Sini Lamoureux

Implementing the General Data Protection Regulation

The experiences of three Finnish organizations

Master's thesis in
Governance of Digitalization
Supervisor: Eija Karsten
Faculty of Social Sciences,
Business and Economics
Åbo Akademi
Åbo 2020

ÅBO AKADEMI UNIVERSITY – Faculty of Social Sciences, Business and Economics

Abstract for Master's thesis

Subject: Governance of Digitalization
Writer: Sini Lamoureux
Title: Implementing the General Data Protection Regulation — The experiences of three Finnish organizations
Supervisor: Eija Karsten
Abstract: This study investigates how three Finnish organizations have implemented the EU's General Data Protection Regulation (GDPR). The GDPR was adopted by the European Council in April 2016 and entered into force on May 25th 2018. The research topics of the study are GDPR implementation, guidance and compliance. The study's literature review comprises a review of central concepts of the study, data protection legislation in Europe and in Finland, as well as a review of the GDPR. The focus of the GDPR review lies on data protection measures targeting data collecting and processing organizations. The GDPR itself and literature about the implementation make up the most important sources for the literature review. The multiple-case study research approach is used as the study's research method. The research design consists of three organizations, a Data Protection Officer (DPO) and an employee informed of the GDPR were interviewed. Qualitative interviews were used as a data collection method for the study. All in all, six interviews were made. The findings of the study are presented in case descriptions. The results of the study show that the organizations have taken similar measures for implementing the GDPR. These are for example, the establishment of task forces, DPO's attending courses held by external experts and GDPR guidance for employees. However, organizational actors influence the implementation of the GDPR. The main factors found were the access to time and resources for data protection activities and the organizational structure.
Keywords: GDPR; General Data Protection Regulation; GDPR implementation; Personal data; Data protection; Organization.
Date: 04.10.2020 | Number of pages: 77

TABLE OF CONTENTS

LIST OF FIGURES

TABLE

List of Abbreviations

DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention on Human Rights
EU	European Union
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
GPS	Global Positioning System
WP 29	Article 29 Working Party

1 Introduction

This is a study about the European General Data Protection Regulation (Regulation 2016/679) and how three different Finnish organizations have implemented it. The General Data Protection Regulation (hereinafter referred to as the Regulation and the GDPR) regulates data protection in the European Union (EU). The Regulation was adopted by the European Council in April 2016 and entered into force on May 25th 2018. The Regulation affects how organizations process and manage personal data, as well as increase citizen rights and control over personal data. This study will address the Regulation, the data protection measures it enforces on organizations and the implementation of the Regulation in three Finnish organizations.

In the beginning of 2018, the Regulation was given great attention also by the average citizen. As the enforcement date approached, millions of organizations and companies sent e-mails to customers and clients informing them that their privacy policy had been updated to be compliant with the Regulation. After the Regulation entered into force, it occurred that websites run outside of the EU were temporarily blocked for IP-addresses located in the EU. This occurred because the websites were non-compliant with the Regulation and the website keepers did not want to risk sanctions. Whether conscious of the Regulation or not, becoming affected by the Regulation during the implementation time period was close to inevitable, especially when using digital services.

An interest in the Regulation was sparked because of its magnitude, the demand it puts on organizations and because of it being the most significant change in EU data protection legislation in 20 years. Implementing the Regulation was not something that data collecting organizations could avoid without the possible consequences of sanctions and negative publicity. The threat of sanctions requires a certain vigilance from organizations handling even the smallest sets of personal data. The Regulation makes little difference between organizations, the clearest division between organizations in the Regulation is defined by the number of employees and the

characteristics of the data processing. Also, small and medium-sized organizations need to be aware of the Regulation and, in some cases, even to a great extent.

There is a vast amount of predictive research about the Regulation and research that, from a legal perspective, criticizes the Regulation. Also, a fair amount of research scrutinizing a specific principle of the Regulation and the Regulation's impact on privacy policies has published. There is little research about how organizations have implemented the Regulation it in practice. Therefore, there is a motivation for this study as it will contribute to the research arena of information and data security management in organizations.

The purpose of this study is to explore how three different organizations in Finland have implemented the Regulation through the following research questions:
RQ1) How did organizations prepare for the implementation of the Regulation?
RQ2) What kind of guidance is used for supporting compliance with the Regulation?
RQ3) How is compliance with the Regulation monitored?

The study begins by defining the concepts of personal data, data protection and by reviewing data protection history. The study continues with a general introduction of the Regulation, a summary of the Finnish adoption of the Regulation and a review of the Regulation's key definitions and elements. Then follows an explanation of six important data protection measures for organizations enforced by the Regulation and a review of the infringements and its effects for organizations. The implementation of the Regulation is discussed through the aspects of planning, responsibilities and guidance.

The methodology chapter contains a description of the research approach and the research design as well as the data collection and data analysis. In this chapter the trustworthiness of the study is also discussed. Subsequently, the findings are presented, and the results of the research are discussed. Finally, the study's conclusions are presented followed by a summary of the research.

2 Personal Data and Data Protection

In this chapter two of the most relevant key concepts of this study will be defined and presented. Understanding the characteristics of personal data and data protection is fundamental for interpreting the Regulation and its provisions.

2.1 Personal Data

Personal data has become a valuable commodity both for the private sector and public authorities (Lynskey, 2016). The quantity of personal data being processed continues to increase exponentially. Kitchin (2014) categorizes data according to form, structure, source, producer and type; these characteristics define how the data can be handled and what it can be used for. One of the most common sources of electronically and directly captured personal data is generated through forms used when for example, making an order or partaking in a survey. What differentiates data from personal data is that the latter can be used to identify an individual. In a legal context, personal data is often referred to as any 'personally identifiable information' (Pangrazio & Selwyn, 2019).

Organizations and governments deal with varying amounts of personal data, however almost all kinds of active organizations possess data that may be connected to a person. For a small company, a set of personal data could consist of staff data such as, contact details and bank details. Nevertheless, a small company's staff generated personal data fades in comparison to the sets of data social media companies like Google or Facebook collect about their users and other persons.

Pangrazio and Selwyn (2019) highlight three of the most important types of personal data: actively given data, extracted data and processed data.

2.1.1 Actively Given Data

The first type of personal data is actively given by individuals to devices and systems. Social media and general personal information are good examples of personal data which individuals feed into different systems whenever creating a virtual profile (Pangrazio & Selwyn, 2019). The social media platforms' datasets are multiplied when individuals use already existing social media accounts to identify themselves on other platforms instead of creating new ones. Facebook is known for letting their users log in to other systems using their Facebook account. While it is convenient for the users, Facebook collects detailed information about its users' behavior by linking them to external systems.

Although data is voluntarily generated, the average citizen might not be aware of the scope of personal data collected through different online activities. This became particularly visible in the Cambridge Analytical scandal connected to the 2016 USA presidential elections. During the time of the election campaign, personal data generated through a personality test on Facebook was processed in order to influence voter behavior (Hsu, 2018). It is estimated that the personal data of around 87 million Facebook users was concerned in the scandal (Brown, 2020). In connection to this privacy on social media became a heavily debated topic resulting in the hashtag #deletefacebook trending on Twitter.

Another less extensive example is different kind of platforms used by institutions and companies. For example, the national Finnish Transport and Communications Agency Traficom's contractual partner Ajovarma is a company in charge of theoretical tests and driving examinations for different kinds of driving permits and licenses (A-Katsastus, 2019). It is the only of its kind in Finland which in theory means that anyone who gets a Finnish driver's license must use Ajovarma's platform. Ajovarma is a company owned by A-Katsastus Group which is owned by the venture capital firm MB Rahastot. A-Katsastus Group is the leading company for vehicle inspections, registrations and driver's examinations in Nothern Europe (A-Katsastus, 2019). This

leads to A-Katsastus Group possessing a vast amount of personal data of both Finnish and other European citizens.

2.1.2 Extracted Data

The second type of personal data is extracted by systems or devices without the user having to actively formulate the data (Pangrazio & Selwyn, 2019). GPS and Internet based applications generally extract a vast amount of sensitive data (Lutz & Ranzini, 2017). These data sets may contain information about the user locations, personal preferences, financial details etc.

Getting access to an application usually requires agreeing to the terms and conditions of the application. In general, this implies agreeing to the application accessing different personal data and depending on the application's characteristics granting access to camera, microphone and contact list may also be required. A user agreeing to the terms and conditions of a service or product legally indicates that the data extracted is owned by the service provider (Pangrazio & Selwyn, 2019).

The mobile and geolocation-based dating application Tinder is a good example of a service that is based on extracting user data. For example, Tinder tracks the user's device information such as IP-address and device sensor information for monitoring the mobile phone's orientation and navigation (Tinder, 2018). The application requires user consent to collect precise geolocation, the user's geolocation can be tracked even when Tinder is not running. One of the basic features of Tinder is allowing the user to set the maximum geographical distance of potential matches. Although Tinder's (2018) privacy policy states that granting access to the GPS only occurs with the consent of the user, the application cannot function properly without the GPS.

Another mobile application with similar extraction of personal data is the fitness application Sports Tracker. Sports Tracker is used for tracking the user's physical

performance in connection to workouts. According to the application's privacy policy it also collects biometric and health data which may be recorded with monitoring devices such as fingerprint readers and heart rate sensors paired with the application (Sports Tracking Technologies, 2016).

2.1.3 Processed Data

The third type is processed personal data, the purpose of processing is to add meaning and value to data entities (Pangrazio & Selwyn, 2019). In many cases the person who is the source of the data, will only be given a fraction of the processed data and have little exposure to the actual data processing steps. Instead, full data sets may be sold to third parties that use the data sets for commercial purposes.

It is common that processed personal data is visualized by using dashboards and simplified analytics. The Finnish Kesko Corporation offers its customers with a loyalty card personalized discounts, an insight in their shopping history and analyzes based on the collected data. The customers can, among other things, compare their shopping records with other customers living in their area and track the proportion of domestically produced goods purchased.

The loyalty card customers have the option of limiting the data collected on three levels or completely deny the collection of any data (Markkinointi & Mainonta, 2016). However, Kesko's Chief Digital Officer, Anni Ronkainen stated in an interview that the more the customer chooses to restrict the collection of data, the less the customer will benefit from the reward system (Markkinointi & Mainonta, 2016). The data processing can be interpreted as an additional service for the customers. Yet the companies that control and own the data have the power to influence the consumers' behavior (Kitchin, 2014).

2.2 Data Protection

According to Article 8 of the European Convention on Human Rights (1950) the respect for private life is considered a basic human right making the protection of personal data fall under the same article (Psychogiopoulou, 2017). However, there are many paradoxes connected to personal data and the protection of privacy. The collection, processing and use of personal data is ethically, politically, socially and legally complex and it is difficult to draw a clear line between 'good' and 'bad' personal data (Kitchin, 2014). Especially on social media users seem to willingly give away detailed data about themselves. This in turn complicates the control authorities and governments can have over data protection (Lynskey, 2016).

Data is generated and used for many different purposes; companies, governmental bodies and institutions use data for making businesses more profitable, protecting societies and efficient decision making among other things. At the same time collecting the data needed for the named causes might result in exploitation and misuse of the single individual's privacy. Lynskey (2016, p.1) goes as far as describing modern society as being *"…in the middle of a tug of war for control over personal data."*. Kitchin (2014) describes how data in connection to purely scientific research may be used to manipulate the citizens' conception of reality.

2.2.1 European Data Protection Legislation – a historical overview

Data protection became a legally relevant topic when personal data and information, at a larger scale, started to become subject to manipulation (Bennett, 1992). During the late 60s people started to become more aware of the endangerment of their individual rights and liberties (Bennett, 1992). In the mid 70s, British barrister Paul Sieghart predicted that personal data increasingly will be disseminated through various channels and that data generally will be easier to access (Bennett, 1992). Sieghart also forecasted that fewer people will be aware of what is happening to the data and that the data will be easier to tamper.

The development of policies for data protection became at an early stage subject to international cooperation. The world's first data protection act was approved in the German federal state Hessen in 1974 (Freude & Freude, 2016; Lloyd, 2018). Five years later the rest of Europe followed in Hessen's footsteps and in 1981 the Council of Europe signed the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* also known as Treaty No. 108 (1981), the convention entered into force in 1985. The objective of the Convention is to protect the individual's right to privacy and regulate cross-border flow of personal data.

In 1995, the European Commission adopted the EU Data Protection Directive (DPD) (Directive 95/46/EC) which set a minimum standard for data protection in the EU. All 27 EU member states implemented the directive in domestic legislation resulting in slightly varying legislation across the EU. When the DPD was adopted in 1995, only 1% of the EU population was using the Internet (Lynskey, 2016). According to Eurostat (2020) Internet access in the EU has since then steadily increased at a fast pace. In 2018, Internet access had risen to 89% which is already 29% higher than in 2008[1]. Since 1995, the increased access to Internet and the launch of web-based companies such as Google and Amazon have radically changed the relevance of the DPD which made an update of the EU data protection legislation inevitable. The data protection reform package was introduced by the European Commission in January 2012 and included a Proposal for Data Protection Regulation (Lynskey, 2016).

[1] The UK included.

3 The General Data Protection Regulation

In April 2016, the General Data Protection Regulation (Regulation 2016/679) was passed in the European Parliament. As of the 25th of May 2018, the Regulation became directly binding for all EU member states, also organizations outside the EU handling EU citizens' personal data became affected by the Regulation. In principle, this means that the Regulation can affect any organization in the world. Prior to coming into force, the Regulation was promoted as a framework that would reshape the European data protection and harmonize privacy legislation among EU Member States in a more effective way than the DPD (Voss, 2012). The objective of the Regulation is to make EU residents enjoy a higher level of protection of their rights, privacy and freedoms while businesses enjoy reduced barriers for movement of data in the EU (IT Governance Privacy Team, 2017). For personal data collecting companies, the enforcement of the Regulation was expected to bring more demanding legal requirements and a need for reallocating resources (Freiherr von dem Bussche & Zeiter, 2016). The general presumption was that the Member States with strict domestic data protection legislation would be required to put in less effort for complying with the Regulation than Member States with rather lenient data protection legislation.

The Regulation has received great attention, especially from personal data collecting companies since penalties for non-compliance may result in significant fines and damaged public relations (Hoofnagle, van der Sloot, Zuiderveen Borgesius, 2019). Although the Regulation has been welcomed as a needed update for European data protection legislation it has also been substantially criticized for its vagueness and complexity (Bygrave, 2017; Davies, 2016; Hoofnagle, van der Sloot, & Borgesius, 2019).

In accordance with the standard for EU directives and regulations, the Regulation is divided into two sections, the first section contains recitals and the second articles (IT Governance Privacy Team, 2017). The recitals provide background and context to

the legislation. The 99 articles are divided into 11 chapters, the four latter ones mostly concern the European Commission and supervisory authorities.

3.1 The Adoption of the Regulation in Finland

Before the Regulation became effective Finnish legislation had several Acts devoted to protecting personal data. The Finnish Act on Protection of Privacy in Working Life (759/2004) defines basic freedoms and rights, as well as ensures privacy in professional life. In order to comply with the Regulation, many EU Member States updated existing legislation. In Finland new legislation was passed. The Finnish Data Protection Act (Act 1050/2018) implemented in 2019, complements and defines the domestic adoption of the Regulation. The Finnish Data Protection Act is thus a legislation that must be used in parallel with the Regulation. According to the Finnish Data Protection Act (Act 1050/2018) 3§ Finland based data controllers and processors must follow both the Regulation and the specifications set in the Finnish Data Protection Act. Another result of the implementation of the Regulation in Finland was the repletion of the Finnish Personal Data Act and the Act on the Data Protection Board and Data Protection Ombudsman.

3.2 Key Definitions and Elements of the Regulation

Next, the most relevant concepts for the implementation and compliance of the Regulation for organizations will be explained. The concepts have been selected based on their occurrence and relevance in the literature. The Regulations complete definitions can be found in Article 4 of the Regulation.

3.2.1 Personal Data

Personal data is any kind of information relating to an identifiable natural person, also known as a data subject in the GDPR context. Westerlund (2018, p.53) defines personal data in the light of the GDPR: *"Personal data is characterised as only such data that can be linked to a natural person (i.e. an individual's physical presence)."* The Regulation's definition of personal data comprises a considerably wider scope than the traditional perception of personally identifiable information (Hoofnagle et al, 2019). Within the Regulation, every piece of information that may identify a person can be considered personal data. For example, IP-addresses, fingerprints, card numbers, cookies and location data may, depending on the context, be legally interpreted as personal data (Hoofnagle et al, 2019). Legal persons such as companies are thereby excluded from the Regulation's interpretation of personal data, the same applies for deceased persons (IT Governance Privacy Team, 2017; Regulation 2016/679 Recital 27).

3.2.2 Data Controller

A controller is a natural or legal person, public authority, agency or other body acting as main decision-makers exercising control over the motives and means of processing personal data (Regulation 2016/679). Examples of typical data controllers are public authorities, businesses and NGOs. The controller determines and controls what data to collect, from whom, how long the data will be kept, for what purpose and whether there is a need to notify data subjects about the chain of events. Thereby, controllers often act as the organization data subjects interact with and supply their information to (IT Governance Privacy Team, 2017). Controllers must be able to prove compliance with the Regulation. Their scope of compliance also includes data processors should data processing services be procured. Controllers may be fined and sanctioned for non-compliance.

3.2.3 Data Processor

A processor processes personal data on behalf of the controller. The processor is usually a third-party actor hired by a controller organization to process the controller's data. A processor organization could for example be an accounting firm processing pay slips on behalf of the controller organization (European Commission, n.d.a). Although controllers are more accountable for managing data protection the processor organization might still need to make decisions on how the data is stored, what IT systems and methods to use for collecting the data among other things. Nevertheless, often the controller and the processor are the same organization, it is considered unusual that a controller would not handle any processing at all (IT Governance Privacy Team, 2017).

3.2.4 Supervisory Authority

A supervisory authority is an independent public authority responsible for the enforcement of the Regulation. In accordance with Article 51 of the Regulation each EU member state must have at least one supervisory authority, Member States may appoint several but must in that case designate one public authority to represent the Member State in the European Data Protection Board (EBPD). In addition to monitoring and enforcing compliance, the duties of supervisory authorities include *"promoting public awareness and understand the risks, rules, safeguards and rights in relation to processing."* (Regulation 2016/679 Recital 122). A supervisory authority is thereby required to act as a public preceptor and provide guidance to both data collecting and processing organizations and to data subjects.

The supervisory authority's powers can be divided into the following categories: authorization and advisory, investigative and corrective (IT Governance Privacy Team, 2017). A supervisory authority has the power to order controllers and processors, carry out investigations in the form of data protection audits, review

certification requirements, notify organizations of alleged infringements of the Regulation and require access to all personal data of controllers and processors if needed for the fulfillment of their tasks (Regulation 2016/679 Article 58). A supervisory authority can exercise its corrective powers and issue warnings, reprimands and fines along with ordering controllers and processors to comply with data subject requests. Supervisory authorities are encouraged by the Regulation to develop standards and certification mechanisms facilitating compliance with the Regulation.

In Finland, there is only one body acting as national supervisory authority, it is named the Office of the Data Protection Ombudsman. The office consists of one Head Ombudsman, two Deputy Ombudsmen and around 40 data protection specialists (Office of the Data Protection Ombudsman, n.d.d). The Data Protection Ombudsman is appointed by the Finnish government for a five-year term of office.

3.2.5 Processing of Personal Data

The processing of personal data refers to any set of operations or activities, both manual and automated, involving personal data. These are for example the collection, structuring, storage, alteration, use and dissemination of personal data (IT Governance Privacy Team, 2017). Less apparent examples of data processing include everything from the planning of processing to the elimination of personal data (Office of the Data Protection Ombudsman, n.d.f).

Processing personal data in compliance with the Regulation must be done in accordance with six principles for data protection (IT Governance Privacy Team, 2017; Regulation 2016/679 Article 5). The principles are: Lawfulness, fairness and transparency; Purpose of limitation; Data minimization; Accuracy; Storage limitation; Integrity and confidentiality. The controller is responsible for demonstrating compliance with all six principles. The principles must be respected throughout the entire data processing process (Office of the Data Protection Ombudsman, n.d.a).

Lawfulness, Fairness and Transparency

The data subject must be clearly informed of the data processing taking place and the processing's characteristics. The actual processing must correlate with the description and the processing must be motivated by at least one of the six lawful purposes stated in the Regulation's Article 6. The lawful bases for processing personal data are the following:

a) Consent of the data subject
b) Processing motivated by a contractual term
c) The controller's legal obligation
d) The protection of vital interests of data subject or of natural person
e) Processing carried out motivated by public interest or the exercise of a public authority based on law or legal provisions
f) The legitimate interest of the controller or a third party
    i. For example, data processing for historical or statistical purposes

Each Member State may keep or introduce more detailed provisions if they are legitimate within the Regulation's scope.

Purpose of Limitation

The second principle is closely linked to the first one and specifies processing limitations. The purpose of the data processing must be determined prior to the commencement of processing, failing to do so will result in illegal data processing although the processing purpose would be supported by the Regulation's lawful purposes for processing. Organizations need to specify and record the processing purposes in addition to providing the information to potential data subjects in the form of for example privacy policy documents, consent forms or terms and condition documents (IT Governance Privacy Team, 2017). Thus, organizations must keep track of the content of the privacy policy and make sure that the information is constantly

updated whenever the data collected will be used for other purposes than previously mentioned.

Data Minimization

The purpose of the data minimization principle is to minimize organizations' excess data. Data minimization also implies regularly deleting unnecessary personal data. In order to comply organizations must set up frameworks and processes that facilitate the ability to provide sufficient proof of data minimization. An example illustrating the data minimization principle can be an employer collecting detailed health information from employees dealing with hazardous tasks in case of health threatening accidents. Would the same employer collect the same kind of information from employees with office jobs it would be classified as excessive collection of personal data (Information Commissioner's Office, 2019).

Accuracy

Collected personal data must be correct and accurate. Defect personal data must immediately be corrected or deleted by the data controller. Faulty personal data may have serious consequences especially in the health care sector; thus, this principle's importance vary according to the purpose of the data collection. Data subjects have the right to rectification which implies that data can be corrected and erased upon their request. Therefore, organizations must develop methods and systems enabling data subjects the access to their personal data and if needed correct the possibility to correct or request its deletion. Organizations are recommended to integrate such schemes into regular processes (IT Governance Privacy Team, 2017).

Storage Limitation

Whenever collected personal data is no longer needed it needs to be deleted or go through encryption without further notice. Pseudonymization may be used to detach

the data subject's identity from the data and thereby ensure secure storage for inter alia statistical, scientific and historical purposes. However, it is not a suitable method for organizations that do not have sufficient resources for reversing pseudonymization as it could be a required measure in for example investigations. In connection with implementing the Regulation, many organizations found themselves in situations where they had to destroy significant amounts of personal records because of the storage limitation principle (IT Governance Privacy Team, 2017).

Integrity and Confidentiality

Personal data must be treated with integrity, confidentiality and security. Data collecting organizations must protect data from any kind of corruption and from getting in the wrong hands. Organizations must also have the ability to restore personal data in case of accidents, such as fires or floods.

4 Data Protection Measures for Organizations Enforced by the Regulation

The Regulation enforces several measures supporting adequate personal data protection in organizations. In this chapter, some of the most significant organizational measures enforced by the Regulation will be discussed.

4.1 Data Protection Officer

One of the most significant measures for organizations enforced by the Regulation is the appointment of a Data Protection Officer (DPO) (Regulation 2016/679 Article 37). The appointment of a DPO is mandatory for processors and controllers whenever one of the following statements are fulfilled:

a) Data processing is carried out by a public authority or body (courts are excluded)
b) The organization's core activities include data processing
c) The organization's core activities consist of processing of sensitive data at a large scale

Exactly under what circumstances and context an organization may exempt the DPO criterion remains unclear (Freiherr von dem Bussche & Zeiter, 2016), the definition of core activities may also vary between Member States (IT Governance Privacy Team, 2017). Furthermore, the Regulation lacks a clear definition of 'large scale'. Controller and processor organizations may therefore not have a clear understanding if the appointment of a DPO is required from them. However, an organization has the possibility to voluntarily appoint a DPO, in that case the DPO will act under the same requirements as if the designation had been required by the Regulation (IT Governance Privacy Team, 2017).

A DPO does not have to be a person employed by the organization, the service of a DPO might be purchased from a third-party service provider if there are no conflicts of interest. The Regulation does not prohibit a DPO from fulfilling other responsibilities unrelated to the role of the DPO. However, the Article 29 Data Protection Working Party[2] Guidelines on Data Protection Officers (2017) states that a rule of thumb is to not give the role of a DPO to a person who has a position within the senior management of an organization. For example, a CEO, CFO, Head of IT, Head of Marketing or Head of Human Resources might have responsibilities conflicting with the DPO role. Traditionally, data protection compliance duties have by default been directed to IT superiors. According to the Regulation, however, this is no longer an option.

The DPO tasks, responsibilities and relationships to other entities are outlined in the Regulation's Articles 37-39. The DPO's role is to act as a contact person for data subjects, internally in the organization and for the supervisory authority. The contact details of the DPO must in accordance with Article 37 (7), be published and publicly available for potential requests from data subjects. The DPO must be available for full cooperation with the supervisory authority on a relatively short notice; the DPO has no longer than one month to react to requests from the supervisory authority.

The expertise and skills required by a DPO are provided in the Regulation's Article 37 (5), the DPO *"…shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39".* In the Working Party 29 Guidelines on DPOs, the following duties connected to monitoring compliance are particularly highlighted (Article 29 Data Protection Working Party, 2017 p.17):

- *"collect information to identify processing activities*
- *analyse and check the compliance of processing activities*

[2] The Data Protection Working Party was an advisory board set up under Article 29 of the EU Data Protection Directive 95/46/EC. Members of the Working Party comprised of Member State representatives and was replaced by the European Data Protection Board in connection with the application of the GDPR. https://edpb.europa.eu/our-work-tools/article-29-working-party_en

- *inform, advise and issue recommendations to the controller or the processor"*

The level of expertise of a DPO is not strictly defined as such. Nonetheless, the more extensive and sensitive data processing the organization does, the more important it is to choose a DPO with sufficient expertise (Regulation 2016/679 Recital 97). Besides understanding the basics of data protection, the DPO should also have knowledge of national and European data protection laws and practices (Article 29 Data Protection Working Party, 2017). In addition, the DPO gains from understanding the organization's practices, processes and the sector it operates in. The DPO is encouraged to foster a data protection culture within his or her organization (Article 29 Data Protection Working Party, 2017). Making data protection embedded in the organizational culture will support the implementation of significant GDPR elements, such as data processing principles and record keeping.

The responsibilities of a DPO are stated in the Regulation's Article 38 (1) *"The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."* In accordance with the Regulation, it is the controller and processor organizations' responsibility to ensure that the DPO is facilitated in carrying out his or her tasks. This can be interpreted as the controller having the duty of providing the DPO with necessary training and adequate equipment for fulfilling the tasks. By contrast, the controller and processor are prohibited from giving the DPO any instructions regarding his or her tasks (Regulation 2016/679 Article 38 (3)). Accordingly, the DPO enjoys a degree of autonomy and neutrality enabling him or her to perform his or her tasks without direct influence from others.

Ultimately, the processor or controller organization is responsible for compliance and the demonstration of it. The Regulation's Article 38 (3) determines that the DPO cannot be dismissed or penalized by the processor or controller for correctly performing his or her duties as DPO. In the Regulation, accountability has been integrated as a principle the organization needs to answer for (European Data Protection Supervisor, n.d.d). Should the controller or processor activities be

incompatible with the Regulation and the DPO's advice, the DPO has the right to report his or her separate opinion of the matter to the highest management (Article 29 Data Protection Working Party, 2017). In summary, the Regulation gives the DPO numerous tasks and responsibilities related to personal data protection.

4.2 Data Protection by Design and Default

Bygrave (2017) notes that the provisions of the Regulation's Article 25 about Data Protection by Design and Default result in the most innovative and ambitious norms of the Regulation. Article 25 requires that the controller integrate appropriate technical and organizational measures which purpose are to implement data protection principles into the organization's practices. Pseudonymization is mentioned in the Regulation as an appropriate measure for embedding Data Protection by Design (DPbD), respectively data minimization for Data Protection by Default (DPbDf). Although the concepts relate to each other, DPbD refers to embedded data protection precautions and mechanisms in services and products while DPbDf refers to the application of such precautions as a default setting (Jasmontaite, Kamara, Zanfir-Fortuna, & Leucci, 2018).

The provisions of the article target especially the development of information systems and business models with DPbD principles embedded. DPbD implies designing systems in which privacy requirements have been considered and built-in in all phases of the system development (Hansen, 2016). Since the Regulation only provides one example for how to fulfill DPbD which is pseudonymization, the controller itself is required to assess whether other measures are deemed necessary for compliance. Adding privacy features to a running system subsequently is not considered to be PDbD. Hansen (2016) emphasizes that today's system design does not, as a rule, meet up the demands of PDdD. One of the reasons behind this is that there is an absence of financial incentives for developers to develop such systems. If controllers and processors are sufficiently legal and compliant in their data processing, they can still use systems without built-in data protection (Hansen, 2016).

DPbDf makes the controller responsible for implementing appropriate technical and organizational measures for limiting, for example the quantity of personal data processed by default. This also includes the extent of processing, the time period for storage and accessibility. It is particularly important that the data subject's information, by default, is not made accessible to other parties without the data subject having the possibility to deny access. The European Data Protection Supervisory (2012) states that the aim of the 'by default' principle is to protect data subjects from situations in which they would not understand or control the technological features of the data processing.

When the Regulation was implemented, few established guidelines on DPbD and DPbDf could be used to facilitate the implementation of Article 25. In the end of 2019, the European Data Protection Board published the document Guidelines 4/2019 on Article 25 Data Protection by Design and by Default which contains practical guidance on the adoption of the principles. As a first step the IT Governance Privacy Team (2017) suggest developing an appropriate compliance framework ensuring that data protection is embedded in the organizational behavior.

4.3 Data Processing Records

Controllers and processors must keep a record of processing activities and upon request make it accessible to the supervisory authority. A complete and correct data processing record is vital for organizations' ability to demonstrate compliance and provide necessary evidence. The records must be kept in a shareable format, preferably electronically (Regulation 2016/679 Article 30 (3)).

Organizations with fewer than 250 employees are exempted from retaining an explicit record of their processing related activities (Regulation 2016/679 Article, 30 (5)). However, there are certain data processing conditions that require data processing records regardless of the 250-employee limit. If the organization's data

processing poses a probable risk to the data subject's rights a data processing record is required. The same applies for organizations that process data on a regular basis, meaning that processing is a regular and frequent activity of the organization. Also, organizations processing special categories of personal data or data relating to criminal convictions and offences, are required to maintain a data processing record.

There are differences in the record details required of controllers and processors, controllers must keep more extensive and detailed data processing records. The records of a controller must contain name and contact information about the controller and processor along with purposes of processing, descriptions of categories of data subjects and personal data, information about data being transferred to a third country or international organization and a general description of the technical and organizational security measures. The controller must also keep records of time limits for erasure and categories of different types of data recipients to whom the data is disclosed. The processor's recording obligation is similar to the named requirements but requires fewer details. Supervisory authorities support controllers and processors in fulfilling this measure by providing templates and guidance for correct record keeping (Office of the Data Protection Ombudsman, n.d.b). For example, The Office of the Data Protection Dataombudsman (n.d.h; n.d.i) provides freely accessible record templates for both controllers and processors on their website.

4.4 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is required under Article 35 from controllers whose processing is likely to result in high risks for data subjects' rights and freedoms. A DPIA is an assessment of the impact planned data processing will have on data subjects' privacy protection (European Data Protection Supervisor, 2020). Mitigating the threats caused by the controllers processing to data subjects are especially considered when performing a DPIA and should support controllers in implementing the DPbD principle. Preparing the assessment should take place when

designing a new processing operation or activity and it should be subsequently reviewed and updated. Performing a DPIA should help the controller since it is an opportunity to detect potential security loopholes and problems and fixing them before they pose an actual threat and cause potential sanctions.

The supervisory authority of each Member State oversees publishing and maintenance of lists of processing activities that require the controller to perform a DPIA. Controllers shall reach out to their DPOs for advice and guidance on the DPIA requirements. A DPIA should include a description of the planned processing and its purposes, a necessity and proportionality assessment, risk assessments to data subjects along with measures to handle the risks and demonstrate compliance (European Data Protection Supervisor, 2020).

According to the Office of the Data Protection Ombudsman (n.d.c) and the European Data Protection Supervisor (2020), a controller's processing activities and operations pose a high risk to data subjects when two of the following characteristics of the processing apply:

a) Systematic and extensive evaluation or profiling
    i. Can occur in connection to marketing profiling for targeted advertising online.

b) Automated decision making
    i. Can occur when a person applies for a quicky loan and no human interaction is needed from the loan giver to approve the loan.

c) Systematic monitoring of data subjects
    i. Monitoring of a publicly accessible area on a larger scale, for example constant video surveillance of a public area.

d) Sensitive data processing
    i. Processing of genetic and biometric data occurs for example, when a mobile phone is unlocked with a fingerprint or facial recognition.

e) Processing on a large scale
    i. Processing of special category personal data revealing health information, ethnicity, political opinions, religious beliefs or sexual orientation.

f) Matching or combining datasets with different purposes
    i. Matching can occur with the purpose of analyzing data subject behavior.

g) Vulnerable data subjects
    i. Vulnerable data subjects entail data subjects that are perceived weak beside the controller, examples are children, data subjects in need of protection and employees.

h) New technologies
    i. Especially applies when a new technology impacts the data processing significantly.

i) Processing that prevents people from exercising their rights or entering a service or contract
    i. Especially applies to processing with the purpose of determining whether the data subject is allowed or denied to use a service.

4.5 Data Breach Notification and Documentation

A personal data breach could be caused by anything from cyber attacks to malware infections. Also, stolen USB-sticks or a fire in a data center are also possible scenarios resulting in data breaches. The consequences of a personal data breach can be devastating, in worst cases they result may result in identity theft, fraud or loss of confidentiality. In case of a personal data breach the controller must notify the

supervisory authority within 72 hours starting from the discovery of the breach (Regulation 2016/679 Article 33). If the 72-hour limit is not met the controller must provide the supervisory with an explanation. Due to the strict time limit, precautionary notifications may be necessary to file (Freiherr von dem Bussche, Axel & Zeiter, 2016). In case of a personal data breach with a high risk of posing a threat to natural persons' rights and freedoms the controller shall, without delay, inform the data subjects about the occurred breach (Regulation 2016/679 Article 34).

When informing the supervisory authority and the data subjects about the breach, the controller must provide exhaustive details about the nature of the data breach, communicate the name and contact details of the DPO, describe the probable consequences of the breach and inform both of the taken and planned preventative measures the controller has and will take to minimize the damages (Article 33). The processor could also be the entity to inform the supervisory authority if so has been agreed, however the primary responsibility remains with the controller (Office of the Data Protection Ombudsman, n.d.e).

For a controller to in an efficient manner comply with the data breach provisions, it is crucial to have appropriate and established data documentation processes. Documentation of the data breach and the management of it is mandatory under the Regulation's Article 33 (5), this also ensures that the supervisory authority can control the compliance of the Regulation under such circumstances. The role of the DPO in a breach situation is to act as a mediator between the controller and the supervisory authority (IT Governance Privacy Team, 2017).

4.6 Data Subject Rights

In comparison to the controller the data subject is weak and can be compared to a customer and business relationship (Wolters, 2018). Nevertheless, data subjects have seven rights that can be exercised defined in Chapter III of the Regulation. These are the right to be informed; of access; to rectification; to erasure; to restrict processing;

to data portability; to object to processing and rights in relation to automated decision making and profiling.

The rights give the data subjects the right to make requests to organizations collecting and processing their data. First and foremost, data subjects have the right to be informed about the data collected about them and how the data is processed. Data subjects also have the right to access and request rectification and erasure of their data (Regulation 2016/679 Articles 13, 15-17). These requests and demands can at any time be exercised making it crucial for organizations to have processes and resources enabling to fulfill the duties they have towards data subjects.

Although data subjects' request might be resource intensive, especially if there is no suitable architecture in the systems in use, controllers can generally not require any financial compensation for performing the request (Regulation 2016/679 Article 12 (5). The data subject requests may be done in any format and through channels that have not been assigned as official for data subject requests. Therefore, it is crucial that staff potentially receiving the requests are sufficiently trained to identify them (IT Governance Privacy Team, 2017). The IT Governance Privacy Team (2017) recommends remodeling existing data access portals to enable data subjects' access to their data, thus facilitating the communication between controller and data subject.

In accordance with the Regulation's Article 12 the controller must react to the requests as soon as possible or within a month from receiving the request. If that time limit is not possible to meet due to the complexity of the request the time limit may be extended to two months. In such a situation the controller is obliged to within a one-month time limit inform the data subject about the motivation behind the delay.

4.7 Infringements and its effects

One of the most significant incentives for complying with the Regulation are the sanctions regulated by the Regulation's Article 83. Prior to the Regulation coming into force the maximum fines for non-compliance in the DPD only reached a couple of thousand euros at the most, also the sanctions were inconsequentially applied throughout the Directive's lifetime which lead to a weakened incentive for compliance (Hoofnagle et al., 2019). According to Privacy Affairs' (2020) fines tracker, 347 fines had been issued in the EU by the end of July 2020, two years and two months after the Regulation came into effect. The total amount of these fines combined was nearly 176 million EUR (PrivacyAffairs.com, 2020). Of those the largest fine of 50 million EUR was issued to Google France for being untransparent about the personal data gathered (Commission Nationale de l'Informatique et des Libertés, 2020). The most frequently issued fine has been due to insufficient legal basis for data processing (CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB, 2020).

Although the Regulation has received a lot of media attention caused by the generous fines, imposing fines is generally not necessarily the first step a supervisory authority takes when an infringement is detected. As visualized in Figure 1 the supervisory authority shall issue a warning when intended processing operations are likely to cause infringements, a reprimand shall be issued when operations have infringed provisions of the Regulation (Article 58). There are two tiers of fines which are applied according to the magnitude and the aforethought of the infringement. The factors considered when determining the seriousness of the infringement are among other things, the preventative and mitigative actions, previous infringements, cooperability with the supervisory authority, adherence to approved codes of conduct or approved certification mechanisms as well as aggravating or mitigating factors applicable to the circumstances (Article 83 (2a-k). The smaller fine can subject to up to 10 000 000 EUR

or up to 2% of the annual turnover while the bigger fine can be subject to up to 20 000 000 EUR respectively 4% of the annual turnover (Article 83 (4,5)).

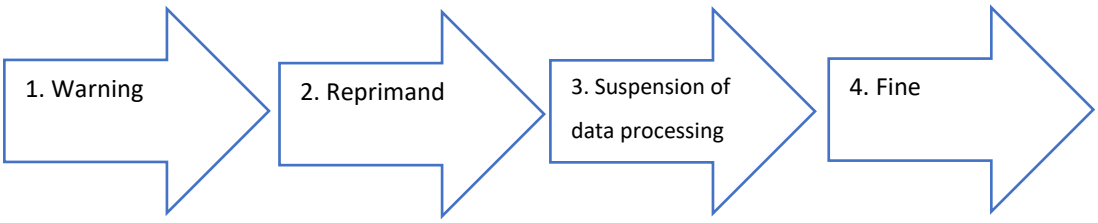

Figure 1 The corrective powers of the supervisory authority. Source: Article 58 and European Commission, 2020.

4.7.1 Specifications in Finnish Legislation

Article 83 (7) allows each Member State to decide whether and to what extent public authorities and bodies may be subject to fines. The Finnish Data Protection Act (1050/2018) Section 24 specifies this for Finnish organizations.

An administrative fine cannot be imposed on central government authorities, state enterprises, municipal authorities, autonomous institutions governed by public law, agencies operating under Parliament or the Office of the President of the Republic, or the Evangelical Lutheran Church of Finland and the Orthodox Church of Finland or their parishes, parish unions and other bodies.

In many Member States geographically close to Finland such as Sweden and Denmark, public authorities can be financially sanctioned. Despite a lack of financial fines, public authorities in Finland may still be subject to other corrective measures issued by the Office of the Data Protection Ombudsman. Furthermore, Section 24 of the Data Protection Act specifies that fines cannot be imposed if more than ten years have passed since the infringements. A fine becomes statute-barred after five years from the date it was imposed. This means that a fine is no longer legally enforceable and can no longer be subject to legal actions.

4.7.2 Infringements in Finnish Organizations

Since the Regulation came into force, the Office of the Data Protection Ombudsman has received multiple data breach notifications from Finnish organizations and complaints from private persons about Finnish organizations not respecting the provisions. Many of these complaints concern phished personal data and websites not allowing the user in a simple and transparent manner, decline the collection of cookies (Fagerström, 2020; Office of the Data Protection Ombudsman, 2019). By June 2020, the Office of the Data Protection Ombudsman had imposed four administrative fines on four Finnish organizations in May 2020. At the time of writing none of the decisions are final, the fines can be appealed in the Finnish national administrative court.

The largest fine of 100 000 EUR was imposed on the leading Finnish postal service operator Posti Oy for deficiencies in the information provided to customers making change-of-address notifications (Office of the Data Protection Ombudsman, 2020b). The customers who made a change-of-address notification, started receiving communications and direct marketing from companies. The Office of the Data Protection Ombudsman's investigation disclosed that Posti had failed in informing the customers about their rights and providing the customers with the option to decline disclosure of their personal data to third-party companies. Only during 2019, 161 000 customers had become victims of Posti's infringements although Posti already in 2017 had promised the Dataombudsman to correct the issue.

The second largest fine of 72 000 EUR was imposed on Taksi Helsinki, a taxi company that had seriously neglected the assessment of risks and consequences of processing personal data prior to installing audio and video recorders in their taxi cars (Office of the Data Protection Ombudsman, 2020a). Taksi Helsinki could not motivate the need for audio recording nor did they inform their customers about the monitoring of them. Furthermore, Taksi Helsinki failed to be transparent about the automated data

processing and profiling connected to their loyalty program as well as failed to conduct proper documentation.

A fine of 16 000 EUR was imposed on a company failing to do a data protection impact assessment although they process employee location data which calls for an impact assessment under Article 35 of the Regulation. The collected location data was used for monitoring employees' working hours. The characteristics of the personal data and its processing resulted in a high probability of risks for the employees' rights and freedoms. The smallest fine imposed to date violated the principle of data minimization by collecting unnecessary personal data from individuals applying for jobs. The fined company asked for information about the applicants' religion, family status and health details among other things. The company was fined 12 500 EUR.

5 Implementation of the Regulation

Implementing the Regulation requires organizations to act both technically and practically. Organizations that prioritized data protection prior to the Regulation have a clear advantage compared to organizations that previously have neglected privacy or kept privacy matters to a minimum. For example, organizations that prior to the Regulation's enforcement were accredited with the ISO/IEC standard 27001 for information security management will already have a lot of data protection processes documented (IT Governance Privacy Team, 2017).

A survey on the awareness of the Regulation (Dimensional Research, 2016) concluded that 93% of the respondents did not have a plan to prepare for the Regulation, furthermore 82% of the respondents were concerned about Regulation compliance. The respondents consisted of data privacy professionals working for small and medium sized businesses and larger enterprises affected by the Regulation. Although organizations had a two-year period to prepare themselves, in 2018 the market research company Forrester (n.d.) predicted that 80% of businesses affected by the Regulation would not be compliant at the time of the Regulation coming into effect. Of those non-compliant, 50% were predicted to aim for compliance but fail, the other 50% were predicted to deliberately not comply.

5.1 Planning the Implementation

Tikkinen-Piri, Rohunen and Markkula (2018) suggest that the first thing organizations need to do is become familiar with the Regulation and identify how they stand under the Regulation's definitions and the measures required from them. Organizations must identify and analyze all processes and activities that in any way are linked to personal data and assess how the Regulation will affect them. Teixeira, da Silva and Pereira, (2019) identified Lopes' and Oliviera's (2018) roadmap as the most complete in comparison with other implementation roadmaps. In their roadmap the first step

is to gather and map all the personal data controlled and processed by the organization. The second step is to analyze the data in order to identify inadequacies and carry out a DPIA if necessary. The last step is to implement necessary measures and security mechanisms. In order to maintain compliance, the organization must regularly perform audits and reviews.

Implementing the required measures might be challenging and organizations might require tailor-made solutions since the Regulation lacks specific prescriptive instructions (Teixeira et al., 2019). Although there are many implementation guidelines provided by the European Commission (n.d.b) among others, putting the Regulation into practice is ultimately up to the organizations themselves. Especially organizations operating with little documentation might experience the Regulation as heavy to implemented (Tikkinen-Piri et al., 2018).

5.2 Responsibilities

It is crucial to decide who or whom in the organization, except for the DPO, that will be responsible for overseeing and implementing the changes along with organizing potential GDPR courses. In accordance with the Regulation's Article 28, controllers are only allowed to work with processors that can prove sufficient compliance of the Regulation. This puts pressure on controller organizations since they have the responsibility of making sure that the potential data processing organizations are compliant.

5.3 Guidance

Supervisory authorities, various consultancies and NGO's have organized GDPR courses and put together guidance documents facilitating organizations' compliance with the Regulation. Many actors also offer freely available implementation

checklists and simple compliance tests that organizations can use to get a basic notion of the compliance status. Also, the European Commission and the EDPB have published numerous guidelines, factsheets, infographics, online videos, webpages and even podcasts guiding organizations in the implementation and compliance of the Regulation. Examples of these can be found in EDPB's collection of factsheets and on their YouTube channel and podcast page (EDPS, n.d.a; n.d.b; n.d.c).

Although there are many actors that provide guidance, supervisory authorities are bound by the Regulation to provide guidance in accordance with Article 57. Supervisory authorities are thus recommended as the primary source for guidance (IT Governance Privacy Team, 2017). Many supervisory authorities provide vast guidance on their websites both for organizations and data subjects along with telephone hotlines and possibilities to regular e-mail and mail correspondence. Examples can be found on the Office of the Data Protection Ombudsman's (n.d.g) website and on the Information Commissioner's Office (n.d.) website.

6 Methodology

In this chapter the methodology of the study will be presented. The objective of the research methodology is to create a research framework allowing to exploratively and qualitatively analyze the research context. First the type of research and the research design will be presented, then follows a presentation of the data collection and analysis methods. The chapter ends with a review of the trustworthiness of the study.

6.1 Multiple-Case Study Research

Case studies are a common form of organizational research (Jones, 2014). Conducting case studies as a research method are widespread within social sciences and are preferred when the questions 'how' or 'why' need to be answered and in contexts where the researcher has little control over happenings (Yin, 1994). He describes a case study as "*an empirical study that investigates a contemporary phenomenon within its real-life context*" (p.13). A case study can be either exploratory, descriptive or explanatory, in many cases the research purposes overlap.

A multiple-case study is one containing more than one case. Some scholars make a distinction between the methodology and describe multiple-case studies as comparative studies (Yin, 1994). He, however, includes both variants of case studies in the same methodological framework. Multiple-case studies are perceived as more robust than single case studies because of the results generally are more convincing and comprehensive. In a multiple-case study each case must be carefully selected and serve a specific purpose. In general, multiple-case studies use replication rather than sampling with the cases selected based on criticality, topicality or feasibility (Jones, 2014). The assumption is that the result of a multiple-case study will either lead to similar results or lead to contrasting results.

6.1.1 Research Design

The research design of this study, presented in Figure 2, demonstrates the framework for the research context and data collection of the study. The aim of the research design is to explore how the research context has been applied in three different cases. To explore the research context in the cases, two entities of analysis in each case organization are investigated. The study was replicated with the approach of literal replication on all three cases meaning that each case was treated identically in terms of methodology.

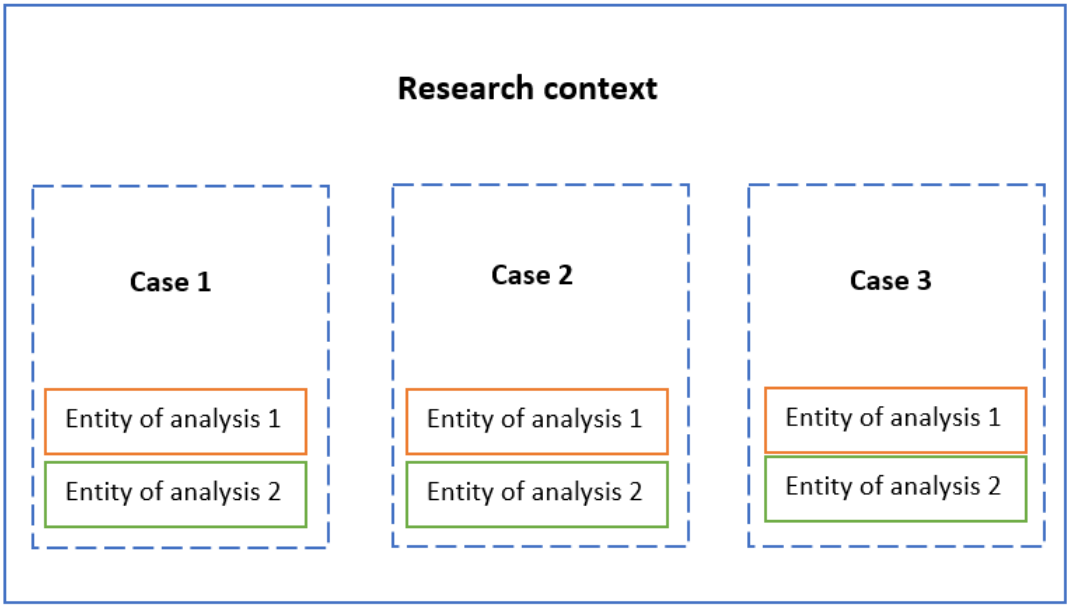

Figure 2 Research design of the study, adapted from Yin (2007, p.60).

6.1.2 The RACI-Matrix

For organizing GDPR responsibilities internally, the IT Governance Privacy Team (2017) suggest using a RACI matrix to divide tasks derived from the Regulation. Therefore, the RACI-matrix was used for determining the entities of analysis in the

research design. In the following section the RACI-matrix will be examined as a framework for supporting the adoption of the Regulation in organizations.

Given the prerequisites the Regulation poses on controller organizations, it might be helpful to use a set framework for clarifying tasks, processes and division of responsibilities. An option is to use a responsibility assignment chart which may support cross-departmental coordination and increase the added value of the data protection actions within the organization (Kane & Koppel, 2013). The Responsibility, Accountability, Consult and Inform (RACI) matrix is an organizational matrix for identifying tasks along with the organizational units and their relationships with the tasks. The RACI-matrix has for example been suggested as a tool for implementing the ISO/IEC standard 27001 for information security management standard and for GDPR implementation in EU institutions (Calder, 2016). This suggests that the RACI-matrix may also be suitable for GDPR implementation in other kinds of organizations.

The first step of creating a RACI-matrix is to identify the areas of responsibility and the respective tasks, the second step is to identify the organizational units and posts that will be involved (Kane & Koppel, 2013). For each task, the organizational units and posts will be assigned a letter representing the role the unit or post will have (see Table 1).

The roles of the RACI-matrix are the following (Kane & Koppel, 2013):

- **R**esponsible
    - The unit or person who works to complete the task.
- **A**ccountable
    - The unit or person who delegates and approves decisions and actions before the deliverable is deemed complete.
- **C**onsult
    - At least one unit or person is consulted and reviews the decisions and actions. Consulted parties are often people who provide input based on their expertise.
- **I**nform

- An informed unit or person needs to be informed about the big picture of the progress.

Each task should have at least one unit or person responsible and accountable. The consult and inform roles are not always required for every task. Thus, the RACI matrix is an efficient way to strategically clarify the resources needed for successful project implementation in addition to detecting loopholes and gaps in the roles and responsibilities.

In this study the entity of analysis 1 equals a person who is responsible for the Regulation, the entity of analysis 2 equals a person who is informed of the Regulation. In this case, it means that all interviewees categorized as responsible hold the position of a DPO in the respective organizations. The criterion of being informed of the Regulation only implies that the interviewee has a work description that requires some knowledge of the Regulation. The purpose of interviewing members of organizations classified as responsible and informed of the Regulation was to get a wide overview of the implementation of the Regulation.

The choice of interviewing responsible and informed employees allowed an investigation of the research context both from a top-down and bottom-up perspective. Interviewing employees responsible for the Regulation, gave a picture of how the implementation was planned and managed. Interviewing employees informed of the Regulation, gave an indication of how the implementation process had been received by regular employees in their daily work. In order to investigate the implementation more thoroughly and from other perspectives, employees accountable for and consulted about the Regulation could have been interviewed. However, it was not done due to time and resource constraints.

Table 1 Example of RACI matrix for GDPR implementation project. Adapted from Vertex42 RACI Matrix Template (n.d.)

RACI Matrix

GDPR implementation

Roles and Responsibilities

Responsible, Accountable, Consulted, Informed

	ROLES	DPO	Steering Board	CEO	CIO	Project Manager	Technical Lead	Task force	IT-support	Consultant	External expert	Associated company	ICT-group	IT steering group
	Deliverable or Task	**Status**	**CIO/Leadership**				**Project Team**				**Other Resources**			
	Priority 1													
	Data minimization actions		A			R	I		R	I	C		I		
	Processing systems and processes		A			R	I			I	C	C	I		
	Priority 2													
	Data subject requests		A	I			A	R	I	I	C			I	I
	System architecture		A	I			A		R	R	C	C		I	I
	Priority 3													
	Reporting		R	I		I	A	I	R		C				
	Documentation		C				A	I	R		C				I
	Priority 4													
	Accreditation		R	I	C	A	I	R			C	C			
	Compliance		R	I	A	C	I	C	I	I	C				I

6.2 Data Collection

The data collection of the study was made through making six qualitative interviews. This section contains information about qualitative interviews as a data collection along with a review of the data collection process.

6.2.1 Qualitative interviews

Interviews are one of the most common methods used in qualitative research (Bryman & Bell, 2011). Interviews are used for collecting information and individual's stories and understandings of a phenomenon. The purpose of qualitative interviewing is making use of the direct meeting and conversation that occurs between researcher and interviewee in a specific context (Widerberg, 2002).

Semi-structured interviews are characterized by the researcher having a checklist of themes or query fields with appurtenant follow-up questions (Jones, 2014; Lantz, 2007). The types of questions can generate both open and closed answers. In a semi-structured interview, the researcher will get an understanding of the questions' meaningfulness to the respondent. However, in replicated multiple-case study the level of the answers' openness may cause difficulties in performing a qualitative analysis of the phenomena (Lantz, 2007).

Jones (2014) discusses the advantages and disadvantages of using interviews for data collection in organizational research. The advantages of interviews are that they are relatively low-cost, enable the covering of a large sample and may result in the researcher gaining access to the organization site. On the other hand, the researcher may intentionally or unintentionally provoke the data and the interviewee's perceptions might have inaccuracies especially if they are reflecting on past events. Also, there is the issue of reflexivity, the interviewee might give the sort of answers he or she expects the researcher wants to hear (Yin, 1994). Furthermore, Widerberg (2002) states that there are no guarantees for the researcher and interviewee to have matching personal chemistry which may influence on the outcome of the interview.

6.2.2 The Data Collection Process

Based on the study's research questions an interview guide was made (see Appendices 1 & 2). All the interviews followed the same interview guide, the first two questions were basic questions about the interviewee's position and his or her brief description of the organization he or she works in. These questions had two purposes of which the first one was to gain valuable background knowledge about the interviewee and his or her perception of the organization he or she is operative in. Acquiring data about the perception is valuable because it provides a deeper understanding of the organization and the interviewee's perspective of it. The second purpose was to allow both the researcher and interviewee to acclimatize to the interview situation thus creating a sense of mutual trust. Lantz (2007) states that

there is a lack of meaning in commencing an interview without the researcher and interviewee having a common understanding of the purpose of their meeting.

The interview questions were based on the study's research questions which were operationalized and grouped according to the research themes implementation, guidance and compliance. Separate interview guides were made for responsible and informed interviewees as their relationships to the research context differs significantly. The interview guides were made in English and later translated to Swedish.

This study's research design requires three different cases to be to be studied through two entities of analysis. Since the objective of the study was to research how three different organizations have implemented the Regulation, different potential case organizations' DPOs were contacted by e-mail in January 2020. All organizations that were contacted are operative in Finland. In the e-mail brief information about the study, its aims and the characteristics of the potential interview were described. All the potential interviewees who agreed to be interviewed received the interview questions beforehand. The reason for doing so was because of several failed attempts to get individuals to agree to be interviewed. This indicated that the nature of the research topic generated some insecurities and comments such as "We do not know or have anything to do with this". Although all interviewees received the interview questions beforehand almost all of them admitted that they had, nevertheless, not reviewed them properly prior to the interview. One reason for that could be that simply having access to the questions beforehand, made the interviewees more comfortable with the thought of being interviewed.

The DPOs were contacted first as the research design's criteria was to interview a DPO in each case organization, a position that cannot be substituted by any other function. In two of the cases, the DPOs were asked to provide a recommendation of a person from the same organization informed of the Regulation and willing to be interviewed. In the third case organization the DPO and a person considered

informed of the Regulation were contacted simultaneously but separately due to recommendations from a contact operative in the organization.

The data collection itself occurred during a six-week period starting in February 2020 and ending in March 2020. The data collection was made through semi-structured interviews, lasting from 30 to 45 minutes. Out of six interviews four were made face to face and two by using Skype video calls. The interviews made face to face were recorded using a dictation machine while the video calls were recorded through Skype. The interviewees were aware of the recording and were all given the opportunity to deny the recording of the interview. All interviews were made in Swedish except one which was made in English due to the interviewees limited language skills in Swedish.

6.3 Data Analysis

Analyzing quantitative data is not straight forward, according to Bryman and Bell (2011) only broad guidelines can be provided on the topic. Lantz (2007) explains that the prominent subjectivity and context-boundness in qualitative studies results in a lack of clear descriptions for how successful qualitative data analysis can be replicated. In many case studies the studies are commenced without knowing exactly how the data will be analyzed, which also was the situation for this study.

Analyzing case study data can, just as quantitative data in general, be difficult because there are no well-defined strategies or technicalities for how the evidence should be analyzed (Yin, 2007). He advocates using the strategy of relying on theoretical propositions. The objectives and research design that formed and led to the study should be used as a baseline for coding the data collected and influencing the analysis. Another option for analyzing data is the development of case descriptions. The case description strategy is especially useful when no hypotheses have been set as a basis for the study.

Reducing collected data is often the first step of the analysis and can be done in several ways (Lantz, 2007; Widerberg, 2002). In order to make the data manageable for analysis it is crucial to sort the data. One way of sorting interviews is to make matrix summaries (Kylén, 2004). For this study, the first step of the analysis was to create spreadsheet matrices for documenting the interview data in writing. Two matrices were made, one for the interviews with the DPO's and another for the informed interviewees as their interview protocols differed slightly. The matrices contained cells for each question and answer along with cells for summaries of the answers to each question. The analysis itself began by relistening to the interviews in their entirety in order to get a general overview of the interview. Comments and general remarks for each interview were documented in the matrices. The second step of the analysis was to listen to the recordings one answer at a time, the answers were noted in the matrices in summarized formats. Since this study is not based on a hypothesis or general assumption the results will be presented in case descriptions which will help to identify the causal links of the study. The case descriptions are not of cross-sectional character because of the significantly different characteristics and starting positions of the case organizations.

6.4 Trustworthiness of the study

The concepts of validity and reliability cannot be applied to qualitative research in the same way as to quantitative research (Shenton, 2004). In line with previous statements about qualitative methodology, there are no established rules for the assessment of quality in case study design (Bryman & Bell, 2011). It all depends on the researcher's judgement of appropriate evaluation methods. Bryman and Bell (2011) advocate that case study analysis should be focused on the uniqueness of the cases and their complexities. Theoretical generalizability, however, is possible to achieve, especially in a multiple-case study.

Bryman and Bell (2011) suggest analyzing the quality of qualitative studies through credibility, transferability, dependability and confirmability. Credibility which equals

internal validity is one of the most important factors for ensuring trustworthiness (Bryman & Bell, 2011). The data collection was completed in accordance with good academic practice, all the interviewees participated voluntarily and were not compensated for their participation. The interviewees were well informed about the purpose of the interviews and how the recorded material was used. No measures such as triangulation or member checks were performed in this study.

Lantz (2007) emphasizes the importance of an adequate description of the research methodology for supporting evaluation and potential transferability of the study. The transferability of context bound case studies is however limited due to the research context's time sensitivity. Replicating this study with similar types of case organizations would not necessarily prove the same results as the time from the critical date in this research context is getting is elapsing by every day. First, interviewees might not be able to recall events in detail and second, operative individuals in organizations are likely to change positions and organizations over time.

The changing nature of the study's research context challenges the demonstration of dependability (Shenton, 2004). Shenton (2004) advocates thorough description of the research design and how it has been applied as a way of enabling future researchers to repeat the study although the same results are not likely to be achieved. Also thoroughly describing the data collection and giving a reflective appraisal of the study supports the demonstration of dependability. In this chapter both the research design and data collection has been described.

Confirmability can be translated to the researcher acting in good faith and not letting his or her subjectivity and personal values influence the results of the study (Bryman & Bell, 2011). One way of proving confirmability is to apply reflexivity which translates to the researcher reflecting on his or her methods, analysis, interpretation of the results and awareness of potential personal idiosyncrasies affect the study. Nevertheless, no substantial measures were taken for proving confirmability.

7 Findings

In this chapter the findings of the study will be presented. The chapter is made up of case descriptions of each case organization and is concluded by a summary of the findings.

All case organizations are located in Finland, in different cities and municipalities. The organizations are remarkably different from each other especially when it comes to functions, size and turnover which is reflected in the findings. Because of the sensitivity of the study the organizations and the interviewees are not named.

7.1 Case Organization: Public Authority

The public authority case organization has around 1800 employees divided into four different departments. The public authority has a lot of different kinds of duties and activities that require the collection and processing of personal data, many of these duties are prescribed by law. As Finnish public authorities are not subject to being fined by the supervisory authority this organization cannot be financially sanctioned.

The public authority's DPO and an informed employee were interviewed for the study. The DPO was not working for the public authority in question when the Regulation was implemented. However, the DPO has experience of data protection work and the Regulation from a previous employment and has detailed information about the data protection measures taken before the current employment started. The DPO does not work full-time with data protection.

The informed employee (herein after referred to as the informed) works with marketing and communication which implies a lot of online communication and website maintenance. The informed did not work in the organization on May 25th 2018, when the Regulation was enforced but had been an employee of the organization prior to the enforcement.

7.1.1 Implementation

The DPO

The first step of the implementation of the Regulation was the establishment of a data protection working group. The initial assignment of the working group was to prioritize measures, assess the organization's training needs emerged by the Regulation's provisions and consequently organize the staff GDPR courses. The second step was to make an inventory of the personal data collected and processed by the organization.

The working group initially included the DPO, a lawyer, an information officer, IT experts and staff representing different departments, all and all the task force included around 12 members. The task force was chaired by an executive senior employee. Today the working group does not exist in its former constellation, it has been downsized to four members: the organization's DPO, Head of IT, a lawyer and a data protection expert in charge of a department dealing with especially sensitive personal data. The working group meets once a month and works hands on with data protection issues. It reports to the organization management.

The challenges faced with the implementation in the organization were mainly related to staff training and information overload. The staff needed to learn many new things about data protection and there was generally a lot of emphasis put on the enforcement date, May 25th 2018 and the impact it would have. The DPO recalled: "*Media almost pointed out the enforcement day as a doomsday*". The huge attention of the enforcement date lead to a slight sense of panic.

The DPO stated that many were confused about the data subject's consent but since the organization is a public authority with legal obligations to perform certain data collecting tasks consent is not required. The confusion led to the staff getting uncertain about what they were allowed to do and not, within the scope of the

Regulation. This led to staff becoming anxious of data protection, the data protection anxiousness is still notable but is something that is worked on in the organization. The GDPR courses were useful for explaining what the Regulation really is about. The first course was organized as an online course but there were also trainings held by external experts. Based on the online training, which was mandatory for all members of staff, the average employee has spent around one hour on GDPR familiarization. The online course consisted of background information, smaller tasks and quizzes.

The DPO states that there was still a lot to be done at the time of the enforcement date. Nevertheless, there was a stable starting point and a plan for what to do, compliance with previous legislation contributed to already having privacy policy documents in order. A little under a year from the enforcement date there are established models and processes in use for the data protection work of the organization. The DPO's comment about the implementation process: "*Now* [just under a year since the enforcement] *I feel like we have gotten to a point where we can draw a line*".

The informed

The informed encountered the Regulation for the first time in connection to the launching of a new website. The new website needed a privacy policy document written in accordance with the Regulation so the informed contacted the DPO to get help with the composition of the document. Through different networks with employees in similar positions in other organizations, the Regulation has been the topic of many discussions and many peers wonder how they will handle it in their work. All and all the informed has spent a couple of days on familiarization with the Regulation. The informed participated in a one-day training in 2019, in addition to that the informed has independently retrieved GDPR information online.

In the daily work of the informed the major challenges are related to visual personal data. For the informed, it is hard to know how to be compliant especially when it comes to handling photos containing faces and other types of personal data. The

informed exemplified: *"How can we categorize thousands of photos so that we can be aware of exactly which rights apply to which photos…This causes many challenges to which we have difficulties finding solutions to".* Other encounters with the Regulation are related to marketing campaigns and competitions that extract personal data from contact forms.

7.1.2 Guidance

The DPO

To get more information and knowledge of the Regulation the DPO attended a consultancy company's GDPR courses. The DPO also took part in the Data Protection Ombudsman Office's training events and participated in a project supporting digital security in public authorities. Guidance material was in the beginning of the implementation process found by self-initiated retrieval but as the data protection work progressed it became easy for the DPO to know where to look for specific information. The Data Protection Ombudsman Office's website has proved to be a helpful source for data protection issues.

The staff of the organization are offered data protection guidance on the organization's intranet. However, it is challenging for the DPO to know if everyone in the staff is aware of the information on the intranet. New employees receive data protection information in connection with the employment.

The informed

The informed has received GDPR guidance from the data protection working group, the DPO and the organization lawyer. Especially the lawyer has been important when there has been a need for specific guidance. The guidance has not been systematic, and in general that is one of the organization's main challenges according to the

informed. When a new person is recruited that person will need to find the information on his or her own.

The informed is of the opinion that the Regulation is an important thing for an organization and that it could have been more emphasized in the organization but that it is the case for many things. The informed recalls that there was some kind of GDPR course, but that she might not have taken part in it because of being too busy and overworked at the time.

7.1.3 Compliance

The DPO

In order to ensure compliance with the Regulation the organization has a data protection plan and a data protection closure which are yearly updated and reported to the management and the executive committee. The data protection closure, which is examined by controllers, contains statistics about the quota of employees finishing the data protection online course, for example. Furthermore, ensuring that privacy policy documents are continuously updated supports the organization's compliance.

The organization has started to use an introductory assessment scheme when starting to use new systems and processes. The assessment contains short questions on whether the system will handle personal data and its level of sensitivity. Based on the results of the introductory assessment the making of a DPIA may be in order. With the support of the DPIAs the DPO can keep track of the systems handling sensitive data and have an action plan should the data be compromised.

The DPO stated that the organization's executive committee has the highest level of accountability towards the Regulation. The biggest challenge in terms of monitoring compliance is related to a lack of time as the DPO is not working full time with data protection responsibilities. With the time available for data protection tasks, it is not possible for the DPO to perform check-ups with the organization's supervisors.

Keeping the data protection information up to date is also challenging with the continuously changing data protection practices. The DPO emphasized the uncertainty of knowing if complete compliance has been achieved: *"You only know if things have been done the right way once something really does happen or goes wrong, and it is only a question of when it happens, not if."*

The informed

For ensuring compliance with the Regulation the informed has no specific systems but she is aware that the organization must be able to demonstrate that the personal data registers are compliant, and that personal data can be extracted. Despite this, the informed revealed that it is not possible based on how the registers are constructed and that it is a big issue that needs to be corrected. Many systems should be constructed so that it would be possible to achieve compliance.

The informed states that the ultimately accountable person of the Regulation's compliance is the director of the organization. However, she points out that the manager of the DPO has public liability. The informed feels like there is a lot of responsibility put on the single employee:

How can we build systems that enables the employee to do the right thing without him or her being that knowledgeable about the issue? Sensitive information is such an important thing and people are very alert about the GDPR - they will tell you if something went wrong.

7.2 Case Organization: Political Organization

The political organization has around 25 employees and over 24 000 members. The organization has three offices in different parts of Finland and over 100 local departments situated in the country. The organization is rather decentralized with

many of their grassroot activities taking place in the local departments. The low number of employees does not require the organization to have a DPO but due to the nature of their activities and the collection and processing of sensitive data the organization decided to establish the post of a DPO.

The DPO who was elected by the organization's board, does not work with data protection issues full-time. In the organization the DPO has an advisory and surveilling role, the organization's secretary takes care of the administrative work related to the personal data. The informed employee (hereinafter referred to as the informed) works with supporting the activities of local departments and facilitating the work of organization members in various boards.

7.2.1 Implementation

The DPO

Prior to the implementation of the Regulation an investigation was made to assess the need of changes brought by the provisions. At that stage it was noted that the organization already complied with the most part of the provisions due to compliance with previous domestic data protection legislation. The local departments were especially informed of the effects since they oversee local data collection and processing. In connection with the enforcement, the members of the organization were informed about the effects the Regulation would have.

The main challenges faced in connection with the implementation were in line with previous challenges the organization had faced. Questions regarding the ownership of the personal data arose since the local departments deal with members' personal data. All this made it difficult to separate the roles. More emphasis was put on the data subjects' rights especially when collecting personal data through online forms. Now data subjects are asked to answer a few more questions regarding consent for how the organization is allowed to use their data.

The amount of time the staff has put on familiarizing themselves with the Regulation varies according to the role and level the employee has. The DPO estimates that the average employee has devoted around ten hours to get familiar with the Regulation. The employees more actively in charge of registers containing personal data have put in more time, around 20-30 hours each. Also, people volunteering for the organization have taken part of the organizations' GDPR information. However, the DPO noted that the work with data protection in the organization is continuous and is not limited to the enforcement of the Regulation.

At the time of the enforcement the DPO states that the organization was quite well prepared although if felt like the enforcement date turned up quickly and there was a lot of information about what it would imply. The huge amount of information was by some perceived as too much which lead to people in general becoming slightly uneasy with the Regulation. The DPO stated: *"People were afraid of the GDPR, it was perceived as a dangerous acronym"*. In the end many necessary measures had already been taken prior to the enforcement and only a few things needed to be adjusted to comply with the Regulation. That included improving the tracking of how and when personal data is collected and processed. The appointing of a DPO ensured that the organization's data protection knowledge was up to date and it was easy to elaborate on how to handle the challenges.

The informed

To the informed the Regulation was first introduced during staff meetings and through an extensive information package received by e-mail. The information package contained information about the Regulation and how it would affect their activities. There were also information sessions held by the DPO during staff meetings in which the staff could ask questions about the Regulation. The informed pointed out that the DPO provided information especially relevant for their activities. The informed spent around six to eight hours familiarizing herself with the Regulation, over time the time spent has increased.

At the time of the enforcement the informed was well prepared and felt like she had received all the relevant information. For the informed there were no bigger changes in her daily work since the organization had been compliant on many levels already before the enforcement. In general, the Regulation might have received more attention than what it finally needed.

The informed did not face any specific challenges with the Regulation in her daily work. The most important reminder is not to collect personal data that is not needed. The third-party systems the organization uses are compliant with the Regulation limiting the need for self-monitoring. It has become known that some of the local departments use registers of their own making it challenging to control how the local departments handle the personal data. Since the local departments act as independent associations the administration can only inform about the Regulation but not control their activities.

7.2.2 Guidance

The DPO

The most important sources of guidance were the Regulation itself and the Finnish Data Protection Act. Some employees took part in an information seminar about the Regulation organized by an outside alliance. The organization has not used any external consultants, but they have received help from lawyers within the organization with the legal interpretation of the Regulation. The employees of the organization are aware of the terms and conditions of services and products they purchase. This allows them to provide correct data protection information about their services to the members of the organization.

The employees have received guidance in the form of information packages which were also sent to the local departments. The Regulation has also received attention during some of the organization's events and in publications disseminated to all the members. Because of the appointment of the DPO, employees have had the

opportunity to individually ask for data protection guidance whenever needed; some members of the staff exercised this opportunity.

The informed

The information package about the Regulation and the low threshold for contacting the DPO contribute to the informed feeling like she has received all the guidance needed. The informed states that the DPO is very accessible and that all the information is customized to their needs.

7.2.3 Compliance

The DPO

In order to have the capability to demonstrate compliance with the Regulation, the organization tracks and documents how the register containing personal data is used. The register has automatic logging enabling a higher level of data security although many employees and members can access the register. The biggest challenge with monitoring compliance is tied to the decentralized nature of the organization; local departments can only access personal data connected to their departments while administrative staff can access the register in its entirety. The DPO of the organization is responsible for compliance with the Regulation although the board has ultimate accountability.

The informed

The informed does not follow any specific procedures for ensuring compliance with the Regulation as all the systems she uses are compliant by default. According to the informed, the board is ultimately accountable for the organization's compliance with the Regulation.

7.3 Case Organization: Global Company

The global company with around 13 000 employees operates in nearly 200 countries of which many are situated in the EU. The interviewees representing the company in this study are based in Finland. The nature of the company's activities, products and services result in the collection and processing of a great amount of sensitive personal data both within the EU and abroad. Given the size of the company and its activities the appointment of an EU based DPO was highly required by the Regulation.

In the organizational scheme the EU based DPO is under the company DPO who reports directly to the board of the company. The DPO's work closely with the Chief Information Security Officer, the Legal and IT compliance departments. Beside ensuring compliance with the Regulation, the EU DPO's (hereinafter referred to as the DPO) tasks include ensuring that the operations and business practices adhere to other applicable data protection laws, monitoring compliance with the Regulation, with other EU member states' data protection provisions and with the data protection policies of controllers and processors. The DPO works with data protection issues on full time. The informed employee (hereinafter referred to as the informed) works as an IT expert with quality and salary systems, as well as with some local software.

7.3.1 Implementation

The DPO

At a corporate level, a project organization including legal experts, risk management officers, IT experts, the HR and corporate compliance departments was put together from October 2017 to July 2018. The purpose of the project organization was to prepare the company for the enforcement of the Regulation. This was done through putting together policies for employees, customers and partners, inventories of processing activities, courses as well as updating the intranet with relevant

information. The employees were informed through several e-mails about the Regulation and its implications. In addition, an online GDPR course was made for the employees, over 90% of the employees completed the course.

The challenges faced with the implementation of the Regulation were mainly related to training and the distance between high level policies and practices in daily activities. The DPO commented that privacy is not a new thing for the company, the size and potential financial damage of the Regulation's sanctions however make the stakes for compliance a lot higher. Also, the development of risk-based management practices in respect of data protection and privacy proved to be challenging. Furthermore, qualifying suppliers as compliant required tight cooperation between the Legal, IT and Compliance departments which proved to be complex and time-consuming at times.

The DPO states that the average employee needed about 15 minutes to get familiar with the Regulation but that they all and all spent around one and a half hour with the online course. However, the DPO emphasises that the familiarization with the Regulation is continuous. At the time of the enforcement the DPO stated that the company was rather well prepared for the Regulation's provisions. The DPO affirmed that she company is used to complying with many strict regulations on a global scale thus having a stable foundation for adapting to changes such as the Regulation: *"We just need to develop our practices rather than creating a whole new set of processes."*

The informed

The informed first encountered the Regulation on television but because the informed works with salary systems he rapidly received information about changes in the system that were caused by the Regulation's provisions. This happened about a year to six months before the enforcement of the Regulation.

The informed attended a GDPR-course organized by the company and recalls spending around one working day on familiarizing himself with the Regulation along

with shorter moments here and there, whenever needed. The informed stated that he did not feel a need to be especially prepared for the enforcement of the Regulation. He explained that the systems he uses are purchased from other parties and should therefore be compliant by default. The Regulation is nothing that he actively thinks of. He described the Regulation as one in the crowd of many legal frameworks he has come across during his career. He also stated that there will always be new policies.

In the daily work of the informed the Regulation has not caused any specific challenges. However, he points out that it happens that peers forget about the Regulation. Especially when new systems are ordered the provisions may require adjustments that cause extra work.

7.3.2 Guidance

The DPO

To get more information about the Regulation the DPO has used the Regulation itself, and other material such as different kinds of documents and templates for risk and gap analysis as well as for making an impact assessment. The material was mainly found online and, in some cases, provided by external experts. In addition to that the management of the company wanted the DPO to attend a course for becoming a certified GDPR practitioner. The course lasted for five days and was held by an accredited training organization.

Beside the information on the company's intranet and the online course the employees are may be offered direct guidance on data protection issues through contacting the DPO. Two different mailboxes were created, one for reaching the DPO and another for more general data protection issues. The employees also receive data protection guidance by reading the company's Standards of Business Conduct under the sections data privacy and confidential property information.

The informed

The informed states that the main source of guidance was the online course provided by the company that he took. According to the informed the course contained multiple tests making it necessary to properly go through the information provided in the course.

The informed is quite satisfied with the guidance provided and thinks he almost has received enough information, however he stated that there are always situations that come up that could have required more guidance in order to be solved. If the informed needs more guidance he turns to the DPO of the company.

7.3.3 Compliance

The DPO

Compliance is monitored through several measures and procedures. The company's data privacy and security policies support the compliance of the Regulation both for internal and external personal data. There are, for example, Employee Privacy Notice and Employment Applicant policy documents that describe what the company will do with the personal data and for what purpose it is collected. On the IT privacy and security side there are policy documents for data classification, encryption, cyber and corporate security.

In terms of monitoring compliance, the biggest challenges are aligning one global, corporate privacy policy and approach with applicable privacy laws that may differ: *"Not only may they differ on a country level but even on a regional basis like the case is with the German States."* The DPO constantly follows the International Association of Privacy Professionals (IAPP) website for news about data protection compliance praxis and precedents. The DPO states that the (EU based) DPO is ultimately accountable for compliance in the company.

The informed

The informed has not needed to apply any formal procedures to his work in order to comply with the Regulation. He states that the DPO is ultimately accountable for compliance with the Regulation in the company.

7.4 Summary of findings

The findings of the study show that the implementation of the Regulation in the case organizations varies while there are similar features that can be identified between the case organizations. Because the prerequisite for the study's case organizations was the appointment of a DPO, it is one of the most natural and clearest similarity between the organizations. The public authority and the global company had both established a working group respectively a project organization with specialists from different domains in order to prepare the organizations for the Regulation's provisions and the implementation itself. The political organization, being much smaller, did not form a task force or similar for the implementation of the Regulation.

The challenges faced, in connection with the implementation, were of slightly different character for all case organizations. It can be explained with the organizations' starting positions and previous needs for data protection measures. The global company, for example, has a very different need for data protection processes than the political organization since they collect and process data at very different rates and for different reasons. The DPOs of the public authority and the political organization both mentioned that people at the time of the enforcement had been distressed about the Regulation and what they thought it could bring. Especially in the public authority the great amount of information that had to be given to the employees and the general perception of the Regulation was perceived as a challenge for the implementation. The informed interviewee stated that the

handling of visual personal data is especially challenging in her work. In the political organization the organizational scheme and structure made it challenging to set straight the ownership of the personal data.

At the time of the enforcement of the Regulation the DPOs of the political organization and the global company stated that the employees were rather well prepared. The DPO of the public authority was not in office at the time of enforcement but stated that measures had been taken in order to prepare the employees. The informed interviewees of the political organization and the global company both ascertain that they trust that the systems they use are compliant thus minimizing the need for preparedness.

The DPOs of the public authority and the global company both attended a GDPR training course provided by external experts. The DPO of the global company took part in the most extensive training among the interviewed DPOs while the DPO of the political organization did not mention attending any course or training.

All case organizations provided their employees with guidance on the Regulation, both the public authority and the global company took use of their intranets to create online courses and provide information to the employees. The political organization's employees put significantly more time on familiarizing themselves with the Regulation than in the other case organizations. All case organization DPO's emphasized that guidance is something that is constantly ongoing.

The case organizations' processes for handling compliance vary. The public authority puts emphasis on their annual data protection closure and the internal revision of it along with having testing procedures for new systems. The political organization focuses on keeping their register containing personal data compliant by tracking the logging activities. The global company on the other hand, steers and monitors the compliance through numerous policies regulating how the company deals with privacy, data protection and data security. Because of the different approaches to

handling compliance and the general differences between the case organizations they have different challenges with monitoring compliance.

Both the global company's DPO and informed interviewee stated that the DPO is ultimately accountable for compliance. The public authority's and the political organization's interviewees stated that the organizations' boards are ultimately accountable for compliance with the Regulation.

8 Discussion

The aim of the discussion chapter is to answer the research questions based on the findings and discuss the outcome of the study. This chapter is commenced by a review of the answers found to the research questions and factors influencing the implementation of the Regulation.

8.1 RQ1) How did organizations prepare for the implementation of the Regulation?

A study done in 2018 predicted that 80% of businesses affected by the Regulation would not be compliant by the enforcement date, May 25th 2018 (Dimensional Research, 2016). The political organization's DPO and the global company's DPO stated that their organizations were quite well prepared for the Regulation. Preparedness in this context is however something that is hard to quantify and defining what being sufficiently prepared is something that must be legally tried in order to have relevance. Also, the consequences for not being prepared at the time of enforcement were hard to predict since the new Regulation lacked previous precedents with similar scope and sanctions.

It is suggested that organizations begin their implementing process by learning about the Regulation and the effects it will have on them (Tikkinen-Piri et al., 2018). GDPR courses organized by external experts is something all case organizations have taken advantage of. The DPOs of the public authority and the global company personally both took part in such courses. The case organizations' employees mainly received information about the implementation through the organizations' internal channels.

According to IT Governance Privacy Team (2017) implementing the Regulation requires both technical and practical measures. The proposed implementation roadmap for organizations by Lopes and Oliviera (2018) includes mapping the already

existing personal data, analysis of the data and implementation of necessary measures and mechanisms. The public authority DPO described an implementation process very similar to Lopes and Oliviera's (2018). Public authorities often want to demonstrate compliance with laws and regulations in order to maintain good relationships with the citizens. Following a clear plan for implementation may have supported the public authority in demonstrating compliance both to the citizens and the supervisory authority.

Furthermore, organizations with prior experience of data protection processes have an advantage compared to organizations with no previous experience. For example, being accredited with the ISO/IEC standard 27001 for information security management has been identified as an adequate ground for implementation. None of the case organizations are at the time of writing accredited with ISO/IEC 27001 although the global company follows its guidelines. The global company DPO's statement very much confirms this; because their activities already before the Regulation were impacted by laws and regulations on a global scale, they are more agile and used to adapting.

Out of all informed interviewees, the IT expert working in the global company had the most relaxed approach to the implementation of the Regulation. The IT expert described the Regulation as just another legal framework that did not require much action from him. The informed interviewee's long career as an IT expert may influence his attitude towards the implementation of laws and regulations impacting his work.

In connection to the implementation of the Regulation, the informed interviewee working in the public authority raised the issue of photos and visual personal information. For photos to be compliant and publishable, a person in a photo must agree to be photographed and give his or her consent for publishing the photo. As a result, photos that lack the required information may no longer be usable for the organization. One alternative for keeping them compliant, would be anonymization of the persons in photos, which in turn would change the visual outlook.

8.2 RQ2) What kind of guidance is used for supporting compliance with the Regulation?

The Regulation makes each EU Member States' supervisory authority responsible for providing guidance both to organizations and data subjects, in this study only the public authority DPO mentioned the supervisory authority as a source of guidance. Based on the data collected for this study, it is not possible to draw any general conclusions for why the other DPOs did not mention the supervisory authority.

The DPO's role as an information source both for data subjects, internally in the organization and for the supervisory authority is emphasized in the Regulation and in the literature. For the DPOs to have the ability to fulfill this responsibility they need to receive training themselves; the Regulation itself and courses held by external experts were mentioned by all DPOs of the study as sources for guidance. The DPOs' cooperation with lawyers also came up as a vital part of supporting compliance especially at the implementation stage. This demonstrates that the Regulation's demanded the case organizations to allocate resources for training the DPO who in turn has the responsibility to provide guidance to the employees.

The guidance to the employees was an important part of preparing for the implementation. The public authority and the global company used their intranets for creating a platform for the employees, a probable reason for the political organization not gathering the material online in a similar fashion is because they do not have an intranet. Also, the sizes of the case organizations play a significant role in the need of gathering material online. The political organization is rather small compared to the other ones and it the threshold for personally contacting the DPO might be smaller. The informed interviewee in the political organization was content with receiving tailor-made information about the Regulation suggesting that despite not attending an internal course, there was sufficient guidance.

The informed interviewee in the public authority stated that she because of being overloaded with work did not manage to complete the course at the time of it being launched. This demonstrates that although there is guidance available it is not self-evident that employees find the time to take advantage of it, the DPO of the public authority was also concerned about the issue of not being sure if the guidance has reached all the employees. The concerns of the DPO were legitimate. For example, there is a contradiction between how the DPO, and the informed interviewee described the guidance new employees receive about data protection. According to the DPO, a newly employed person receives data protection information in connection with the employment. In contrast, the informed interviewee stated that a newly employed person needs to find data protection information on his or her own. It is possible that an explanation for this can be found in the organizational structure and management. In an organization with many functions, departments and managers, the recognition and prioritization of data protection guidance to employees will vary. Hence, not all employees will receive data protection guidance as expected by the DPO.

8.3 RQ3) How is compliance of the Regulation monitored?

Non-compliance with the Regulation might result in significant fines for organizations. Therefore, the ability to demonstrate compliance is important for organizations wanting to prove their conformity with the Regulation. Supervisory authorities have the right to request documentation that proves compliance from data collectors and processors. As previously mentioned in this study, public authorities are by Finnish law exempted from fines. Nevertheless, infringements are something that public authorities want to avoid to not lose the trust of citizens and other cooperation partners. In addition, they might be subject to other sanctions such as warnings, reprimands or suspension of personal data processing.

Each case organization monitors compliance through processes that match their overall activities and ways of working, another aspect which influences is the amount of personal data the organizations collect and process. The public authority applies annual reporting and evaluation of new systems while the global company relies on several internal policies for monitoring compliance. The political organization emphasizes documentation and tracking of how their personal data register is handled. Looking from a bottom-up perspective it became clear that at least two of the informed interviewees trust that the systems they use are compliant and thus their need for monitoring compliance is minimized. This especially applies when the systems are bought from externals.

Scrutinizing the accountability of the DPO is important because of the special position the Regulation puts the DPO in. The DPO is obliged to report the organization he or she is working for in case of infringements without that being a ground for organizational reprimands although the reporting could cause large fines and negative publicity for the organization. According to the European Data Protection Supervisory (n.d.f) the organization employing the DPO is ultimately accountable for compliance as they need to make sure they hire a DPO with sufficient knowledge of the Regulation, alternatively training the DPO for the task. This interpretation would thus make the DPO responsible but not accountable. In this study both the interviewees from the public authority and the political organization stated that the organization board was accountable. The interviewees of the global company, on the other hand, mentioned that the DPO was accountable. The DPO's special role as a data protection intermediary makes it complicated to clearly define the areas of responsibility.

8.4 Factors Influencing the Implementation of the Regulation

The organizational factors influencing the findings deserve to be discussed as they largely impact the results of this study. These factors are cannot be classified as

unexpected findings but the extent to which they influence the organizations' adoption of the Regulation is significant.

8.4.1 Time and Resources

Especially in the public authority it became clear that a lack of time impacted compliance monitoring and ability to take part of guidance. The lack of time affected the DPO's possibility to make sure that the employees had gotten enough information and it also led to the informed interviewee not having the resources to take part of the information at the time of the enforcement. No general conclusions can be made based on these findings but it is possible that the DPOs' limited time allocated for data protection issues could derive from the public authority's financial situation; the DPO is primarily employed for another role and handles data protection issues on top of the other tasks. Depending on the other tasks' urgency and prioritization it could potentially lead to data protection issues coming in second hand regardless of the DPO's own preferences.

In a contrast to the public authority DPO, the global company DPO works full-time with data protection issues and took part in the most extensive training compared to the other case organization DPOs. What is also clear is that the global company has more at stake in terms of personal data compared to the other case organizations. This makes them more likely to encounter substantial fines in case of non-compliance. Therefore, the global company cannot easily compromise on the resources allocated for data protection.

8.4.2 Organizational Structure

A decentralized organizational structure makes it challenging for the management to control the data protection measures taken on lower levels of the structure. The decentralization of the political organization resulted in challenges working out the

ownership of the personal data. Similar issues could occur for instance in companies with several affiliates and subsidiaries. The legal form of the company, the organizational structure and the number of employees it could impact the appointment of a DPO or even DPOs along with defining the roles of collector and processor. The global company solved this by having two DPOs, one for the company as a whole and one responsible for the EU situated in an EU member state as is required by the Regulation.

9 Conclusions

In this chapter the study is concluded. The chapter begins with a general conclusion, it continues with a reflection on the limitations and contributions of the study. The chapter is finalized with suggestions for further research.

The Regulation has been implemented in organizations through various measures depending on the Regulation's provisions, the case organizations' starting positions and needs. The implementation depends on factors such as the time and resources devoted to the implementation as well as organizational structures. There are however elements of the implementation that can be identified in more than one of the case organizations. These are the establishment of a working group, trainings and information about the Regulation for employees as well as DPO's taking part in training organized by external experts.

9.1 Reflections and Limitations of the Study

The main limitation of this study is the number of interviews, with only six interviews the amount of data collected is small. Also, the small number of case organizations in this study makes it difficult to draw any general conclusions making the findings of this study representative for only the participating organizations. It is however possible that the findings could come up in a similar kind of study that would not research the implementation of the Regulation but the adoption of another legal framework of the same magnitude and significance or another type of organizational change. Also, the organizational cultures of the case organizations heavily influence the findings. When an organizational culture values conformity with laws it is more likely that the people working in the organization will make a higher effort with compliance regardless of the law or regulation.

Because the data collection took place around one year after the enforcement of the Regulation, important details might have been forgotten when the interviewees reflected on the events. On the other hand, the interviewees could give review of the events without being caught up in them at the same time.

There is a lot of criticism towards the Regulation, legal loopholes and grey areas heavily influence how organizations choose to implement the Regulation. Although some of them were mentioned, the study did not focus on them as the purpose was not to examine the Regulation through its flaws. Although data subjects and their rights are the very core of the Regulation the focus of this study has not been on the data subject perspective of the implementation.

9.2 Research Contribution

This study has contributed with descriptions of how three organizations in Finland have implemented the Regulation; how they prepared for the implementation, the kind of guidance they used and how they deal with compliance. The study provides an understanding of how organizations act when an external legal change with significant consequences for non-compliance is enforced.

9.3 Suggestions for Further Research

Based on the findings and limitations of this study further research could be done on how organizations align themselves with data protection and their data protection agility. It could be fruitful to test employees' knowledge of data security and the threat it could potentially cause organizations in attempts of data breaches or similar situations. Another suggestion for further research is the services and systems sold to organizations meant to make their activities compliant with the Regulation and their actual performance.

REFERENCES

A-Katsastus. (2019). Ajovarma oy. Retrieved from https://www.ajovarma.fi/information-about-ajovarma-oy 17.07.2020

Act on Data Protection 1050/2018. Ministry of Justice, Finland. Available at https://www.finlex.fi/en/laki/kaannokset/2018/en20181050

Act on the Protection of Privacy in Working Life 759/2004 englanti. Ministry of Economic Affairs and Employment, Finland. Available at https://www.finlex.fi/fi/laki/kaannokset/2004/en20040759?search%5Btype%5D=pika&search%5Bpika%5D=759%2F2004

Article 29 Data Protection Working Party. (2017). Guidelines on data protection officers ('DPOs'). Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 26.07.2020

Bennett, C. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. ITHACA; LONDON: Cornell University Press. Retrieved from http://www.jstor.org/stable/10.7591/j.ctv2n7hxs 22.08.2020

Brown, A. J. (2020). "Should I stay or should I leave?": Exploring (dis)continued Facebook use after the Cambridge Analytica scandal. *Social Media + Society, 6*(1), p. 205630512091388. doi:10.1177/2056305120913884

Bryman, A., & Bell, E. (2011). *Business research methods* (3rd ed ed.). Oxford: Oxford University Press.

Bygrave, L. A. (2017). Data protection by design and by default : Deciphering the EU's legislative requirements. *Oslo Law Review, 4*(2), pp. 105-120. doi:10.18261/issn.2387-3299-2017-02-03 ER

Calder, A. (2016). *Nine steps to success : An ISO27001:2013 implementation overview*. Ely: IT Governance Ltd. Retrieved from http://ebookcentral.proquest.com/lib/abo-ebooks/detail.action?docID=4519667

CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB. (2020). Statistics: Fines imposed over time. Retrieved from https://www.enforcementtracker.com/?insights 08.08.2020

Commission Nationale de l'Informatique et des Libertés. (2020). Le conseil d'État valide la sanction prononcée à l'encontre de la société google LLC. Retrieved from https://www.cnil.fr/fr/le-conseil-detat-valide-la-sanction-prononcee-lencontre-de-la-societe-google-llc 08.08.2020

Dimensional Research. (2016). GDPR: Perceptions and Readiness - A Global Survey of Data Privacy Professionals at companies with European Customers. Retrieved at https://www.eurocloud.fr/wp-content/uploads/2016/10/gdpr.pdf 27.09.2020

Directive 95/46/EC. The protection of individuals with regard to the processing of personal data and on the free movement of such data. European Parliament, Council of the European Union. Available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:html

European Commission. (n.d.a). What is a data controller or a data processor?. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en 27.09.2020

European Commission. (n.d.b). Rules for business and organisations. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en 27.09.2020

European Convention on Human Rights. European Court of Human Rights, Council of Europe. (1950). Available at https://www.echr.coe.int/documents/convention_eng.pdf

European Data Protection Board. (2019). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Retrieved from https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en 23.08.2020

European Data Protection Supervisor. (2012). Opinion of the European Data Protection supervisor on the data protection reform package. Retrieved from https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf 28.07.2020

European Data Protection Supervisor. (2020). Data protection impact assessment – infographics. Retrieved from https://edps.europa.eu/data-protection/our-work/publications/factsheets/data-protection-impact-assessment-infographics_en 30.07.2020

European Data Protection Supervisor. (n.d.a). Home [YouTube Channel]. Retrieved from https://www.youtube.com/user/EDPS2011 27.09.2020

European Data Protection Supervisor. (n.d.b). Podcasts [Audio Podcast]. Retrieved from https://edps.europa.eu/data-protection/our-work/our-work-by-type/podcasts_en 27.09.2020

European Data Protection Supervisor. (n.d.c). Factsheets. Retrieved from https://edps.europa.eu/data-protection/our-work/our-work-by-type/factsheets_en 27.09.2020

European Data Protection Supervisor. (n.d.d). Accountability. Retrieved from https://edps.europa.eu/data-protection/our-work/subjects/accountability_en 28.08.2020

Eurostat. (2020). Digital economy and society statistics - households and individuals. Retrieved from https://ec.europa.eu/eurostat/statistics-

explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access 21.07.2020

Fagerström, N. (2020). Finländsk webbplats som inte gav användarna rätt att säga nej till cookies gjorde fel, enligt färskt beslut – det kan få stor betydelse för många sajter. Retrieved from https://svenska.yle.fi/artikel/2020/05/15/finlandsk-webbplats-som-inte-gav-anvandarna-ratt-att-saga-nej-till-cookies-gjorde 09.08.2020

Forrester. (n.d.). Predictions 2018 - A year of reckoning. Retrieved from https://go.forrester.com/wp-content/uploads/Forrester-2018-Predictions.pdf 27.09.2020

Freiherr von dem Bussche & Zeiter, A. (2016). Practitioner's corner · implementing the EU general data protection regulation: A business perspective. *European Data Protection Law Review, 2*(4), pp. 576-581. doi:10.21552/EDPL/2016/4/16

Freude, A. & Freude, T. (2016). Echoes of history: Understanding German data protection. Retrieved from http://bfna.insomnation.com/research/echos-of-history-understanding-german-data-protection/ 26.07.2020

Hansen, M. (2016). (2016). Data protection by design and by default à la European General Data Protection Regulation. Paper presented at the *IFIP International Summer School on Privacy and Identity Management,* pp. 27-38.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European union general Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), pp. 65-98.

Hsu, T. (2018, March 21,). For many Facebook users, a 'Last straw' that led them to quit. *New York Times* Retrieved from https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html 22.07.2020

Information Commissioner's Office. (2019). Principle (c): Data minimisation. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ 22.07.2020

Information Commissioner's Office. (n.d.). Home. Retrieved from https://ico.org.uk/ 27.09.2020

IT Governance Privacy Team. (2017). *EU general data protection regulation (GDPR): An implementation and compliance guide*. Ely: IT Governance Ltd. Retrieved from http://ebookcentral.proquest.com.ezproxy.vasa.abo.fi/lib/abo-ebooks/detail.action?docID=5056760

Jasmontaite, L., Kamara, I., Zanfir Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, 4(2), pp. 168-189. https://doi.org/10.21552/edpl/2018/2/7

Jones, M. (2014). *Researching organizations: The practice of organizational fieldwork*. Los Angeles, California: SAGE.

Kane, G., & Koppel, L. (2013). *Information protection playbook*. Burlington: Elsevier Science.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*. London: doi:10.4135/9781473909472

Lloyd, I. (2018). From ugly duckling to swan. The rise of data protection and its limits. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(4), pp. 779-783. doi:10.1016/j.clsr.2018.05.007

Lutz, C., & Ranzini, G. (2017). Where dating meets data: Investigating social and institutional privacy concerns on tinder. *Social Media + Society, 3*(1), p. 2056305117697735. doi:10.1177/2056305117697735

Lynskey, O. (2016). *The foundations of EU data protection law*. Oxford: Oxford University Press. Retrieved from http://ebookcentral.proquest.com/lib/abo-ebooks/detail.action?docID=4310752

Markkinointi & Mainonta. (2016). Kanta-asiakasjärjestelmät "mitä enemmän asiakas rajoittaa, sitä vähemmän palveluja ja etuja tarjotaan". *Markkinointi & Mainonta* Retrieved from https://www.marmai.fi/uutiset/mita-enemman-asiakas-rajoittaa-sita-vahemman-palveluja-ja-etuja-tarjotaan/d122c963-1df8-32d8-9582-7bc0e1068f57 22.07.2020

Office of the Data Protection Ombudsman. (2019). Antalet ärenden som anmälts till dataskyddsombudsmannen fortsätter att öka. Retrieved from https://tietosuoja.fi/-/tietosuojavaltuutetulle-ilmoitettujen-asioiden-maara-edelleen-kasvussa?languageId=sv_SE 09.08.2020

Office of the Data Protection Ombudsman. (2020a). Påföljdskollegiet vid dataombudsmannens byrå påförde administrativ påföljdsavgift för flera brister i behandlingen av personuppgifter. Retrieved from https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-hallinnollisen-seuraamusmaksun-useista-puutteista-henkilotietojen-kasittelyssa?languageId=sv_SE 09.08.2020

Office of the Data Protection Ombudsman. (2020b). Påföljdskollegiet vid dataombudsmannens byrå påförde tre påföljdsavgifter för dataskyddsöverträdelser. Retrieved from https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista?languageId=sv_SE 09.08.2020

Office of the Data Protection Ombudsman. (n.d.a). Dataskyddsprinciper. Retrieved from https://tietosuoja.fi/sv/dataskyddsprinciper 22.07.2020

Office of the Data Protection Ombudsman. (n.d.b). Demonstrate your compliance with data protection regulations. Retrieved from https://tietosuoja.fi/en/accountability 25.07.2020

Office of the Data Protection Ombudsman. (n.d.c). Impact assessment. Retrieved from https://tietosuoja.fi/en/impact-assessments 30.07.2020

Office of the Data Protection Ombudsman. (n.d.d). Office of the data protection ombudsman. Retrieved from https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman 24.07.2020

Office of the Data Protection Ombudsman. (n.d.e). Personal data breaches. Retrieved from https://tietosuoja.fi/en/personal-data-breaches 30.07.2020

Office of the Data Protection Ombudsman. (n.d.f). Processing of personal data. Retrieved from https://tietosuoja.fi/en/processing-of-personal-data 22.07.2020

Office of the Data Protection Ombudsman. (n.d.g). Home. Retrieved from https://tietosuoja.fi/en/home 27.09.2020

Office of the Data Protection Ombudsman. (n.d.h). Controller's record of processing activities. Retrieved from https://tietosuoja.fi/en/controller-s-record-of-processing-activities 04.10.2020

Office of the Data Protection Ombudsman. (n.d.i). Processor's record of processing activities. Retrieved from https://tietosuoja.fi/en/processor-s-record-of-processing-activities 04.10.2020

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society, 21*(2), pp. 419-437. doi:10.1177/1461444818799523

PrivacyAffairs.com. (2020). GDPR fines tracker & statistics. Retrieved from https://www.privacyaffairs.com/gdpr-fines/ 09.08.2020

Psychogiopoulou, E. (2017). The European Court of human rights, privacy and data protection in the digital era. In M. Brkan, & E. Psychogiopoulou (Eds.), *Courts, privacy and data protection in the digital environment* (pp. 32-62). Cheltenham, England; Northampton, Massachusetts: Edward Elgar Publishing.

Regulation 2016/679. *The protection of natural persons with regard to the processing of personal data and on the free movement of such data*. European Parliament, Council of the European Union. (2016). Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*(2), pp. 63-75.

Sports Tracking Technologies. (2016). Privacy policy. Retrieved from https://www.sports-tracker.com/privacy-policy 20.07.2020

Teixeira, G. A., da Silva, M. M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance, Vol.* 21(4), pp. 402-418. https://doi.org/10.1108/DPRG-01-2019-0007

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), pp. 134-153.

Tinder. (2018). Tinder privacy policy. Retrieved from https://policies.tinder.com/privacy/intl/en#information-we-collect 20.07.2020

Treaty No. 108. (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).* European Parliament, Council of the European Union. Available at https://rm.coe.int/1680078b37

Voss, W. G. (2012). Preparing for the proposed EU general data protection regulation: With or without amendments. *Business Law Today, 2012*(11), pp. 1-5.

Widerberg, K. (2002). *Kvalitativ forskning i praktiken*. Lund: Studentlitteratur.

Wolters, P. (2018). The control by and rights of the data subject under the GDPR. *Journal of Internet Law, vol. 22*(1), (2018), pp. 7-18.

APPENDICES

1 Interview Guide in English

GDPR interview guide - Responsible

1. Briefly explain what kind of organisation you work in?
2. Briefly explain what your tasks are?

3. How was GDPR introduced in the organisation?
4. What kind of challenges did you face with the implementation?
5. How much time do you estimate that the employees, on average, for familiarising themselves with the GDPR?
6. How well prepared do you estimate that the employees were at the time of the implementation?

7. What kind of material have you used for getting information about the GDPR?
8. How did you get the material?
9. What kind of training and support have the employees been offered for guidance?
10. What kind of procedures do you follow for ensuring compliance of the GDPR?

11. What are the biggest challenges in terms of monitoring compliance? How do you handle them?
12. Ultimately, who is accountable for compliance in your organisation?

GDPR interview guide – Informed

1. Briefly explain what kind of organisation you work in?
2. Briefly explain what your tasks are?

3. How was GDPR introduced to you?
4. How much time have you spent familiarising yourself with the GDPR?
5. In your opinion, how well prepared for the GDPR were you at the time of the implementation?
6. What kind of challenges has the GDPR caused in your daily work?

7. What kind of guidance regarding the treatment of personal data have you received?
8. Do you feel like you have received enough support and information about the GDPR?
    a. IF NO: What kind of support/information would you have liked to receive?

9. What kind of procedures do you follow for ensuring compliance with the GDPR?
10. Ultimately, who is accountable for compliance in your organisation?

2 Interview Guide in Swedish

Intervjuguide Ansvarig

1. Kan du kort beskriva vilken typ av organisation som X är?
2. Kan du kort beskriva vad ditt jobb går ut på?

3. Hur introducerades GDPR i organisationen?
4. Hurdana utmaningar stod ni inför i och med implementeringen?
5. I genomsnitt hur mycket tid uppskattar du att de anställda har använt för att bekanta sig med GDPR?
6. Hur väl förberedda uppskattar du att de anställda var då förordningen trädde i kraft?

7. Vilken typ av material har du använt för att bekanta dig med GDPR?
8. Hur fick du tag på materialet?
9. Vilken typ av vägledning och stöd har de anställda erbjudits för att få information om GDPR?

10. Vilken typ av procedurer använder ni er av för att säkerställa att ni följer GDPR?
11. Vilka är de största utmaningarna med att övervaka att GDPR följs? Hur hanterar ni dem?
12. I slutändan, vem hos er är ansvarsskyldig för att GDPR följs?

Intervjuguide Informerad

1. Kan du kort beskriva vilken typ av organisation som X är?
2. Kan du kort beskriva vad ditt jobb går ut på?

3. Hur introducerades GDPR för dig?
4. I genomsnitt hur mycket tid uppskattar du att du använt för att bekanta sig med GDPR?
5. Hur väl förberedd uppskattar du att du var då förordningen trädde i kraft? (25 Maj 2018)
6. Hurdana utmaningar har GDPR orsakat i ditt dagliga jobb?

7. Vilken typ av vägledning om dataskydd har du fått?
8. Tycker du att du har fått tillräckligt med vägledning och information om GDPR?
    a. Om INTE: Vilken typ av vägledning och information hade du önskat?

9. Vilken typ av procedurer använder följer du för att säkerställa att du följer GDPR?
10. I slutändan, vem hos er är ansvarsskyldig för att GDPR följs?