General Data Protection Regulation: Preparing HR for Change

Heidi Ndiili-Ronkainen

Bachelor's Thesis
Degree Programme in
International Business
2018

Haaga-Helia
University of Applied Sciences

Abstract

Date

Author

Heidi Ndiili-Ronkainen

Degree programme

International Business

Report/thesis title	**Number of pages and appendices 32 + 7**
General Data Protection Regulations: Preparing HR for change	

The European General Data Protection Regulation (GDPR) replaces the outdated Data Protection Directive that was introduced in 1995 by the European Parliament. The new directive will be stricter than the earlier one. The General Data Protection Regulation is a legal outline for organizations that gather and process the personal data of European residents. The regulatory framework provides people with the right to data confidentiality and principles for processing personal data, while also imposing hefty fines for organizations that fail to comply with the law.

The aim of this thesis is to look at how the case company´s subsidiaries´ Human Resource departments are prepared to implement the new legislation. The focus is on whether the subsidiary group companies´ HR managers are taking the necessary steps to move towards adopting the General Data Protection Regulation that was set by the European Parliament and Council for storing personal data by 25 May 2018. The study will also identify the procedures that need to be developed to comply with the regulation through content analysis.

The questionnaire was created together with the commissioning company's thesis supervisor to ensure a clear structure that provides coherent results. The study was thus conducted through a qualitative research approach, utilizing methods such as questionnaires as a primary source of information and secondary desk-top data research.

The findings show that the subsidiary group companies´ were not ready with the implementation of the necessary processes towards GDPR compliance. As the case company is centralising its operations, an action plan for HR´s policies and procedures is needed towards GDPR compliance. The HR is recommended to audit its data in order to understand what documents, policies and procedures are currently compliant with the GDPR.

Keywords

General Data Protection Regulation, Data Protection Directive, Change Management, facilitating HRM, Data Protection Officer, Privacy Impact Assessment

Table of Contents

1 Introduction 1

1.1 Background 1

1.2 Research Question 2

1.3 Demarcation 3

1.4 International Aspect and Link between HR with Study 4

1.5 Benefits 4

1.6 Case Company 5

1.7 Key Concepts 5

2 Literature Review 7

2.1 Data Protection Directive (1995) 7

2.2 General Data Protection Regulation (2016) 8

2.2.1 Introduction and Definition 8

2.2.2 Consent 9

2.2.3 Enhanced Rights 10

2.2.4 Lawfulness, Fairness, and Transparency 11

2.2.5 Integrity and Confidentiality 11

2.2.6 Accountability 12

2.3 Data Processing 12

2.3.1 Data Storage and Minimization 13

2.3.2 Pseudonymous Data 13

2.3.3 Breaching Of Data 14

2.4 Data Protection Directive Vs General Data Protection Regulation 15

2.5 Finnish Law on Personal Data 16

2.6 Human Resources: Handling Employee Data in Relation with the Law 17

3 Methodology 20

3.1 Research Design 20

3.2 Data Collection 21

3.3 Risks and Risk Management 23

3.4 Reliability and Validity 24

4 Results 25

4.1 HRM Status towards GDPR Requirements 25

4.2 Identifying the Processes and Databases 25

4.3 Evaluation of Data Processes and Implementation of Secured Data 26

4.4 Demonstration of the Government Model 26

5 Discussion 28
5.1 Key Results 28
5.2 Recommended Steps for HR towards GDPR Compliance 30
5.3 Further Research 31
5.4 Personal Learning 32
References 33
Appendices 36
Appendix 1. Questionnaire 36
Appendix 2. Thesis activities timeline as a Gantt chart 38

1 Introduction

Beginning in 1995 the European Parliament and council adopted the Data Protection Directive which regulated the processing of personal data within the European Union. The directive has been used for many years and is soon to change. This chapter introduces the background of the thesis study in hand, how the research process has been created and a brief introduction to the case company. The research topic, reason for the study and the investigative questions are clearly stated in this chapter. This chapter also clearly states the international aspects related to the study, the anticipated benefits, and the key concepts.

1.1 Background

European organizations are currently undergoing a change in preparation for the General Data Protection Regulation (GDPR) which was adopted in 2016 and will be enforced on 25 May 2018. After four long years of discussion, the European Commission has set to replace the Data Protection Directives (DPD) with the General Data Protection Regulation (GDPR). The changes govern personal data stored by organizations. This could be customer data or employee data. (Voigt & Bussche 2017, 2.)

The GDPR aims to harmonize data privacy laws across Europe, in order to protect and empower all European Union citizens' information confidentiality and to reform the way organizations deal with data privacy. Unfortunately, with change, organizations are finding it challenging to comply with the new regulation. Not every entity recognizes the need for change (Lingard 2017). Organizations, on the other hand, have a lot of work to do in order to comply with the new regulation, failing to comply with the regulation results in heftily fined. (European Commission 2016.)

The thesis looks at how the subsidiary group companies are preparing to adapt to the new GDPR. Gathering this data allows the group HR to get insight on the preparation status of the subsidiary group companies in order to create a plan, initiate coordinated actions and to prepare the data protection activities to the required level. This is to ensure a streamlined documentation in relation to the GDPR compliance.

Professionally, this study helped the author gain in-depth knowledge on the General Data Protection Regulations. This, in turn**,** serves as a stepping stone towards the career path the author has chosen. The study is a current topic trending within the EU, which is required to be adapted by all organizations. The thesis research required the author to think deep, think outside of the box and allowed her to gain in-depth insight on facilitating HRM processes, as well as the overall field of her interest. The field of study is personally inter-

esting, which serves this research as a bonus and motivation to complete the research successfully.

1.2 Research Question

The aim of this thesis was to look at how the case company´s Human Resource departments prepared to implement the new legislation. The author had to investigate whether the HR managers were taking the necessary steps to move towards adopting to the General Data Protection Regulation that was set by the European Parliament and Council for storing personal data by 25 May 2018. The results of the study aimed to identify the procedures that are needed to be developed to comply with the regulation through content analysis.

The research question is worded as:
What areas of data protection does the case company need to develop further in order to comply with the GDPR requirements?

The research question is further divided into four Investigative questions (IQ), namely;
IQ 1. What actions have been taken to identify the process and databases that are currently used for employee data?
IQ 2. What actions have been taken to evaluate the processes and use of secured employee data systems?
IQ 3. What actions have been taken to commence the demonstration of training and communication to ensure employee engagement and understanding of the new changes?
IQ 4. What are the recommendations for further GDPR compliance?

Table 1 below presents the theoretical framework, research methods and results chapters for each investigative question.

Table 1. Overlay matrix

Investigative Question	Theoretical Framework*	Research Methods	Results (chapter)
IQ 1. What actions have been taken to identify the process and databases that are currently used?	HR GDPR framework	Questionnaire (a) i-v (b) i-v	4 and 5
IQ 2. What actions have been taken to evaluate the processes and imple-	HR GDPR framework	Questionnaire (a) i-v (b) i-v	4 and 5

mentation of a secured data?			
IQ3. What actions have been taken to commence the demonstration of the government model, training, and communication program?	HR GDPR framework	Questionnaire (a) i-ii (b) i-v (c) i-iv (d) i-iv	4 and 5
IQ4. What are the recommendations for further GDPR compliance?	HR GDPR framework	Questionnaire and desk-top research	5

An excel Gantt chart was created to illustrate the thesis research schedule. The chart acted a guiding tool for the author to manager her study and illustrated the duration of each activity. It further shows how it helped the author stay on track with the research schedule. (See appendix 2 for the Gantt chart).

1.3 Demarcation

This research primarily looked at the General Data Protection Regulations. The study concentrated on the steps and measures being taken by the subsidiary group companies in EU/EEA countries to adopt and comply with the new laws governing personal data. This study was conducted to ensure that all the subsidiary group companies are taking the necessary steps to follow the new regulations. The case company need to keep track of this and provide a report to the European Commission showing that the company is, in fact, complying with the law. Failing to protect the personal data of employees and breaching of data protection laws results in hefty fines of 20 million or 4% of the company's annual turnover worldwide. The amount fined is determined by which fine is bigger, meaning the greater amount is to be fined to a company that does not comply with the law.

The study primarily looked at how the subsidiary group companies are preparing for the GDPR and not the requirements set for documenting personal data or what exactly needs to be kept confidential by the Human Resources (HR). It concludes with suggestions on how the HR, executives and the management level can adapt to the change. The demarcation is so that the study is not too broad. Further studies need to be conducted to look at the requirements needed to document personal data of employees and whether the legislation change has been a success.

1.4 International Aspect and Link between HR with Study

The topic fulfils the international aspect required by concentrating on nine operating countries of the case company. The General Data Protection Regulation is an international legislation that concentrates on all the countries that are part of the EU, regardless of the companies are operating within the EU zone or not. The international aspect is so that the study is done by looking at how the different subsidiary group companies are approaching the change from Data Protection Directive to General Data Protection Regulation.

The General Data Protection Regulation is based on the value of accountability which directly has an influence on HR work. The link between HR and the GDPR is that the GDPR is concerned with personal data and the HR works with employee´s personal data. With the new regulations set through the GDPR, HR needs to comply with the law when dealing with personal data by: requesting for consent from data subjects, giving the right to change and deleting data, providing easy access to data for the data subjects, making sure to store clear data and giving the reason to why the data is being stored as well as ensure that data is stored in a secure system.

1.5 Benefits

Towards completing a successful thesis and internship for the case company, the author expected to complete a successful thesis study that can be used to see how the subsidiary group companies have been preparing to adapt to the changes. Regarding the company management, the study gave insight of the actions being taken to adapt to the change which is mandatory for the company. The management board can then make decisions to support the operating branches that are for instance not taking the necessary steps to comply with the new law governing personal data. The employee stakeholders can get a slight insight of how the HR has been complying with the new regulations, ensuring that their data is stored accordingly.

This study helped the author gain experience by getting insight on how international companies prepare themselves to deal with change and how they maneuver to adapt to it. Through the research study, the author gained a grasp on the requirements needed for obtaining and storing personal data. This is favourable for the author as the GDPR applies to all the companies operating within the EU, those that are registered and operating in other countries outside the EU, as well as those that deal with the data of EU citizens. The field of study was personally interesting, which served this research as a bonus and motivation to complete the research successfully.

1.6 Case Company

The thesis research was commissioned by an international company: Company X. The company operates in the chemical industry with several production sites within EU countries. The company's products are available worldwide. In 2016, the company recorded a headcount of a few thousand employees.

Since the company operates within the EU, it must comply with the legislation in relation to the General Data Protection Regulation. The results of the study will identify the areas that need to be further supported in the preparation for compliance of the GDPR.

1.7 Key Concepts

General Data Protection Regulation: Which is abbreviated as GDPR is a legal outline that was set by the European Commission to set guidelines for organizations when gathering and processing personal data of people within the EU. The regulatory framework provides people with the right for data confidentiality and principles for managing personal data, while also imposing hefty fines for organizations that fail to comply with the law. (Investopedia 2016.)

Data Protection Directives: Which is abbreviated as DPD is a directive which was set to regulate the processing of personal data by the European Union Commission, within the European Union. The directive protects personal data of EU citizens. It was first proposed by the Organization for Economic Co-operation and Development (Rouse 2018).

Human Resources management: Which is abbreviated at HRM is "a term used to describe formal systems devised for the management of people within an organization" (Encyclopedia 2014).

Personal Data: Is referred to as; information that relates to an identifiable person who can be directly or indirectly identified based on data factors such as identity number, physical appearance, bank account information, health etc. (Data Protection Commissioner 2007).

Change management: This is a term used to describe the guidance of how organizations formulate and support the staff to adapt to change successfully in order to drive a great outcome and success (Rouse 2018).

Privacy Impact Assessment: Is identified as an analysis tool used to identify and minimise privacy risks of processing personal data. It is also used in minimizing project risks (Freeman 2016).

Data Protection Officer: Is a designated person in an organization who develops, implements policies and carries out acts that are needed to meet the General Data Protection Regulation (Lord 2018).

2 Literature Review

The literature review starts by looking at the idea behind Data Protection Directive from 1995 which is the former law governing data protection. It is then followed by the General Data Protection Regulation which is yet to be enforced by the year 2018. The chapter further explains the different principles behind the General Data Protection Regulation, the idea behind this new regulation and how to lawfully process personal data. Furthermore, the chapter shows the GDPR theoretical framework that will be used to analyse the research results. To go in depth of the study and have a purposeful meaning, the author looks into the Finnish law governing personal data of employees and how the HRM handles employee data in relation with the study topic at hand.

2.1 Data Protection Directive (1995)

The Data Protection Directive from 1995 is the former legislation protecting European citizens' rights concerning personal data (Lynskey 2015, 46). It was first proposed by the Organization for Economic Co-operation and Development (OECD) (EUR-Lex 1995). The directive was set to direct the processing of personal data with an official directive of 95/46/EC, within the European Union until the year 2016. It protected personal data of EU citizens and foresaw the law of transferring personal data outside the EU to ensure full-on protection of an individual´s personal data. The directive was formed to harmonise the way data should be processed and stored within member states. However, according to Lynskey (2015, 47), the member states interpreted the legislation differently according to their local laws and further states that it is not clear whether the national courts have been correctly adopting and implementing the Data Protection Directive. Regardless of this, Lynskey (2015, 46) states that the Data Protection Directive presented several definitions and purposes that will remain in the General Data Protection Regulation.

The Data Protection Directive consisted of six principles that governed the legislation, which is as follow:

- Data should always be disclosed with the subjects' consent.
- The data collected should be used for the purpose it has been collected for and not for anything else. When collecting and storing personal data, it should be a legitimate, specific and explicit reason and not for any other matter that is dissenting for those purposes. **(**Directive 95/46/EC.)

- The data stored should be kept secured from abuse. The data is stored by a controller who should ensure that the organizational technical measures protect the personal data against unauthorised access, altercations, accidents or unlawful destructions. **(**Directive 95/46/EC.)
- The data subjects have the right to access and make a correction to the data stored. Under the Data Protection Directive, the data subject has the right to access his/her information, update or delete the data. The data subject also has the right to know the reason for processing the data, the recipients and who the data is disclosed to. **(**Directive 95/46/EC.)
- Storing of personal data should not be kept for a longer period than its primary purpose. Data should be deleted once it has reached its expiration period. All the member states are responsible for securing personal data that should be stored for longer periods for either statistical or historical use. Compared to the General Data Protection Regulation, data stored for a longer period should only be for archiving purposes, statistical or historical purpose according to Article 89 (1) of the Data Protection Directive. **(**Directive 95/46/EC.)

2.2 General Data Protection Regulation (2016)

The General Data Protection Regulation chapter gives insight on the legislation governing personal data. By the end of the chapter, you will understand its purpose, definition, and principles of the new EU regulation.

2.2.1 Introduction and Definition

The General Data Protection Regulation is a legal outline that was set by the European Parliament and Council to have guidelines for organizations when gathering and processing personal data of people within the EU. The regulation has similarities to the Data Protection Directive; which is to protect the rights of data subjects who are EU citizens and to regulate the processing of personal data by organizations (Lynskey 2015, 46). The regulatory framework provides people with the right to data confidentiality and principles for managing personal data, while also imposing hefty fines for entities that fail to comply with the law. (Voigt & Bussche 2017, 2.)

Comparing the GDPR to the DPD, the GDPR is not a directive but rather a regulation which is implemented to unify the supervisory of data across the EU. The DPD, on the other hand, sets rules to be implemented differently within different countries. In the GDPR, personal data is redefined to be information that could be used to identify an indi-

vidual while the DPD allowed different countries to identify personal data according to their own constitution. (Gross 2016, 1.)

The GDPR was adopted in 2016 and it is set to be enforced on 25th May 2018 by all member states of the European Union. The new regulation key privacy principles for HR include:

- Fair and lawful processing of personal data.
- Personal data should be acquired for one or more specified lawful purposes.
- The obtained personal data should be adequate and relevant and not for any other purposes.
- The obtained data should be kept up to date and accurate
- The obtained data should not be kept for longer purposes exceeding the purpose of its original use and timeframe.
- Secured and reliable technology should be used to store and process personal data to avoid accidental losses and unauthorized access.
- Personal data is not allowed to be transferred outside the European zone, unless the area the data is being transferred to has adequate level of data protection rights.
  (Voigt & Bussche 2017, 87.)

2.2.2 Consent

Obtaining data subject consent is as important in the new regulation as it was in the old directive (Bird & Bird 2017, 14). The General Data Protection Regulation and the Data Protection Directive share common grounds concerning data consent, although the new regulation has a wider definition of the term. The data controller who oversees the processing of personal data is responsible for obtaining consent from data subjects to collect their data. This can be done as simple as using a ticking box to show approval (Voight & Busshe 2017, 94). In addition to this, the data controller is responsible to process the data obtained in a transparent manner with clear information for the data subject, who should be able to easily access the data and know what his/her data is being used for (Lynskey, 2015, 14).

According to Article 4 (11) of the EU GDPR defines data consent to be “any freely given, specific, informed and unambiguous indication of the data subject´s wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

According to EUR-Lex regulation (2016, article 6), the data controller is forced to acquire consent every time the purpose of data processing changes. Entities that process data after the purpose has changed and haven't received data subjects consent have violated the law, thus, the “obscure consent” appears to be ruled out (Regulation 2016/679/EU art. 6, EUR-Lex, 2016). Lingard (2017) of the HR zone states that although the GDPR consent requirements seems to be relevant at first glance. However, relying on a consent-led approach to gather and process employee-related data, is in her context to be; administratively too complex to manage and possibly difficult in a wider context to the employees and, as well as the capability to assist in running the organization effectively. Lingard (2017) further explains that it is normally accepted by the employer to have the upper hand. With the new legislation, the employee may feel that if he/she refuses to give data consent to their employer, he/she will put their relationship in jeopardy, meaning that by law the employee has given consent not willingly.

The new data subject consent and access right included in the GDPR has a major impact on Human Resources. The organization should be able to prove that they have obtained the consent of the data subject and that the employees´ stored information complies with the regulation. (Javanainen 2017)

2.2.3 Enhanced Rights

The General Data Protection Regulation has strengthened the rights of individuals that were in the Data Protection Directive. Data protection controllers need to consider all the aspects relating to processing data, ultimately being able to demonstrate compliance with the new regulation and providing answers to data subjects. The strengthened rights include; access rights, right to be forgotten, right to restrict processing and right to object.

Data subjects have the right to access their data to ensure that it is correct and up to date and it is the controller´s responsibility to ensure that the data subjects can easily access their gathered data. Individual´s access requests may possibly place a burden on the administration with the new regulation as data subjects may feel the right to exercise their rights (Lingard 2017). The right to be forgotten already exists under the Data Protection Directive. However, the right is strengthened in the regulation by having the data controller demonstrate that the entity is complying with the law. Individuals have the right to be forgotten if the data is being processed unlawfully, the data is no longer serving the purpose for which it was collected or the individual has withdrawn his/her consent. (Bird & Bird 2017, 29.)

The right to restrict processing replaces the Data Protection Directive right to block. According to the Bird & Bird (2017, 30) guide to the General Data Protection Regulation, if an individual restricts further processing of personal data, the data controller may continue to store the personal data only until consent has been given or the processing is necessary for establishment. When the HR processes data automatically, the system used should have restrictions affected by technical means that block or transfer the data to other systems and send a notification to the controller who should overlook that the data is temporarily blocked or moved to a separate system. (Bird & Bird 2017, 30.)

2.2.4 Lawfulness, Fairness, and Transparency

According to the EU GDPR article 5, section 1, states that personal data should be processed lawfully, fairly and in a transparent manner. Thus, the processing should only take place when it is done legally and when consent has been given to do so. With the increased transparency under the GDPR, the data subject should be able to understand clearly what their personal data is being used for. Therefore, it needs to be transparent about what their personal data is being used for and to what extent it will be used. The article further states that processing of personal data needs to be legitimate and explicit.

Voight & Busshe (20017, 88) states that the transparency of personal data requires to: make data subjects aware of the rules, safety, and risks of processing their personal data. Thus, explaining how data subjects can exercise their rights too. Moreover, transparency requires getting confirmation to process data and communicating the process actions. All information concerning processing should be easily accessible and understood by all individuals. All data subjects have information rights stipulated in the EU GDPR article 13 to 14, section 5 and data controllers should be able to provide proof of compliance which will influence the privacy statements and notifications.

2.2.5 Integrity and Confidentiality

Under The General Data Protection Regulation, the legislation requires processing of personal data to be done with integrity and confidentiality. Processing data should be done in a manner that ensures data security. Thus, when HR is processing employee data, it needs to use appropriate technical support to protect data from unauthorised access, damages or accidental losses. This is one of the main principles in the EU GDPR (Voight & Busshe 2017, 92)

2.2.6 Accountability

The GDPR comprises requirements that administer governance and accountability. These complement the GDPR's transparency requirements. While accountability has been formally implied as one of the principles of data protection, the new regulation puts more prominence to elevate its meaning. Under the new legislation, controllers are held accountable to a certain extent for providing the required materials expected from an organization to show compliance. (Voight & Busshe 2017, 237.)

The General Data Protection Regulation has integrated the principle of accountability for entities to demonstrate their actions towards compliance through the use of appropriate technical and organizational measures. The Human Resources play a role in ensuring that the handling of personal data complies with the legislation. Measures included ensuring accountability compliance include: stating the purpose of processing employee data, how it´s done, for how long and an overall documented process of the procedures, including the Data Protection Officer who is responsible for the organizations' operations and planning. (European Data Protection Supervisor 2017, 1.)

When adapting to the new regulation, the HR plays a big role in facilitating the employee data processes of GDPR. The HR department needs to keep track and collect large volumes and variety of employee information to access the organizations status towards adapting to the new regulation. Part of GDPR compliance includes selecting a Data Protection Officer who is responsible for providing electronic copies of where the subject´s data is stored and for what reason. With this workload, the group HR gathers the status of the sub-operating countries to follow up the actions taken towards GDPR compliance. Furthermore, a plan is then set up to initiate coordinated actions to ensure a streamlined process documentation in relation to the GDPR.

2.3 Data Processing

Under the GDPR, data processing requirements have become tougher. With the newly defined terms, data processing is defined as operations performed on personal data, either manually or by automated means (Regulation (EU) 2016/679). Handling of personal data such as gathering, recording, forming, configuring, storing and deleting is considered as processing (Voight & Busshe 2017, 9).

Data controllers need to grasp the concept of storage limitations, data minimization, and pseudonym data. The EUR-Lex (2016) GDPR states that data should not be stored without a good reason. Moreover, data needs to be processed at minimal, meaning that only purpose related data should be processed to be regarded as legal processing. Another

form of processing data is through pseudonymous data, which protects personal data from harm.

2.3.1 Data Storage and Minimization

The GDPR EUR-Lex (rec 39) states that personal data should be relevant, adequate and restricted to what is considered relevant in relation to the processing of data. Data storage and minimization is part of the Data Protection Directive with a comparable meaning. However, the GDPR requires a stricter processing. (Voight & Busshe 2017, 90.) Article 5, section 10 of the Regulation states that it is not an obligation to process data at an extreme minimization, but data should be processed in a minimal manner that is adequate to the prime reason of processing. Data minimization aims to reduce irrelevant data collection at the least possible level of purpose processing (Voight & Busshe 2017, 90).

Data storage and minimization can be implemented through the Privacy by Design and Privacy by Default concept. The principle of storage limitation works in relation to the role of data minimization. An overload of irrelevant data needs to be deleted without undue delay. (Voight & Busshe 2017, 91.)

2.3.2 Pseudonymous Data

Pseudonymising of data is one of the ways entities can use to process data in a secure way that does not link a specific data subject. The GDPR EUR-Lex (2016) states that pseudonymising can be used as a mean of protecting personal data and entities. Organizations can use this to protect themselves from conceivable data breaches. (EUR-Lex 2016, article 4).

According to the GDPR (Regulation (EU) 2016/769), pseudonymising of data is defined as, “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

When data subjects give consent for data processing and the data is so that it is possible to identify a specific person, the data subject should be able to gain access to his/her data for rectification or erasure. However, data controllers can deny giving data subjects access if the controller is able to demonstrate that the data cannot be linked to a specific person, therefore, hard to identify a data subject through Pseudonymised data. When data

is Pseudonymised and the controller cannot identify a data subject, they don't have to give access to a person for rectification or erasure (Regulation (EU) 2016/769.)

2.3.3 Breaching Of Data

An organization may have an incident whereby data has been lost, changed without concern, disclosed without authorisation or otherwise stored and processed without data subject concern. The EUR-Lex (Regulation (EU) 2016/769) then states that in such situations, it is obliged for data processors to notify the data controllers without undue delay. The data controllers are then responsible to notify the supervisory authorities within 72 hours of becoming aware of the incident. If the timing is not met, the data controllers are responsible to give reasons to the supervisory authority. All breaches need to be reported to the supervisory authorities. Data controllers are held liable to communicate and notify the data subjects about the personal data breach. (Bird & Bird 2017, 38.) Failure to meet the GDPR requirements risks the organization to be fined a fee of up to €20 000 000 or 4% of the organizations worldwide annual turnover, whichever is higher (EUR-Lex 2016, article 5).

According to Hooson (2017, 2), most of the data breaches that occur in organizations are caused by employee negligence. There have been cases reported whereby organizations have not destroyed data that should´ve been destroyed. All entities need to be attentive and aware of their actions to comply with the General Data Protection Regulation.

Figure 1. HR GDPR framework (Council of the European Union 2015).

The above HR GDPR framework works as a guiding tool in comparing the research question and studied theory to the findings. Every bubble surrounding the HR GDPR framework is a principle regulation that the HR needs to follow to comply with the GDPR. This framework will be used to see the status of the operating companies in relation to the framework.

2.4 Data Protection Directive Vs General Data Protection Regulation

The replacement of the Data Protection Directive has been made to be stricter. With the GDPR, the new legislation binds all member states with an explicit new definition of terms and concepts which are regulatory, while the old legislation acted as a directive to be implemented through national legislation. However, the General Data Protection Regulation still has a lot of similar terms adopted from the Data Protection Directive.

Table 2 below presents the difference between the Data Protection Directive and the General Data Protection Regulation.

Table 2. DPA vs GDPR

Area of comparison	**Data Protection Directive**	**General Data Protection Regulation**
Data subject rights	Right to erasure, rectification, and right to copy of data by payment.	Explicit rights to data erasure and rectification. No required fee for copy of data.
Consent	Consent free given, informed and specific.	Clear confirmation from data subject with the ability to withdraw.
Accountability	Limited accountability	Fully explicit accountability
Data Protection Officer	There is no need for a Data Protection Officer.	A Data Protection Officer is needed by an organization with over 250 employees.
Data Breach	No need to report data breaches.	Data breaches need to be reported within 72 hours to the supervisory authority.
Penalty	A fine of 500 000 or 1% of the organization's annual turnover.	A fine of 20 million or 4% of the organization´s annual turnover.

2.5 Finnish Law on Personal Data

The Finnish law governing personal data looks at the general rules of processing personal data, the data subject rights, storing and securing personal data. Chapter 1, Section 1 of the Personal Data Act (523/1999) defines personal data as information of an individual´s personal matters and characteristics where this information can be traced to the data subject. The act applies to data controllers who process personal data in the Finnish territory.

Like the Data Protection Directive, the Finnish law has similar laws governing personal data. Chapter 2, Section 5 of the Personal Data Act (523/1999) states that processing of personal data should be done lawfully, carefully and in a way that the data is secured from harm. The data should be processed in an appropriate and justifiable manner, providing a reason for processing data. The Finnish law gives rights to data subjects. Chapter 6, section 24 of the Personal Data Act (523/1999) states that when personal data is collected, the data controller should give information of the processing of data. This information, such as the controller's representative should be provided at the time of collecting and recording the data. Moreover, data subjects have the right to access and rectification, regardless of the privacy provisions. All data subjects have the right to access their data

stored in Finland, however, the controller may charge a minimal provision fee of access to the data. The data controller is responsible to rectify or erase personal data, either by own initiative or by request of the data subject without undue delay. If the data controller rectifies or erases data, he or she should notify the data subject and the recipients whom the data is disclosed to. Chapter 7, section 32 of the personal data act (523/1999) states that entities are responsible to carry out technical measures for securing personal data from unlawful destructions, accidents, and unauthorised access. According to chapter 9, section 39 of the Personal Data Act (523/1999) Data that is no longer relevant for operations and processing should be erased and destroyed without undue delay. The data protection Ombudsman in Finland has the right to access personal data regardless of confidentiality provisions.

2.6 Human Resources: Handling Employee Data in Relation with the Law

Entities typically store different employee information, often regarded as personal data files as a way of documenting the employee´s relationship with the organization. Additionally, the Human Resources is required to handle and process personal data according to the national legislation. Organizations collect a substantial amount of personal information from their employees and use the collected data for a variety of purposes: from assessing vacancy applications during on boarding process to administrating payroll and employee benefits within the HR department (Winthrop, P & Pittman, S 2011).

There are several HR processes that deal with the employees´ personal information. Some of the HR data processes include the recruitment process, the appraisal and compensation process and the exit management process. To make an example of the recruitment process, minimal data is usually obtained from job candidates. When an employee is hired, the employee gives more of his/her information to the employer. The HR department then processes this information into the organizations files. During processing of data, the Human Resource is responsible for maintaining the confidentiality of the employees´ data. As a result, handling of employee data in HR is complex and should be handled attentively that the data is kept accurate and secured. The Human Resource department is responsible for creating policies and procedures for handling the employees' data. Under their action plan of processing and storing personal data, the HR department ask themselves the following questions; what personal data will they process? Why is the data being processed? Where is the data stored? Whom has access rights and for how long will it be retained? (Addlesshaw Goddard 2017.)

The Human Resource Management is not only responsible for keeping the employees sensitive data and managing it, but it is also responsible for protecting the information under the national laws governing confidentiality (HR Insight 2013). When creating privacy policies for HR processes, the HR needs to identify what information is supposed to be kept confidential and follow the necessary procedures to keep the employees´ information private.

There is sensitive data that needs to be kept confidential at all times. An employee's sensitive data is regarded to be data that relates to the data subject. This data includes criminal records, sexual life, political beliefs and, or ethnic origins. Under personal information, the HR protects the employees´; social security number, marital status and the date of birth. When evaluation of performance takes place the following are considered to be confidential; the warning and disciplinary notices, performance review and promotions. Furthermore, the department is responsible or payroll, compensation and benefits. When processing under those acts, the following information is regarded as confidential data; salary, authorisation for withholding pay, bonuses and benefit information. Health and medical information is also processed by the HR. The employees' information need to be kept secured and confidential under the local national laws governing personal data confidentiality. Information such as the medical exam details and the insurances of the employee need to be kept secured at all times. Information under investigation records such as the employees' violation of policies, complaints of harassment or safety issues is also regarded to be sensitive, and therefore, should be kept confidential. (HR Insight 2013; Liontis 2017.)

Employee data management is a lever for fostering a dialogue between the HR, trade unions and employee representatives. Meaning that when the HR handles employee data, they should be attentive to the information that the employees consider to be sensitive and private. A question may arise of; who secures data in an organization? Ultimately, in an organization the Information and Technology Department is considered to secure data, but the Human Resource Department is where the employee data is managed. The HR has majority of access to manage the data while, IT is concerned with the protection of data, whereby, the access rights to the data and security is enforced by the IT department. (Lestrange 2015.)

Access to personal data is usually restricted to HR, Executive officers, and Management level. The HR department has a data controller who is responsible for processing and handling employee data in a lawful and confidential manner. Data can be stored in digital software systems, physically in the supervisor's office, payroll office or the organizations vice presidents office. Employees can access their personal files to rectify or block their

data from being processed. If an employee choses to block their data from being processed in HRM, this may be challenging for the organization to run their records smoothly and could possibly end in job loss. (Webster 2013, 61.) Furthermore, according to the Finnish Personal Data Act (523/1999), No data older than 10 years should be stored. After 10 years, the data needs to be disposed.

There are three direct stakeholders in HR. The stakeholders are the owners, the employees and the external parties. These stakeholders are involved in some of the HR operations. Processing of employee data needs clear guidelines of what is being processed, what type of information is being processed, how much of an employee´s data is being transferred and who is responsible for getting certain information. Owners of entities usually have access to all the company´s data, including that of employees. This however does not imply to all entities. Some entities have strict regulations on the amount of data owners have of employees for security reasons. There are certain employees who are responsible for handling and processing employee data. Not all the employees have access to data. Moreover, some entities operate with external parties such as recruitment agencies. The HR and external agencies share relevant and minimal information of employees or potential employees. This is done within the strict laws of transferring data to external parties.

There are several challenges within the HR department when it involves data entry. Firstly, there is a need to understand that there are two ways of entering and processing data, namely; manual entry and digital entry. Manual data entry and processing can be tricky and mind numbing. It usually involves transferring data from a physical state to digital, systematic based documents where other procedures are involved as well. With evolving technology, organizations and HR departments use less of manual data entry and more of computers through advanced technology. This is because there are challenges to manual data entry. Challenges such as money loss from less efficiency, human errors, misinterpretation and time consuming. (Biels 2015.)

To avoid mishaps, HR carries out training programs for its staff and senior managers. The program involves training the attendees for data protection requirements. It gives the attendants a solid understanding of the legal requirements with practical practice for the HR function in the organization. Furthermore, the training includes analysing data protection principles, understanding HR related data protection requirements, apprehend the evolving practices of data protection and how the law influences HR practises. (Cork Chamber 2017.)

3 Methodology

This chapter looks at the research design, research question, the investigative questions and the research method used. It further explains the data collection process, the risks of the research and how they are managed. The possible reliability and validity of the study research in hand are later discussed at the end of the chapter.

The research question has been created based on the company needs to understand where more support could be given towards successfully complying to the GDPR. From the research question, four investigative questions have been formed to assist in formulating an answer to the research question.

3.1 Research Design

The research was designed carefully to the need of the case company. After developing the questionnaire, the author needed to keep in mind of the issues that may arise. One of the issues considered during the study is the fact that the GDPR only concerned EU countries. Therefore, only the subsidiary HR group companies received the questionnaire. Another consideration was the time frame the respondent had to answer the questionnaire. The respondent had two weeks to send their response back to the author. This time frame allowed the respondents to contact the author for further questions and to make sure that there is enough time between the time responses are received, analysed and the GDPR legislation enforcement date. The development of the questionnaire and the study timeframe was calculated and planned that everything goes smooth and accordingly. Below is the planned research method, stating every phase and stage.

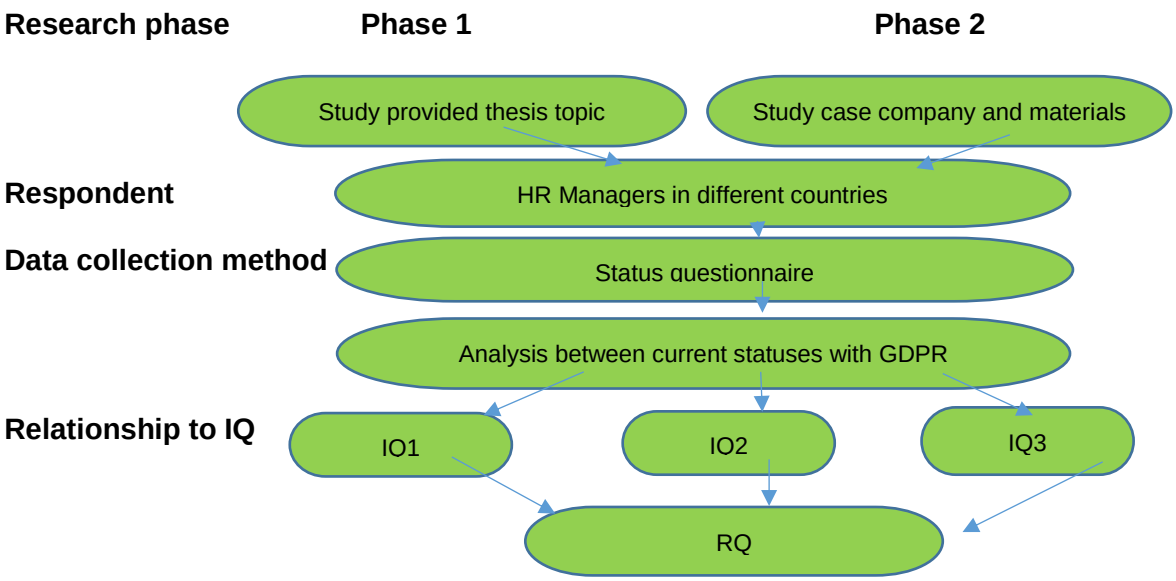

Figure 2. Research Method

The research study started when the case company provided a topic of interest in phase 1, followed by studying the company's´ processes through secondary data research and the theory related to the study in phase 2. The candidates for the questionnaire were HR managers from different subsidiary group companies who were responsible for employee data and were preparing for GDPR. The form of data collection method used is both qualitative and quantitative status questionnaire that gave the candidates an option to choose from which indicates their status towards GDPR. When the qualitative data was gathered, a deductively based analytical procedure further took place where a conceptual framework was used for the gathered data to create an explanation building as a form of deductive based analysis (Yin 2003). The HR GDPR conceptual framework was used to analyse the gathered data.

This thesis included a secondary data research. The literature was extracted from sources such as articles, books, journals, and reports. Valuable and reliable internet sources were used to study the background of the GDPR and they were used to provide the theoretical framework of the thesis study. The literature was properly reviewed and chosen critically to provide information that is accurate and relevant.

3.2 Data Collection

The questionnaire was designed based on the several GDPR requirements that are coherent to the literature review. It was done this way to get clear information on various processes and steps taken. The key points in the investigative questions are: identifying, evaluating and implementing which is a general process used in change management. Every question is answered by choosing from the available 3 options- ready, in progress or not ready. This indicated whether the HR has already completed the activity, is currently working on it or has not started with any actions. The questionnaire design and structure enable a clear reporting structure for the entity. The thesis is a research-based study through content analysis. See appendix 1 for the status questionnaire. Table 3 below shows the status questionnaire design frame.

Table 3. Design of status questionnaire

Investigative question (IQ) 1-3	Status Questionnaire
IQ 1. Identification	a) i- v b) i- v
IQ 2. Evaluation	a) i- v b) i- v
IQ 3. Implementation through compliance demonstration	a) i- ii b) i- v c) i- iv d) i- iv

The first investigative question looked at identifying the current processes being used by HR managers when handling employee data. This for an example helps to identify archives containing employee data that need to be deleted as a regulation of data minimization principle. The GDPR requires the employee data to be stored in a secured system. Therefore, the second investigative question looks at the actions taken by HR managers to ensure employee data protection. The third investigative question aimed to see whether the HR managers have begun training and communicating the explicit changes of handling employee data.

Because the study was conducted through both qualitative and quantitative research approach, utilizing methods such as questionnaires as a primary source of information and secondary desk-top data research, results provide more meaningful content. Qualitative research is explained to be research done to obtain data that has not been quantified and can be used as a product of other research strategies (Saunders & Lewis, Thorrnhill 2009, 482). The data obtained through quantitative research can further be analysed through a deductively or an inductively analysis. The study suits best to be analysed through the deductive analysis whereby it creates an explanation building. For the data to be useful and have its means understood, an analysis of the qualitative data is conducted using conceptualization. (Yin 2003.)

The data was collected through purposive sampling, which means that the candidates were chosen on a basis of those that the GDPR effect (Recker 2013). The GDPR applies to all EU and EEA countries that hold data of EU citizens. However, global companies handling EU citizen's employee data need to comply with the regulation. Given the wide territorial scope of the case company, the population has been sampled to those in the EU and EEA. After sampling the population, HR Managers from nine countries remained to be the target research of the case company. Without sampling, the population would have been too large to conduct the research and the data obtained would´ve been irrelevant

from those subsidiary group countries that are not part of the EU/EEA. Moreover, the results would have held no purpose.

A week after sending out the questionnaires, a reminder was sent to the HR Managers to respond in time. Out of the nine questionnaires sent to the subsidiary group company HR Managers, only five responded, having a 78% response rate. Reason being that the two outstanding responses were too busy occupied with other work. This was communicated to the commissioning company group HR.

A status questionnaire was used for the data collection. This questionnaire was sent to nine HR managers across different sub-operating countries to look at how these managers are preparing for the GDPR and at what stage they are at, at doing so. Since the HR managers are responsible for the handling of employee data, they were our candidates to bring answers as to what stage they were at adapting to the change. The informants were motivated by informing them about how their input and co-operation is vital for the company in avoiding hefty fines.

The questionnaire was created on an excel file that was sent by e-mail to the HR managers. This is the best option to obtain the data as it is a secured form to obtain data for the commissioning company, which I'm currently working for as an intern. The company's privacy and regulation policies state that internal data should remain secured.

The questionnaire was designed carefully to the need of the company. It was well structured and acted as a guiding step towards adapting to the GDPR. The results of the study were then be analysed. This identified the areas that needed support towards the regulation compliance.

3.3 Risks and Risk Management

Since the research included a secondary data research, some sources were outdated with bad articulation of the article, non- factual or not of value to the study (Saunders, Lewis, & Thornhill 2012, 82). To minimise these risks, the author searched for high-quality sources that are reliable. This was done by using materials from the EU GDPR organization site, material that is not older than 3 years. Other materials that was used had to be of high-quality books that provided the theory of the study.

One of the risks this study faced is a low response rate. The author tried to avoid this by sending a reminder to the candidates and motivating them to respond, informing them that their response is of importance to the company. During this stage the author was not wor-

ried about this risk as she was made assure that the HR Managers always respond on time and they know their role in working towards the GDPR compliance.

3.4 Reliability and Validity

To make this study reliable, a well-structured questionnaire was created depending on the interest of the group HR. The results were be obtained through primary research and evaluated with secondary data. The data obtained was be referenced correctly according to the Haaga-Helia UAS referencing guidelines and the data was interpreted with academic integrity. All the other necessary information such as figures and appendices are clearly stated to allow a further study.

The author trusts that she has not made any mistakes starting from the development of the questionnaire to the analysis of the results. The questionnaire was developed together with the HR group Manager, were by it has been changed a couple of times for it to be more precise and generate understandable, purposeful results. Moreover, the author followed the guiding principles to a successful research, following the legislation components needed to build and analyse the study.

Looking at the response rate of the questionnaires, the five responses received were from the top performing subsidiary group companies. Out of the five that responded, Germany was the only country that stated that all their HR operations already follow the General Data Protection Regulations, which was unexpected. For some of these status responses, documents were shared on the company´s SharePoint to show validity of their operations. Thus, the results and the discussion are only valid for the case company and its subsidiary group companies that have responded. The countries that did not respond to the questionnaire included; the Balkan countries, Norway, Poland and Denmark. After evaluation, the responses looked to be of quality and truthful considering the time of response and the attached documents. Since the case company chose to be anonymised, the documents sent as an attachment to the questionnaire could not be added to the thesis report as it would directly link the thesis study to the case company, which is not the plan. The documents however showed to be resourceful and informative during this study.

4 Results

In this chapter, the author presents the results from the respondents. The results will be presented by starting with the identification, evaluation and then the implementation through compliance demonstration IQ. The author will present the most relevant and significant findings.

4.1 HRM Status towards GDPR Requirements

There are a lot of requirements to be considered when following the GDPR. The first phase has to do with identifying the processes and the databases the company is currently using. The following steps usually require an evaluation of the processes and systems used. This enable s the company to figure out what is important, relevant and what should be deleted or updated. The company therefore moves to documenting their processes, policies and creates their government model. During the last phase, the company trains their employees and tests their new procedures. This is the format used to create the questionnaire and present results stated below.

4.2 Identifying the Processes and Databases

Investigative question 1 (a) looked at identifying and analysing the status of the current processes in each country. Finland, Sweden, Estonia, and Lithuania stated that they are currently in the process of listing all processes and systems containing personal data, as well as listing all the parties who have access to the employees' data. All the countries have been asked to identify physical archives containing personal data, Estonia and Lithuania show that they have already identified these while Finland and Sweden are yet to complete the process. However, all the countries have indicated that they´re in the process of identifying their electronic archives that contain the employees' personal data.

Investigative question 1 (b) looked at analysing data content that is considered to be relevant for the new organizational setup. Finland, Sweden, and Estonia stated that they are in the process of ensuring the ownership and validity of each identified process containing personal data, while Lithuania shows to be ready. The General Data Protection Regulation states that a data privacy coordinator should be selected and named. Finland, Estonia, and Lithuania have identified their data privacy coordinator while Sweden is in the process of selecting one. All the countries show that they´re in the process of cleaning out unnecessary achieves and systems containing outdated personal data, except for Lithuania who has already done this. Lithuania identified to have not started anonymizing personal data that will be shared outside the HR department, while the rest of the countries

show that they´re in the process of doing so. Unnecessary systems need to be discontinued. Finland and Estonia are in the process of getting rid of unnecessary systems, Sweden has not started while Lithuania has already done so.

Overall, comparing all the countries in IQ1, Lithuania shows to be ahead of the other countries. Their HR manager shows to be ready for most of the processes needed to be completed in the identification and analysis stage.

4.3 Evaluation of Data Processes and Implementation of Secured Data

The investigative question 2 focused on the evaluation and implementation phase. IQ 2 (a) looked at identifying the current status of each country´s streamline and validation of the necessary processes and databases containing the employees' personal data. Both Finland, Sweden, and Estonia indicated that they´re in the process towards completing the phase. Lithuania, on the other hand, indicated that they've not started yet. IQ 2 (b) looks into privacy and protection. Finland and Estonia are the only countries showing that they´re in the process of changing their software to an automated database storage. Sweden and Lithuania indicated that they have not started yet. Estonia shows to have the privacy and protection phase in progress, whilst Finland, Sweden, and Lithuania have not started yet.

4.4 Demonstration of the Government Model

The third investigative question looks at the HR manager’s readiness to demonstrate GDPR compliance and follow up development plans for improvements. Under communication, all the countries have indicated to have not started with the translation and compliance of the five main privacy policies of employee data. Moreover, none of the countries started with creating a communication plan that ensures organization awareness. Under the training stage, Finland and Sweden show to be in the process of HR and managers training. The remaining countries haven't started yet. All the countries also indicated that they´ve not started with assistant service training, informing the employee's representatives about the employees' processes and creating an employee awareness campaign for handling personal data.

The results in investigative question 3 a and b indicate that other than Germany, all the countries have not started preparing the documents needed in cases of data breaches, if the employee asks for their data to be removed or show what data the company is holding, outsourcing processes of personal data and starting to gather new personal data. Moreover, all the countries have not started working on the governance model that ensures ongoing practices that personal data is up-to-date, roles and responsibilities to ana-

lyse change have been designated and the creation of internal audit practice model to monitor the organizations GDPR compliance is in place.

Overall, the results show that most of the countries were not yet ready and were going through the process of stabilizing and adopting the General Data Protection Regulations. In hopes of GDPR compliance, the organization needs to be ready by 25th May 2018. The author believes that there is enough time for the organization to organise everything in accordance to the new regulation.

Table 4. Compilation of key results per investigative question

Sub-IQ´s	**Estonia**	**Finland**	**Germany**	**Lithuania**	**Sweden**
Identifying processes	In progress	In progress	Ready	In progress	In progress
Analysis of data	In progress	In progress	Ready	Ready	In progress
Validating Processes	In progress	In progress	Ready	Not started	In progress
Privacy protection	In progress	Not started	Ready	Not started	Not started
Communication plan	Not started	Not started	Ready	Not started	Not started
Training of employees	Not started	In progress	Ready	Not started	Not started
Documenting processes	Not started	Not started	Ready	Not started	Not started
Government model	Not started	Not started	Ready	Not started	Not started

5 Discussion

In this chapter, the author presents data from the previous chapter in relation to the theory provided in chapter 2. Based on the findings, the author will then draw a conclusion to the recommended steps for HR towards GDPR compliance and offer suggestions for further research. Finally, the author assesses her personal learning on the study topic, the development the study created and how the study plays a role in the career path she has chosen.

5.1 Key Results

With the first investigative question, the author aimed to get the status of the HR Managers on identifying the current processes and databases that were existing in the company for processing personal data. This is the first phase of change management. Hence, the General Data Protection Regulation requires entities to take account whether processing of personal data is compatible with the initial purpose of collecting the data. This is referred to the theory provided in chapter 2.3. Majority of the countries indicted to be in the process towards fulfilling the identification and analysis phase. With the limited timeframe remaining, it raises a question of whether the operating countries will be ready on time.

The organization is required to analyse data content which is considered to be relevant to the current organization set up. Hence, all the countries were in the process of owning ownership of data processing, cleaning archives and discontinuing unnecessary systems. In relation to this, a Data Protection Officer was needed to oversee the data protection strategies in the organization to ensure compliance with the General Data Protection Regulation requirements. The officer should Pseudonymise relevant personal data to ensure that it can´t be linked to a specific person. The selection of a Data Protection Officer and the pseudonymising of personal data referrers to the theory chapter 2.2.6 and 2.3.3, which clearly states the requirements.

The privacy protection design and default questions were created to see how active the countries are to implement privacy for the data subjects. The results indicated that the subsidiary group companies were not started with the act of privacy protection by design and default. This could be that the data protection by design is considered to be challenging because it follows a new legal view that is regulated by the General Data Protection Regulation. Moreover, the data controller needed to measure and create techniques that effectively protect the data subject rights. This is done before and during implementation.

The new regulation requires a restriction on automated processing of personal data. Looking at the results obtained, officers responsible for processing personal data need to be vigilant when it comes to automated processing. The operating entities need to ensure that during their adaptation phase, the automated software used is examined and altered were necessary, remembering that the employees have the right to subject to decisions made solely on automated processing. Since all the countries have indicated to have not started or in the process of privacy protection by design and default, HR Managers and those handling employee data should keep in mind the employees' rights to be forgotten (refer to theory in chapter 2.2.3). This means that when data no longer serves its initial purpose, it should be deleted unless data consent is given by the data subject. This protects the employees from having their data processed for unnecessary transactions.

Furthermore, transferring employees´ data outside the EEA continues to be prohibited under the new regulation. However, the requirements from the Data Protection Directive remain the same with slight changes. These changes are to be considered by HR. The transfer of employee data is only acceptable where there is an approved code of conduct. (Find reference to this in chapter 2.2.1).

The last investigative question looks at the status of demonstrating the General Data Protection Regulation compliance, as well as a follow-up development. Entities handling personal data are responsible for documenting their compliance and providing proof to the European Union Council. From the provided information all the operating countries have not started demonstrating their compliance. The countries, however, need to have a Privacy Impact Assessment. The Privacy Impact Assessment will aim to identify and diminish the non-compliance risks which the GDPR provides guidance for this process. It is a requirement processing activity before the GDPR is commenced. In reference to the theory in chapter 2.2.6, entities are held accountable for all their actions.

Moreover, entities are required to keep documented records of all their employee data processing activities. In case of data breaches or employees asks about their data, controllers should be able to obtain records and provide them when needed. Furthermore, data breaches should be recorded and communicated without undue delay. A communication plan should be developed and communicated with the data subjects and the European Data Protection Board.

On an overall basis, the subsidiary group companies seem not to be ready for the enforcement date of the General Data Protection Regulation. An operation strategy to get all the countries on the same wavelength to adopt the regulation quick needs to be devel-

oped. The author believes that there is enough time to plan and implement a successful plan before May 2018.

5.2 Recommended Steps for HR towards GDPR Compliance

As the case company changes its operations to be centralised, an action plan for HR´s policies and procedures was needed towards GDPR compliance. Firstly, the HR is recommended to audit their data in order to understand what documents, policies and procedures are currently compliant to the GDPR. For the documents and procedures that are not; need to be terminated and erased. This refers to the theory provided in chapter 2.3. To move on, a competent Data Protection Officer then needs to be identified. The DPO ensures GDPR organizational compliance.

Furthermore, the HR Manager and the DPO need to understand the legal aspects for processing different types of personal data. One type of personal data is that which is sensitive. Sensitive personal data such as the employees' political opinions, sexual life or religious beliefs etc. need to be processed differently according to the conditions provided by the regulation.

It is then recommended for the HR to develop and implement the following policies:

- Data Retention and Disposable Policy- as part of the GDPR requirements, data should not be retained for more than its initial purpose. The case company should, therefore, be able to demonstrate that data has been retained for an appropriate period of time. This can be demonstrated by creating a retention policy with a time frame and disposable procedures known as the data destruction procedures. According to the Finnish law, employee data is allowed to be stored up to ten year. After ten years the data then needs to be disposed. The HR Specialist is usually responsible for monitoring this procedure. Disposing documents can be done in two ways; either by shredding physical archived documents – which is to secure the safety of the personal data or by deleting digital stored documents out of the company's software.
- Subject Access Request Policy- new policies should be updated and created according to the GDPR requirements. This policy is created for those responsible for handling access requests and responding in a timely manner. According to the regulation, the company then needs to select a Data Protection Officer who is responsible for compliance when developing and implementing policies and procedures for handling personal data. The DPO works together with the HR manager in

communicating the development and implementation of policies regarding processes of handling personal data.

- Data Breach Plan and Notification- the Data Protection Officer is responsible for creating a well-developed procedure plan. This procedure plan is needed to ensure that data breaches are handled accordingly and in line with the GDPR requirements. The plan includes training the employees on how to act when they´ve been aware of the data breach, communicating the data breaches with the manager and carrying out the disciplinary policy acts when data has been breached.

It is important to understand that the regulation has significantly enhanced the employees' rights. HR is therefore responsible for processing the data accordingly. Processing the employees' data should be done with the data subject´s consent. A detailed set of information is then provided to the data subject stating the purpose of processing the data and the retention period. The data processors should also remember the employees' rights to be forgotten and rectified. With that being said, a systematic procedure is recommended to give the data subject access rights to their information whereby they could rectify the information or chose to be forgotten. This is in reference to chapter 2.2.2 and 2.3 that gives insight on data consent and processing.

After evaluating the policies, upgrading them and creating compliant procedures, the DPO needs to create a communication plan. This communication plan consists of whom the policies and changes will be communicated with, when the communication will take place, the key message and the best channels used to communicate. The HR manager and the DPO will then need to organise a training for organizational teams about the changes coming into force.

Moreover, it is important for HR to recognise that the regulation does not provide a full set of rules to be followed. It is, therefore, recommendable that they remain aware of the nation's laws especially those that are related to employee and HR data. The HR Manager is then responsible of assigning who has the competencies to act as a Data Protection Officer when designing, monitoring the data procedures, evaluating and correcting all the processes related to this.

5.3 Further Research

As a recommendation for further study, the author suggests further research into how European companies have adapted to the General Data Protection Regulation successfully. Looking into what was challenging during adaptation and how to overcome the challenges. A more detailed research is recommended on the guiding steps or a detailed checklist

to adapting to the regulation. Furthermore, this study could be fostered into the study of a detailed GDPR compliance document.

5.4 Personal Learning

For this final section, the author will be reflecting on what has been learned during the study, what she has developed and how the study has contributed to the career path she has chosen. The author had a great opportunity to learn more about one of the current topics trending around Europe in the EU law.

During the study, the author learned more about the EU data laws that govern personal data. This was not only from a HR´s perspective but as well as the technical and third-party involvements. She learned of the needed requirements when processing personal data, what improvements have been enhanced for the data subject´s rights and how to act when one becomes aware of data breaches.

Moreover, the author learned that during big organizational changes its best for the operations to be centralised in order for all the subsidiary group companies to follow the same instruction accordingly, on time and successfully. This enables a unified organization with similar standards throughout. The author also learned that it takes a lot of work to plan, organise and implement policies and changes. Talking about planning, the author learned to view and think outside of the box during data collection and analysis. As the author received a response from the HR, she had to critically view information in order to build a concrete foundation for future research. The study turned out to be more useful and fruitful than expected by learning more about the case company and how tasks are carried out.

Studying business and choosing to specialise in Human Resources, this study played a significant role in the career path the author has chosen. It gave a broad outlook on understanding not only the national laws but those of the EU as well.

References

Addleshaw Goddard 2017 .Guidance of Employee Personal Data. URL: https://www.addleshawgoddard.com/globalassets/insights/employment/gdpr-guidance-on-employee-personal-data.pdf. Accessed: 10 February 2018.

Biels 2015. Problems of Manual Data Entry. URL: http://biels.com/the-problems-of-manual-data-entry/. Accessed: 10 February 2018

Billgren, P & Ekman, L. 2017. Compliance Challenges with the General Data Protection Regulation. URL: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8911983&fileOId=8911995. Accessed: 11 October 2017.

Data Protection 2007. What is personal data? URL: https://www.dataprotection.ie/docs/What-is-Personal-Data/210.htm. Accessed: 03 September 2017.

Encyclopedia 2014. Human Resource Management. URL: https://www.inc.com/encyclopedia/human-resource-management.html. Accessed: 03 September 2017.

ERC 2013. What HR needs to keep Confidential? URL: https://www.yourerc.com/blog/post/What-HR-Needs-to-Keep-Confidential.aspx. Accessed: 10 February 2018.

EUR-Lex Europa 1995. Directive 95/46/EC of the European Parliament and of the Council. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Accessed: 16 October 2017.

European Commission 2016. Protection of Personal Data. URL: http://ec.europa.eu/justice/data-protection/. Accessed: 03 September 2017.

Freeman, R. 2016. GDPR and Privacy Impact Assessment. URL: https://www.itgovernance.co.uk/blog/gdpr-and-privacy-impact-assessments-why-are-they-required/. Accessed 13 January 2018.

Global Data Hub 2016. The data protection principles under the General Data Protection Regulation. URL: https://united-kingdom.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html. Accessed: 03 September 2017.

Hill, D. 2010. Data Protection, Governance, Risk management and Compliance. CRC Press. New York.

Investopedia 2016. General Data Protection Regulation. URL: General Data Protection Regulation (GDPR) Definition | Investopedia http://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp#ixzz4sSnQgwQq. Accessed: 01 September 2017.

Jarvanainen, M. 2017. HR´s secret weapon to GDPR Compliance. URL: http://hrnews.co.uk/hrs-secret-weapon-gdpr-compliance/. Accessed: 06 September 2017.

Jay, R. Clarke, J. 2010. Data Protection Compliance in the UK. 2nd edition. IT Governance. London.

Lestrange, G. 2015. Employee Data. URL: https://www.cornerstoneondemand.co.uk/blog/employee-data-handle-care. Accessed: 10 February 2018.

Lingard, S. 2017. HR data and GDPR: what you need to know about consent (and why not to rely on it). URL: https://www.hrzone.com/perform/business/hr-data-and-gdpr-what-you-need-to-know-about-consent-and-why-not-to-rely-on-it. Accessed: 20 October 2017.

Lord, N. 2018. What Is a Data Protection Officer? URL: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance. Accessed: 12 January 2018.

Lynskey, O. 2015. The foundations of EU data protection law. 1st edition. Oxford University Press. London.

Personal Data Act 523/1999.

Pitmans Law 2017. What are the differences between the Data Protection Directive and General Data Protection Regulation? URL: https://www.pitmans.com/insights/publications/what-are-the-differences-between-the-dpa-and-gdpr/. Accessed: 01 September 2017.

Rouse, M. 2008. EU Data Protection Directive. URL: http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC. Accessed: 01 September 2017.

Rouse, M. 2014. Change Management. URL: http://searchcio.techtarget.com/definition/change-management: Accessed: 13 January 2018.

Saunders, M. Lewis, P. & Thornhill, A. 2009. Research Methods for Business Students. 5th edition. Pearson Education Ltd. London.

Saunders, M. Lewis, P. & Thornhill, A. 2012. Research Methods for Business Students. 6th edition. Pearson Education Ltd. London.

Singleton, S. 2003. Data Protection law for employers. 1st edition. Thorogood. London.

Toolshero. 2014. ADKAR model of change. URL: https://www.toolshero.com/change-management/adkar-model/ . Accessed: 03 September 2017.

Two birds 2017. Guide to the General Data Protection Regulation. URL: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en. Accessed: 18 October 2017.

Voigt, P. & Bussche, A. 2017. The EU General Data Protection Regulation (GDPR). Springer. Hamburg.

Winthrop, P. Pittman, S. 2011. Employee Data Privacy. URL: https://www.lexology.com/library/detail.aspx?g=e904c6fd-7c91-4c1d-9c48-6b059552658b. Accessed: 12 November 2017.

Appendices

Appendix 1. Questionnaire

1. Identification and analysis		
	a. Identification of processes and databases that are currently existing in the company for processing personal data by HR function	
		i. List all processes that include personal data (Attach in separate document)
		ii. List all systems that contain personal data, list all parties who can access employee data or process data for(Attach in separate document)
		iii. Identify all interfaces between HR and business where personal data is given or possibly stored outside HR´s databases
		iv. Identify all physical archives containing personal data
		v. Identify all electronic archives containing personal data
	b. Analysis of the data content and which of those are considered relevant for the current organization set-up	
		i. Ensuring the ownership and validity of each identified process containing personal data
		ii. Naming of HR Data Privacy Coordinator per country
		iii. Cleaning of unnecessary archives and systems containing outdated and not relevant personal data
		iv. Anonymization processes for data that will be needed to be shared outside HR for further data processing purposes in business
		v. Discontinuation of unnecessary systems
2. Evaluation and implementation		
	a. Streamlining and validating necessary processes and databases containing personal data of employees	
		i. Create documentation about the processing activities per identified main registers
		ii. Identify the needed HR and business roles who will have access to data per each lifecycle phase
		iii. Ensure a streamlined personal data management lifecycle that will describe the maintenance, anonymization, blocking and deletion phases of personal data (see attached ppt. example)
		iv. Create required descriptions per each sub-register containing personal data per each identified process
	b. Privacy protection by design and by default	
		i. Negotiate and ensure the needed software changes and/or automation steps for the databases (if required)
		ii. Ensure documented roles and process for access management practices
		iii. Ensure the maintenance process and up-to-date register description per database
		iv. Sign an Annex to an agreement with each Service Provider for the

		processing of personal data (attached model contract annex)
		v. Sign an additional data transfer agreement, in case the data is processed outside of EEA (EU + Norway + Switzerland), to be coordinated with Legal
3. Demonstrate compliance and follow-up development		
	a. Communication	
		i. Translations and compliance of 5 main privacy policies of employee data > information shared in Arena and other relevant locations
		ii. Create a detailed communication plan to ensure organization awareness
	b. Trainings	
		i. HR trainings
		ii. Assistant services trainings
		iii. Manager trainings and instructions about what data they are allowed to store (where, how, for how long)
		iv. Discussions and informing the Employee representatives about the Employer's processes of gathering personal data of employees
		v. Employee awareness campaigns to build trust for the handling of personal data
	c. Documentation and instructions on how to act in case of	
		i. suspected data breach (to be notified to authorities within 72 hours)
		ii. a person asks to remove their data or to show what data the company is having of them
		iii. outsourcing processing of personal data
		iv. starting to gather new personal data
	d. Governance model	
		i. Ensure with ongoing practices that the personal data is always up-to-date and in place according to GDPR
		ii. Create internal audit practices to monitor the organization´s compliance to GDPR
		iii. Create a model to follow changes to laws and regulations
		iv. Ensure roles and responsibilities to analyse, evaluate and implement changes whenever neccessary per process

Appendix 2. Thesis activities timeline as a Gantt chart