a specific person and thereby protects the person's privacy in the event of a breach. An example of a function that can be used in this implementation is shown below in Figure 8.3, the figure shows how part of a function for RSA encryption written in the language C#, the function is shown in its entirety in Appendix E36.

```
        static public byte[] RSAEncrypt(booty[] DataToEncrypt, RSAParame- ters   RSAKeyInfo, Bool
DoOAEPPadding)
        {
            Try
            {
            byte[] encryptedData;
            Create a new instance of RSACryptoServiceProvider. using
            (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
                {
                Import the RSA Key information. This only needs
                toinclude the public key information. RSA.
                ImportParameters(RSAKeyInfo);

                Encrypt the passed byte array and specify OAEP padding.
                OAEP padding is only available on Microsoft Windows XP or
                Later.
                encryptedData = RSA. Encrypt(DataToEncrypt, DoOAEPPadding);
                  }
                  return encryptedData;
            }
            Catch and display a CryptographicException
            to the console.
            catch (CryptographicException e)
            {
                Console.WriteLine(e.Message);
                return zero;
            }
        }
```

Figure 8.3 - Encryption with RSA written in C#

12.7 Investigation of the economic impact of an implementation

A cost estimate has been made on it Technical implementation that this study addresses. The cost is calculated on the account creation process, the process has been worked through together with the solution proposal until the technical solution is implemented. A calculation has also been made at different levels of the sanction cost that may arise in the event of non-implementation for ASSA Abloy based on what the regulation has as guidelines. This has been divided into three different scenarios which are discussed in chapter 9.
The billing cost for development is an average value calculated on ASSA Abloy's own hourly billing for consulting assignments together with an approximate hourly wage for an ASSA Abloy employee who is not on a consulting assignment. This calculation has been made to cover part of the income that is lost when a consultant works internally and is not on assignment. Tables 8.3 to 8.7 below are designed to show the costs of the different scenarios discussed in Chapter 9.
Annual sales of ASSA Abloy in 2016

Table 8.3 - Cost of implementation of proposed solutions and technical implementation (SEK)

Hours Charged	Kr á timme	Cost
160 x 2	600	192 000

Table 8.4 - Sanction costs for ASSA Abloy depending on sanction level (Guessed amounts)

Annual sales of ASSA Abloy in 2016	Level of sanctions	Sanction cost
9 123 000	4%	365 000
	3%	274 000
	2%	182 000
	1%	91 000

Table 8.5 - Scenario 1 - Implementation of encryption functions only (SEK)

Implementation cost	114 000
Sanction cost	91 000
Total cost	205 000

Table 8.6 - Scenario 2 – Only implementation of change for the Terms of Use Acceptance (SEK)

Implementation cost	78 000
Sanction cost	0
Total cost	78 000

Table 8.7 - Scenario 3 – Implementation of both solutions (SEK)

Implementation cost	192 000
Sanction cost	0
Total cost	192 000

12.8 Cost calculation company X

The cost calculation that was performed at company X was carried out in a limited implementation when company X was in a process of implementing GDPR in 20 out of a total of 48 critical systems.

The calculation below concerns the costs of implementing the following changes in one of Company X's critical systems.

- Delete sensitive personal data
- Delete personal data in unstructured form
- Manage accesses (remove and add accesses), which should have access to CRM systems
- Encryption of the transfer of data between the different systems within company X
- Create a feature that informs users how to handle personal data when they log in to the system

The work to make these changes in this system has been ongoing since February and worked on the implementation of GDPR and this team has consisted of a system owner, coordinator, team leader and five developers.

Table 8.8 – Cost per hour, role and time spent at company X (SEK)

Role	ent per week	Cost per hour
System Owner	4	800
Coordinator	3	800
Team Leader	6	800
Developer	23	800

Table 8.9 – Total costs and hours worked at company X (SEK)

Role	Total hours worked	Total cost
System Owner	68	54 400
Coordinator	51	40 800
Team Leader	102	81 600
Developer	391	312 800
Total cost		489 600

Company Y did not share the figures for the implementation as they felt that there are far too different backgrounds between companies for a financial comparison for the implementation of

GDPR to yield anything, especially since the directive does not say exactly what to do but only what issues to solve.

13 Analysis and discussion

This chapter presents own interpretations together with an analysis and evaluation of the results presented in Chapter 8. The results will be critically discussed in comparison with alternative solutions.

13.1 Definition of personal data

In the result, I have concluded that the GDPR's definition of personal data is very straightforward and easy to understand if you only need to identify direct or sensitive personal data. However, according to the interviews and research I have done in this study, I believe that the difficulty comes when it comes to identifying indirect personal data, how far should the interpretation be made and what is considered to be indirect personal data. In this regard, I find it extremely difficult to know how far the identification of indirect data should be taken because there are not sufficient guidelines for this. For example, if I have a picture of a house, it can be indirect personal data if the person who sees the picture knows who lives in the house, but when other people see the picture, it is only a house and nothing else, is this then indirect personal data when only one or a few who may never see the picture can identify a person? These are questions that organizations will need to ask themselves as the guidelines in the regulation are not sufficient.

13.2 Interviews

The companies that were interviewed were two completely different companies, both in size and what their business concept is. This meant that they respond to the implementation of GDPR in two different ways. As described in the method, the interviews were semi-structured and this gave the opportunity to validate the checklist that I developed. Both companies have divided the implementation into phases similar to the phases found in our checklist. Both state, for example, that they have chosen to train their staff, analyze the different processes they have and identify personal data in these to later move on to a risk analysis and then create an idea of what changes they need to make to meet the GDPR directive. I believe this gives a validity to the checklist that has been developed in this study as the phases and identifications are similar. It could be argued that the validation should be stronger, as there is no exact specification to follow or any practice from cases at the Swedish Data Protection Authority, this must be considered sufficient at the time this investigation was carried out.

13.3 General plan for implementation

In this sub-chapter, the phases and checklist in the general plan that has been developed in this study are discussed. How it is intended to be used and how it is constructed. Why it is developed as a general plan and not specific tasks. The plan is also being discussed critically to try to get a picture of where it could be stronger.

13.3.1 Phase I

It can be discussed whether there are enough points in the preliminary investigation to make a total analysis of the organization. I believe that identification of functions and processes is a central part of being able to handle an implementation of GDPR, however, I have chosen not to go into depth into what can be a process as one organization is never the same. I want to get the organization to think for itself in order to succeed in identifying all processes that process personal data. The preliminary investigation in the proposed solution is created to get the organization to understand the meaning of GDPR, the idea is that through this, the organization will take in knowledge that makes the identification of problem areas easier. The other two points are only there to support the organization in giving an idea of what they should identify in the different processes in order to know if the process needs to be managed. This is complemented by a checklist of additional questions that

an organization can ask itself in the search for the processes involved. Just as one organization is never the same, a final list of processes will never look the same, hence the checklist addresses questions that this survey considers to be general questions that probably exist in all organizations. The goal is for the organization to be able to identify all its processes and not just the obvious ones.

13.3.2 Phase II

The risk phase is difficult to give guidance in as it is based on the preliminary investigation and what the organization looks like. But I believe that when you have done the preliminary investigation, it creates knowledge about GDPR and what risks the organization can be exposed to. This goes hand in hand with the risk thinking that GDPR wants to develop in organizations in order to be able to manage personal privacy in a good way. It is because of this that clearer guidelines were not developed on what risks the organization should analyze in Phase II and that it is entirely dependent on what kind of activities the organization runs. The strength of this survey is that there are basic questions in the checklist that can provide guidance on what risks may exist and thus start the risk thinking in the organization.

13.3.3 Phase III

This phase consists of the content of the implementation and is a result of the preliminary investigation and risk analysis, here I have developed parts that are a requirement according to GDPR that every organization must handle when implementing GDPR, these parts are specified in the checklist. In addition to this, there are the changes identified in the results of the preliminary investigation and the risk analysis. One question that all organizations will be forced to deal with is how to handle unstructured data as there are no guidelines on how this should be handled. Previously, this point could be avoided by the abuse rule, which is now disappearing. Since I have been forced to make delimitations, I have not found a solution to handling unstructured data in this study. Discussions regarding this have only occurred during the course of the survey and one thought I have for handling unstructured data is to think privacy by design when developing new or existing processes. This highlights the issue early in the process to handle this in the best way.

13.3.4 Technical solution

Measures to ensure that the user reads the terms of use

The scrolling function ensures that the user has read the terms of use and given their consent to the organisation's processing of personal data. The fact that the user is forced to scroll through the user agreement and click accept means that the user has every opportunity to understand how the organization processes the personal data.
I felt that the scrolling function is a central part of the solution to force the user to read the terms of use. Something I think can create confusion is if the user does not understand that the button to approve the agreement is activated until after scrolling through the text, the argument for still using this method is based on the fact that in today's society the majority of users have good computer skills and that it is understood that the button is not activated until you have scrolled through the text. There is also a risk that the user does not read through the user agreements, but only scrolls down and approves the agreement. However, I believe that this solution satisfies the directives laid down in Chapter III, Article 12 of the regulation. *'The controller shall take appropriate measures to provide the data subject with all information referred to in Articles 13 and 14 and all communications referred to in Articles 15 to 22 and 34 relating to processing in a concise, clear, intelligible and easily accessible form, using clear and unambiguous language, in particular for information specifically addressed to children'*.

An alternative solution is to start from the original method with a checkbox and next to this checkbox a link to the terms of use, here a function can be introduced that does not activate the

checkbox until the user has clicked on the link for the terms of use. This would then need to be clarified with an explanatory text next to the checkbox. With this solution, I believe that there is a high risk that the user will only click on the link and not look at the user agreements, which is why I decided to use the former solution.

13.3.5 Encryption

The solution I have developed as a proposal is to protect the direct personal data with encryption and through the encryption stop the identification of a person through indirect personal data. Since the indirect personal data identified in the process of creating a new account consists of company data, I believe that the direct personal data should be encrypted to prevent the identification of a specific person through company data that is stored. I chose to give the suggestion to encrypt the information in the web application so as not to be hindered by a database manager's own encryption algorithm. (This is seen outside the framework of SSL/TLS). This gives a strength and freedom of choice in that different algorithms can be chosen depending on the level of security you want, and in addition, there is the option to change the encryption algorithm in the future to increase security if needed. Through this solution, I believe that personal privacy is protected in the event of a database attack as specific people cannot be identified if they get hold of the data that is in the database. When encryption takes place in the application layer, the decryption must also take place in the application layer for all the functions that process this data. In my opinion, these functions only need to invoke the decryption function that is created in connection with the encryption. What can be problematic is identifying which functions need to make use of encryption and decryption. Here, I believe that these functions should already be identified during the preliminary investigation and this list of processes can then be reused to identify which ones will also require encryption or decryption. An alternative solution is to split direct and indirect personal data into two different databases. This means that the indirect personal data cannot be linked to a person if there is only one database breach in one of the databases. The disadvantage is that if it happens in that database with the direct personal data, the attacker can identify the people directly. To avoid this, an additional security measure can be taken, to encrypt the direct personal data in the database specified to the first solution.

13.4 Financial calculation

The technical implementation in chapter 8.6 is from a financial perspective only a cost, there are no possible revenues associated with it as the function is a basic requirement from GDPR. It should be taken into account that this implementation is not a complete implementation but only a small part, this means that the cost of a total implementation will be much higher. But in our opinion, it can be seen as a cost saving compared to risking large and expensive sanctions from the Swedish Data Protection Authority in the event of non-implementation.

In the event of a personal data breach, the costs for the organizations can be very high as they risk a very large sanction fee in addition to this, there can also be talk of damages in cases where a registered person has been harmed. There could also be legal fees and legal costs, however, this is something I have chosen not to take into account as the research I have carried out at lawyers and law firms has yielded such mixed and uncertain results.

I made a calculation of the technical solutions and implementation in Kommers and compared it with the cost of a possible personal data breach. When calculating the cost of an incident, I calculated different levels of sanctions, legal costs and damages to the victim. If an incident occurs that the Data Protection Authority considers to be of such a degree that a sanction fee is needed, then in addition to that cost, the cost of implementation will also be added to solve the problem that the Data Protection Authority says exists. After a comparison, I believe that it is most cost-effective to implement a solution now before May 25, 2018 as the organization will otherwise most certainly risk

an incident occurring and that the Swedish Data Protection Authority will then issue a reprimand and force an implementation to be carried out and also a risked sanction fee and damages to the victims.

13.4.1 Scenarios

I have selected a few scenarios to show why you as an organization should make investments to implement GDPR. As can be seen in the table in chapter 8.7 there is an administrative fine of 4% of the annual turnover, this would in ASSA Abloy's case be replaced with 20,000,000 € in sanction fee according to the regulation which is the same as bankruptcy, for the reason that a comparison with this in all possible cases indicates that you should do all the implementations you can think of, then I completely disregard using this scenario.

13.4.2 Scenario 1 - Implementation of encryption features only

The first scenario that I have looked at is to only implement the encryption function where first name, last name and email address are encrypted. This function, as the table in the result shows, has a relatively high cost as the choice of encryption algorithm and where in the systems the actual encryption should take place is not entirely simple. If only this implementation is carried out, I believe that the company has done a preliminary investigation of what needs to be done to meet the requirements of the GDPR and also introduced a form of protection for the personal data that is stored. This should show in the event of a personal data breach that the company has tried to reduce the risk for the data subject and this should according to the regulation only give a minor sanction. Since the organization has not taken measures to collect consent from the data subject, I see it as a sufficient misstep to risk a lower amount in sanction. The cost of implementing encryption features and any estimated penalty cost will be higher compared to implementing both encryption and the change in the Terms of Service acceptance. Thus, I believe that it is more profitable to implement both solutions.

13.4.3 Scenario 2 - Only implementation of change for the Terms of Service acceptance

In the event of an implementation of the change in how consent is obtained as shown in Chapter 8, I see that the cost of the implementation is lower than in scenario 1. This is because the function does not require as much work as an encryption algorithm requires to be implemented, however, after interpreting the regulation, I believe that this function is extremely central, that the data subject gets the opportunity to read up on how the personal data will be stored is one of the most important parts that the GDPR has been developed to handle. Since consent is very central, I believe that this, together with the checklist being followed in the remaining parts of this process, should minimize the risk of sanctions from the Swedish Data Protection Authority in ASSA Abloy's case.

13.4.4 Scenario 3 - Implementation of both solutions

Implementing both solutions may initially be unnecessary as scenario 2 states that the organization should avoid the cost of a sanction and there is a saving in not implementing the encryption. However, one must ensure that if scenario 2 falls in and a reprimand from the Data Protection Authority comes, then this may conceivably include taking measures to protect that personal data and the measure that I have mentioned here is to encrypt. Then I see in retrospect that both costs will occur anyway and I then believe that if the possibility of avoiding sanctions completely exists, these should be taken from the beginning.

13.4.5 Cost comparison with cost calculation for companies X and Y

Table 9 shows a price difference of approximately SEK 300,000 for an implementation at company X compared to ASSA Abloy. It may seem like a big difference in sums, but the implementation that has been carried out at company X is larger than the implementations carried out in ASSA Abloy's system, because to introduce the same things at ASSA Abloy, the cost would go up and approach each other significantly. Since Company X has 20 similar projects underway and these are estimated to cost about the same amount, this proves that ASSA Abloy should carry out the implementations developed in this study as the cost is in the same range as with Company X which has done a detailed feasibility study and market analysis.

Company Y only discussed structural capital and considered that the sum for an implementation of GDPR cannot be calculated directly as there are costs for the implementation of new systems that are carried out at the same time because the cost of that implementation decreases as the GDPR implementation is already carried out. The fact that the already invested structural capital in the Personal Data Act differs greatly between players in the market is also an incentive for an economic comparison to be difficult to create in a correct way.

13.5 Durability

With the introduction of GDPR, companies are forced to take stricter measures to protect personal privacy. Since GDPR is an EU directive, the citizen's rights are strengthened in a broader and more sustainable way compared to the previous solution that was based on the law that in Sweden is called PUL, the member states interpreted PUL differently and this meant that the personal data was handled in different ways depending on which member state handled the data. As development in today's information society is taking place at a high pace and the way digitalization has taken off in most companies, this entails risks for the data subject as a data breach does greater damage in today's society compared to when GDPR was introduced. The sustainability challenge is becoming greater and this must be addressed globally, in a common way. The introduction of the GDPR is a big step in the right direction, as even non-EU members who handle data from any of the countries where the GDPR has been introduced must handle this data in the same way as EU members. This, in turn, can be a starting point for other countries to strengthen the requirements for how data is to be handled within their own borders. The GDPR also requires that the personal data will be handled clearly for the parties concerned, this then creates awareness in the individual of what they are giving consent to and the ability to control how their personal data will be processed. The introduction of GDPR is not only positive for the individual, companies become more transparent about how the personal data should be processed, which means that the customer becomes more secure, which in turn leads to customers appreciating the companies more and this strengthens the company's brand as they can show that they care about their customers.

14 Conclusion and recommendations

The goal of developing a general plan and a general specification has been achieved in this survey by developing a solution to support an organization that is at the beginning of the process of implementing GDPR. It will help the organizations get started with the project and ask the key questions about GDPR. After the results of the interviews, information from seminars and the analysis of ASSA Abloy, the survey has concluded that an organization should evaluate whether the checklist has enough questions to cover the entire organization's needs and, depending on the outcome, add or remove questions from the checklist.

The solution proposal developed in this study has been applied to a limited part of ASSA Abloy where it has yielded positive results. By applying the proposed solution at ASSA Abloy and through the interviews conducted earlier in the study, I believe that the result is positive and that the proposed solution can also be used in other processes and in other organizations. I developed a checklist during the investigation and the credibility of this has been developed on the basis of the Swedish Data Protection Authority's guidelines. These have been supplemented with the results of our own surveys and the interviews conducted during the survey. The goal of studying what personal data is is considered to have been achieved and the result has given a greater opportunity to use the solution proposal in a clearer way, which shortened the time it took for the identification of personal data in the process. The economic objective of evaluating the cost of an implementation versus not carrying out this implementation can be considered to have been achieved. However, it should be taken into account that the study shows that the regulation is designed to force an organization to make the necessary implementations as the costs according to this study will otherwise always be higher if an implementation is not carried out, which means that a recommendation to do the implementation will be a requirement from the economic study.

Company Y believes that it is extremely difficult to make economic comparisons on the subject as there are large differences in the situation of the compared companies. There may be differences in how personal data has been handled and what size and market the companies operate in. After the interviews that were carried out at companies X and Y, I believe that the calculation that I performed at ASSA Abloy is considered reasonable as company X operates in the IT market just like ASSA Abloy and they do not have a huge handling of personal data, also similar to ASSA Abloy. The smaller projects that company X is now using to secure themselves against GDPR are in the same order of magnitude as an implementation at ASSA Abloy entails, so I believe that these can be compared with each other as the costs correlate with each other.

This survey does not provide a solution to how unstructured data should be handled, as this is an issue that is extremely important within GDPR, a further investigation on this topic must be carried out. Since this survey was carried out before May 25, 2018, it should be taken into account that there may be sharp updates from the Swedish Data Protection Authority that have not been studied now.

15 References

2http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204

3 https://europa.eu/european-union/eu-law/legal-acts_sv

4 https://unstats.un.org/sdgs/indicators/database/?indicator=17.8.1

5https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivlag-1990782_sfs-1990-782

6https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/bokforingslag-19991078_sfs-1999-1078

7 http://www. ASSA Abloy .se/en/hem/

8 https:// www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-en-personuppgift/

9https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/kansliga-personopplysning-uppgift-om-brott-och-personnummer/detta-ar-kansliga-personopplysning/

10 https://developer.mozilla.org/en-US/docs/Learn/JavaScript/First_steps/What_is_JavaScript

11https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/tryckfrihetsförordning-1949105_sfs-1949-105

12https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/yttrandefrihetsgrundlag-19911469_sfs-1991-1469

13 https://it-ord.idg.se/ord/ansvarig-utgivare/

14 https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

15 https://sv.wikipedia.org/w/index.php?title=RSA&oldid=40916360

16https://msdn.microsoft.com/en-us/library/system.security.cryptography.rsacryptoserviceprovider(v=vs.110).aspx?cs-save-lang=1&cs-lang=csharp#code-snippet-2

17https://docs.microsoft.com/en-us/dotnet/csharp/getting-started/introduction-to-the-csharp-language-and-the-net-framework

18 http://csharpskolan.se/article/introduktion-till-net

19 https://en.wikipedia.org/w/index.php?title=Electronic_discovery&oldid=820657934

20 https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#1

21https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/bokforingslag-19991078_sfs-1999-1078

22https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivlag-1990782_sfs-1990-782

23https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#9

24https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#K3

25https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registredes-rattigheter/ratt-till-delering/

26https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registredes-rattigheter/ratt-till-begransning-av-behandling/

27https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registredes-rattigheter/ratt-till-information/

28https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registredes-rättigheter/dataportability/

29https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#4

30https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#28

31 https:// www.datainspektionen.se/Documents/Riktlinjer%20om%20dataskyddsombud.pdf

32https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#K5

33https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#K9

34 https:// www.datainspektionen.se/utbildning/

15.1 List of references

1. C. Tankard, "What the GDPR means for businesses", *Netw. Secur.*, Vol. 2016, No. 6, pp. 5–8, June 2016.
2. S. Mansfield-Devine, "Meeting the Needs of GDPR with Encryption", *Comput. Fraud Secur.*, vol. 2017, no. 9, pp. 16–20, Sep. 2017.
3. H. Månsson and J. Erichsen, "Accommodation of GDPR - Challenges from a technical and process-oriented perspective", Bachelor's thesis, Lund University- Department of Informatics, 2017.
4. L. Ryz and L. Grest, "A new era in data protection", *Comput. Fraud Secur.*, vol. 2016, no. 3, pp. 18–20, Mar. 2016.
5. S. Adolfsson and P. Lundholm, "Retail's preparations for GDPR : A case study on what changes companies need to make and their work around GDPR", Bachelor's thesis, Uppsala University, http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1112096&dswid=5860, [Accessed date: 20-Feb-2018].
6. K. Pormeister, "The GDPR and Big Data: Leading the Way for Big Genetic Data?", in *Privacy Technologies and Policy*, 2017, pp. 3–18.
7. J. Pettersson and M. Brädefors, "It's not the laws that pass, it's the laws I remember: how companies prepare for the changes that the introduction of GDPR entails", Bachelor's thesis, Uppsala University, http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-340743, [Accessed Date: 02-March-2018].
8. Smouter Kim, "The Year of the GDPR", *Res. World*, vol. 2018, no. 68, pp. 48– 49, Feb. 2018.
9. D. Stark, B. Reg, and Q. Ashlin, "ESOMAR Data Protection Checklist", ESOMAR - World Research codes and guidelines.
10. H. Gjermundrød, I. Dionysiou, and K. Costa, "privacyTracker: A Privacy-by- Design GDPR-Compliant Framework with Verifiable Data Traceability Controls", in *Current Trends in Web Engineering*, 2016, pp. 3–15.
11. Legal text, The Swedish Data Protection Authority, "The General Data Protection Regulation - the text in its entirety - The Swedish Data Protection Authority". [Online]. Available at: https:// www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/. [Accessed Date: 09-Feb-2018].
12. Alan Bryman, Social Research Methods, Fourth edition., vol. 2012. Oxford University Press

13. M. Denscombe, The Good Research Guide, For small-scale social research projects, Fifth edition., vol. 2015. McGraw-Hill Open University Press.

16 Attachments

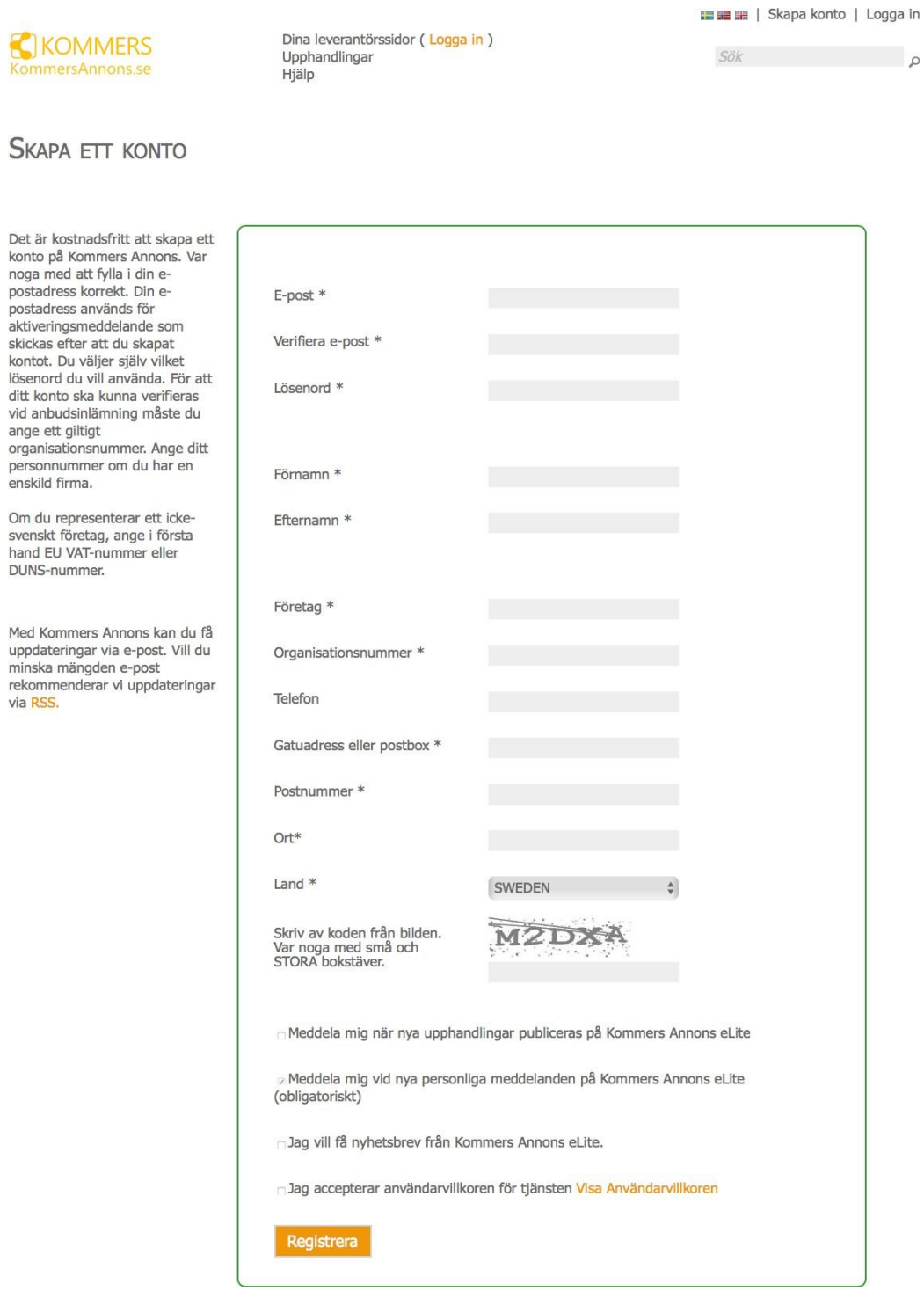
16.1 Appendix A - Checklist for implementation of GDPR

The left column can contain three different letters S, D, I that refer to the source that has produced the question in the checklist. S - This survey, D - The Swedish Data Protection Authority and I - Interviews from this survey. Some points have been developed in combination of the results of this survey and information from the Swedish Data Protection Authority.

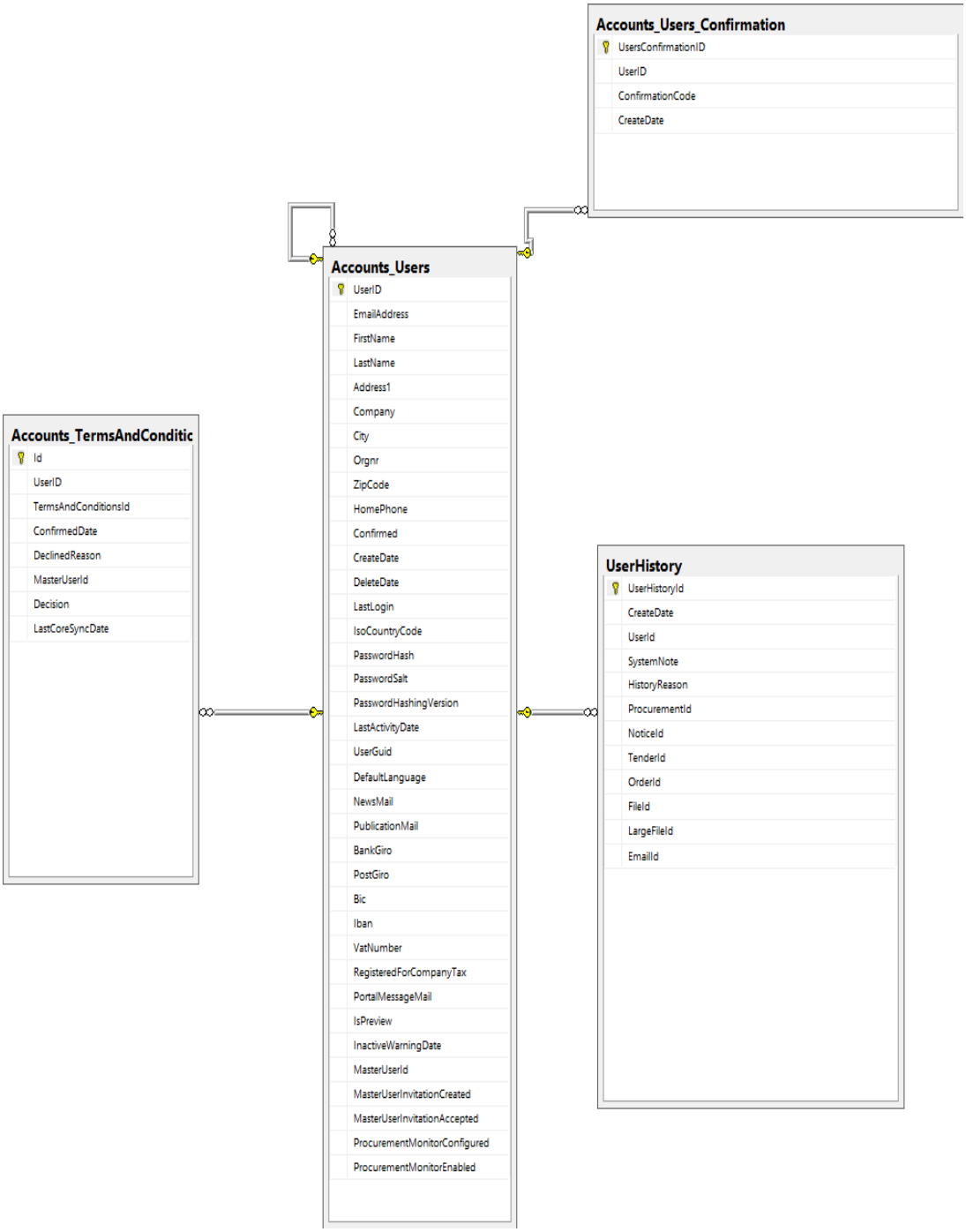
	Phase I - Preliminary investigation	**Results of analysis**
S	Read up on what GDPR is and understand how you must relate to the requirements of the General Data Protection Regulation.	
S	What functions and where do you handle personal data (processes)	
S	Internal processes that process personal data	
D	Third-party processing of personal data	
D S	Identify and map what personal data you handle.	
D S	Create a register of the type of personal data that is processed and for what purpose	
S	Split into indirect and direct identifying data	
D	How is personal data collected?	
S In	How do you store personal data that you have collected?	
S	Which people handle personal data?	
D	Do you use the abuse rule today?	
D	How and what information do you provide about the handling of personal data to customers today?	
D	Do you process personal data about children under the age of 16 (13 years according to the proposal for Sweden)?	
	Phase II - Risks	**Results of analysis**
S In	Analyze the risks for the company of not being "GDPR-ready"	
D S	Can the company identify privacy breaches?	
S In	How is the company affected by a privacy breach?	
S I	Can you handle personal data requests that are added by the new regulation? (Extract from the register, Change, move, delete)	
S In	An impact assessment on the consequences of the company's failure to have adequate measures in place to handle personal data	
	Phase III - Content of implementation	**Results of analysis**

S	Appoint a person responsible for the implementation of the implementation	
D	Appoint a Data Protection Officer	
D	Appoint a data processor	
D S	What measures need to be taken in the system and the processes that are in place?	
S	Update user agreements and information to obtain consent	
D S	Produce a document with a plan to verify compliance with the GDPR after completion of the implementation	
S	Produce or update legal documents (e.g. user agreements and supplier agreements)	
D S	Create governing documents for how the staff should handle personal data.	
D S	Create policy documents for how staff should act in the event of a personal data breach or suspicion of a breach has been identified.	
D S	Create governing documents for how a personal data breach is to be assessed.	
D S	Create governing documents for handling extracts of personal data that the company has about the customer at the customer's request.	
D S	Create governing documents for handling the deletion of personal data at the customer's request.	
D S	Create governance documents for managing data portability.	
D	Create training packages for staff depending on their tasks.	
S		
D S	Develop deletion routines - The company's own routines for how deletion should take place on an ongoing basis in accordance with applicable laws and agreements.	
D S	Create a transparent user interface towards the customer if possible and economically justifiable	

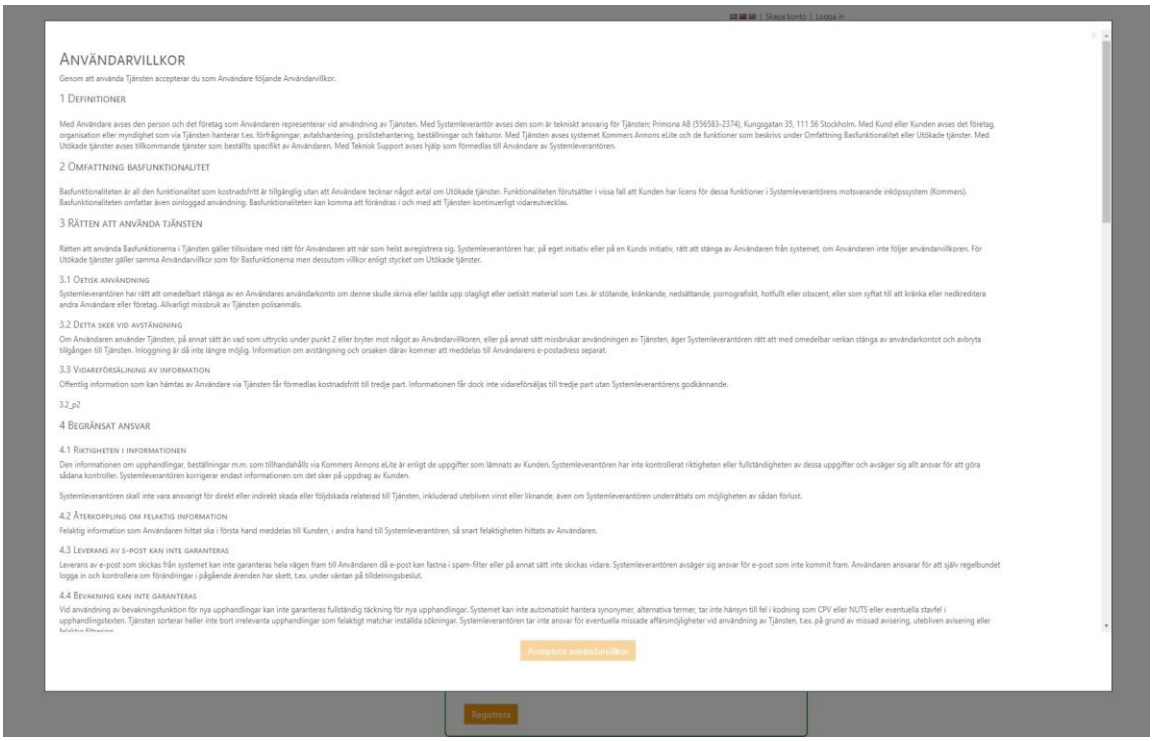
16.2 Appendix B – Create supplier account (before implementation)



16.3 Appendix C – Database structure for registering new supplier account



16.4 Appendix D – Results of implementation for approval of contract terms



16.5 Appendix E – RSA Encryption

```
using System;
using System.Security.Cryptography; using System.Text;
class RSACSPSamp
{
static void Main()
{
Try
{
Create a UnicodeEncoder to convert between booty array and string.
UnicodeEncoding ByteConverter = new UnicodeEncoding();
Create byte arrays to hold original, encrypted, and decrypted data.
byte[] dataToEncrypt = ByteConverter.GetBytes("Data to Encrypt"); byte[] encryptedData;
byte[] decryptedData;
Create a new instance of RSACryptoServiceProvider to generate
public and private key data.
Static public byte[] RSAEncrypt(byte[] DataToEncrypt, RSAParameters
RSAKeyInfo, bool DoOAEPPadding)
{
```

```
Try
{
byte[] encryptedData;
Create a new instance of RSACryptoServiceProvider.
using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
{
Import the RSA Key information. This only needs
toinclude the public key information. RSA. ImportParameters(RSAKeyInfo);
Encrypt the passed byte array and specify OAEP padding.
OAEP padding is only available on Microsoft Windows XP or
Later.

encryptedData = RSA. Encrypt(DataToEncrypt, DoOAEPPadding);
}
return encryptedData;
}
Catch and display a CryptographicException

to the console.
catch (CryptographicException e)
{
Try
{
Create a new RSACryptoServiceProvider object.
using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
}
Export the key information to an RSAParameters object.
Pass false to export the public key information or pass
true to export public and private key information.
```