RIITTA VALAVUO

GDPR – after the hype

DEGREE PROGRAMME IN BUSINESS MANAGEMENT
AND ENTREPRENEURSHIP

2020

Author Valavuo, Riitta	Type of Publication Master's thesis	Date November 2020
	Number of pages 44 + 6	Language of publication: English

Title of publication
GDPR – After the hype

This thesis was done to answer the following questions: What is the difference between the national act and the EU's regulation? How do the companies see the challenges? Has anything improved? Have people used their right to see what data has been collected from them? What kind of security breaches are there and how are they handled? What would the companies do differently now?

The main intent was to study the new Data Protection Act and compare it to the General Data Protection Regulation in order to see how it was complemented. This study also focused on the implementation and monitoring of the two. Also data protection and data security were briefly explained. The legislation is still fairly new and there is no case law. The first fines in Finland have been issued during summer 2020.

This study was a case study using mixed data collection methods. A case study is often used when researching a particular phenomenon, in this case the legislation and its adaptation. The main focus of this thesis was on the interviews and the data collected by them. By this way the research questions could be answered.

The GDPR and later the Data Protection Act applies to everyone and none of the companies regardless of their size are excluded. This means that these matters should affect us all. It remains to be seen how the data protection will be seen in future and how it will develop, what will be the means and also the consequences if not followed. This thesis studies it as is currently giving companies a brief introduction to the matter. This thesis can be used as a guide or as a source of reference material making it easier to understand what it is about.

Key words
GDPR, data protection, data privacy

CONTENTS

ABBREVIATIONS (IN ORDER OF APPEAREANCE)

GDPR	General Data Protection Regulation
EU	European Union
ERP	enterprise resource program
ID	identification
MFA	Multi-factoring Authentication
USA	United States of America
EDPB	European Data Protection Board
EFTA	European Free Trade Association
EEA	European Economic Area
CEO	Chief Executive Officer
HVAC	heating, ventilation, and air conditioning
SME	small and medium sized company
G20	Group of Twenty, an international forum for the governments from 19 countries and the European Union
G7	The Group of Seven is an economic organization consisting of seven major developed countries: Canada, France, Germany, Italy, Japan, the United Kingdom and the United States (Chen, 2020)

1 INTRODUCTION

In general, people understand the importance of their privacy and want to preserve it. Yet at the same time they are free willingly sharing information about themselves, their shopping habits and movement. This is not seen as a threat nor a problem by most. In order to have unified standards, legislation is needed.

The General Data Protection Regulation came into force on 25.5.2018 after a two-year transition period. The regulation displaced the old-fashioned directive that had not served its purpose. The goal was to grant similar rights to all people throughout the EU while providing the companies equal opportunities to function. As companies operate multi-nationally this was an important step. One of the goals was also to ensure the free movement of people and their information. Even though there was a transition period, many companies were poorly prepared. Some did not think that the regulation changed anything, some overreacted. In addition, individuals started using their right to check the information gathered from them. This strained the companies even more.

The Data Protection Act came into force in Finland on 1.1.2019 making the Personal Data Act obsolete. This act will complete the EU's regulation and it is designed to be used simultaneously with it defining some problematic points. The act also defines the authorities and explains some of the special circumstances. (Ministry of Rights, 2018) As national acts can only tighten the EU's regulation, these two are compared to see the differences and what the changes and special cases are.

At the time GDPR was about to put into force, a huge and also vigorous campaign was ongoing to both inform about the changes but also to sell different related services. European Union had an information campaign, so did the national officials to inform both people and organizations about the changes. Companies were contacted by various operators to sell services related to preparations for GDPR. This combination

created a hype around the GDPR. This continued for a while and was finally diminished. Most likely this also affected the companies in a negative way, eventually this marketing was seen annoying and it may have had an impact on the preparations. The same did not happen with the Data Protection Act, in fact, very little was published about it. Both of these facts may have an influence on how the companies see the legislation and how they have prepared. In this thesis these preparations and also the image of GDPR will be studied.

In the writers' bachelor's thesis, General data protection regulation and changes caused by it in a case company, GDPR and the changes made because of it in an ERP (enterprise resource planning) program were studied. The purpose of that thesis was to explore what GDPR retained and what the case company would need to change in their program so that it would comply with the regulation. The modifications were tested, and written instructions were made for them and their customers. That thesis also was used as a guide by that company. For this thesis, that company's representative will be interviewed to see the status of the company and their ERP program now. This is done to see if they had to make additional changes, if all the changes they did were necessary and if would they do now something differently. These findings will be compared with other companies and organizations to see how they prepared originally and if they share the same views and problems.

The legislation is still fairly new and there is no case law. The first fines have now been issued in Finland after GDPR has been effective for two years. It seems like GDPR and the Data Protection Act are somewhat forgotten even if they should be present in our daily lives and especially emphasized and practiced by each company and organization. This thesis aims to see the companies' point of view in practice. The national act will also be viewed and compared to GDPR.

2 PURPOSE, OBJECTIVES AND FRAMEWORK OF THE STUDY

2.1 The purpose and objectives of the study

The purpose of this thesis is to study and compare the legislation on national and EU level, and how do the companies see and understand them. The preparations the case companies did in 2018 when GDPR was introduced will be studied as well in order to see if they were necessary, did they need to make additional changes later and what challenges they have faced if any. The main research problem is what is the difference between the national act and the EU's regulation. How do the companies see the challenges? Has anything improved? Have people used their right to see what data has been collected from them? What kind of security breaches are there and how are they handled? What would the companies do differently now?

A questionnaire was sent to the 730 members of Rauman Yrittäjät ry in spring 2019 and again in summer of 2019 to gather data that could be then deepened via interviews. The interviews are done during summer 2020. Because of the Covid-19 crisis at hand they are all done either via email, phone or then online. The first interview will be conducted to the ERP company of the previous thesis to see the status now. The other interviews are done to see if companies share the problems and thoughts. The other interviewees are selected so that there would be always at least two companies sharing something either in the field that they operate on or they are of similar sizes.

An interview will be done to a representative of another ERP company, a competitor. Both operate in the same field; their programs are designed for construction companies. Interviews are done also to two public sector organizations, to a local accounting company (both programming companies also provide accounting and payroll services) and few larger companies in the field of insurance and telecommunication. In addition, the Data Protection Ombudsman will be interviewed.

The theory part of the thesis focuses on the national Data Protection Act and the monitoring of it and GDPR. As the role of the Data Protection Ombudsman is established by the act it is also emphasized in the study.

2.2 The framework of this study

The Figure 1 below shows the frame of this study. It follows the list of contents.

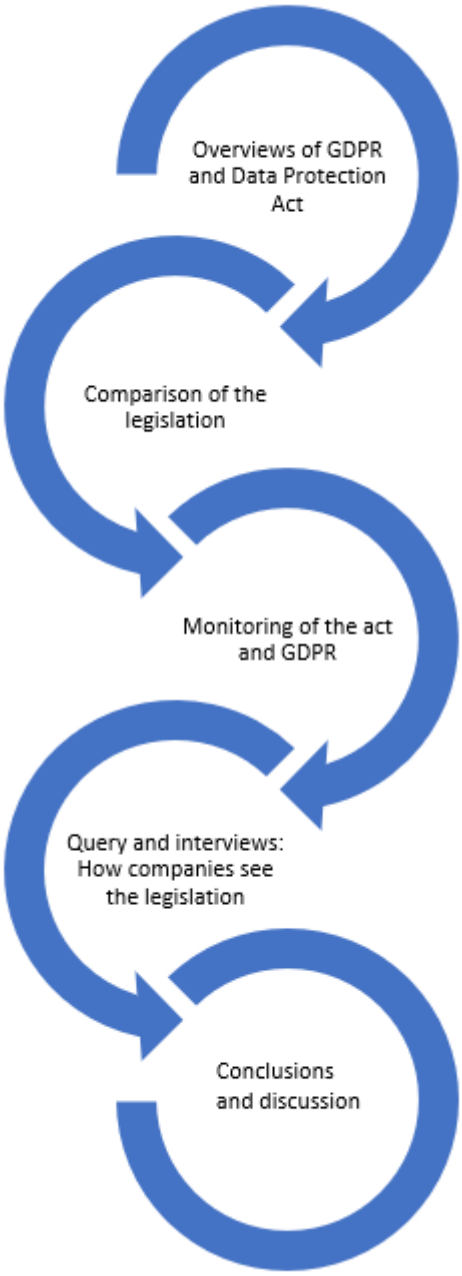

Figure 1. The framework of the study.

The study begins by defining what is meant by data security and privacy and then continues by an overview to both GDPR and the Data Protection Act. The thesis itself could be used as a guide by the companies pointing the reader towards the right

direction by explaining the legislation and the terms in a simple way. Collecting information from the organizations is vital and can be later used by others either as an example or cross-referencing.

3 DATA PROTECTION AND DATA SECURITY

Data privacy refers to the means of keeping a person's information and information about his actions safe so that it cannot be collected or used without permission. Data privacy or simply privacy refers always to a person. Data security aims on keeping information intact and confidential. (Järvinen, 2010, p. 15) This leaves a lot in the hands of the person itself. Even the strictest laws and regulations will not work if the people are willing to share their information.

When people think about data security they often think about firewalls, updates, and computer viruses. But data security and protection is much more than just that. The usage of Internet and online services have skyrocketed in private households. Even older people are using tablets, mobile phones or computers to read newspapers or use internet banking systems. Our society pushes and drives them to do that. People who do not have online banking ID are a rarity and often must struggle to get service otherwise. Online banking ID is used to verify one's personality in many public services but also on other services like for example tax services and insurances.

It is impossible to know on how many databases our information is preserved in. It often depends on the individual and his activity – for example if one is not on social media platforms, less information is listed and can be found. It is often the user's choice of where he registers and what information he is willing to share. One should always think about this before entering the information. There is always a chance of it getting into wrong hands.

Data security is a broad concept and not easily defined. It can be seen as confidence and integrity. If an information is classified as confident it means that its usage is

limited to certain, pre-defined people. This is often done by limiting the access based on the user profiles. It might be a wise idea to use different email addresses for work related Internet sites and other platforms and another for leisure or private usage. The passwords used should also be different and it is not recommended to use the same password on all services used. (Rousku, 2014, pp. 29-33) It is vital to keep the user ID and password to oneself and not to save it on a browser of written on a paper under the keyboard. (Rousku, 2014, p. 44)

Multi-factoring Authentication (MFA) uses more than one factoring whilst identifying a person. It is asked in addition to a username and password when signing into a service, an application, or a program. Also signing in with a banking ID is a good example of MFA. This additional verification can be for example a pin code sent to a mobile phone or a scanned fingerprint. (OneLogin, 2020) In figure below is an example of strong authentication. Often steps two and three are optional and not necessarily both used simultaneously.

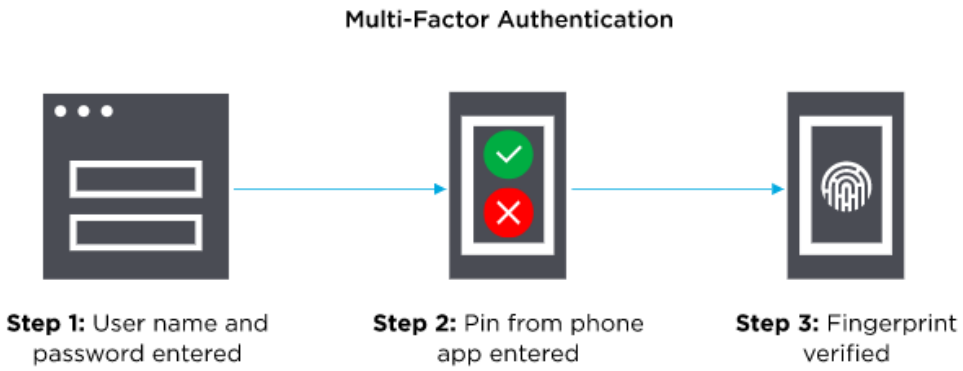

Figure 2. Multi-factoring Authentication (OneLogin, 2020)

When talking about data security one must think also about vulnerability. A program can be vulnerable for many reasons. One of them is an outdated version of a program. It is easy to keep the computer and its programs up to date by enabling the automatic updates, yet this is still often ignored. Also, a perpetrator utilizing a vulnerability in a program to enter the computer can use a spy ware or other malware to collect information from the user making the computer and its information vulnerable. (Rousku, 2014, p. 30)

We leave traces of ourselves everywhere we go and of everything we do. We are registered daily in so many ways that it is impossible to keep track of it all. It is also impossible to deny the registration or to avoid it. Mobile phones track us, when we go shopping information is registered, we are followed when we go to our workplaces. A huge amount of data is gathered and registered everywhere, even by the officials. We give a lot of information about ourselves to different registers and often free willingly. It is done in order to get discounts, pleasure or simply because we need to. We are also adding information, checking the information, and processing the information. The phenomenon is not new but has changed and increased by the technology. (Järvinen, 2010, p. 9)

Some registers are needed and considered to be good, like our health databases. But databases are different and can be used in various ways. In USA, the information collected in a register is owned by that registrar and there are companies whose sole purpose is to collect personal information in order to sell them forward. And because this is done businesswise there is no way of checking or correcting the information. (Järvinen, 2010, pp. 249-268) This is one of the main reasons why European Union chose to create the General Data Protection Regulation.

Not all information is personal data. Personal data is information that can be used to identify a person directly or indirectly. Combining an individual data item with some other piece of data that enables identification, are personal data. Persons can be identified by their name, personal identity code or some other specific factor. Personal data are for example: phone number, email address, car registration number and IP address. No matter in which format the data is collected or saved or how it is processed, if a person can be identified with it, it is a subject to the GDPR. (Office of the Data Protection Ombudsman, n.d.)

Finland got the first Person Register Law in 1988 and it was followed by Personal Data Act in 1999. Some forms of privacy is protected also by the Constitution law like the inviolability of the mail for example. How to process and maintain private data by the authorities is managed in several acts like for example in the Population Register or the register of right to study. (Office of the Data Protection Ombudsman, n.d.) The General Data Protection Regulation created unified regulation to be used in the whole

European Union. Later it was followed by the national regulation, The Data Protection Act. These will now be studied further in the following chapters.

4 A BRIEF OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION

The European Parliament and Council of the European Union have established regulation 2016/679 on 27.4.2016. After a two-year transition period it came to force on 25.5.2018 in the whole European Union, making the previous directive obsolete. The purpose of the regulation is to protect the natural persons by defining how their personal data should be processed and also to ensure the free movement of such data. (European Parliament and Council of the European Union, 2016, pp. 1-6)

In order to understand the GDPR and later the national Data Protection Act, few concepts need to be defined. **Personal data** means any information that can be used directly or indirectly to identify a natural person (also called a data subject in the regulation). **Pseudonymization** means altering the information in such a way that it cannot be linked anymore with the original data subject without additional information. This additional information has to be protected as well. **Processing** of the data refers to any action done automatically or manually to the collected personal data. It includes all the actions done including collection, storage, and erasure. **Profiling** means any form of automated processing of personal data to evaluate personal aspects in order to analyze or to predict the behavior or performance for example in work or economic situations. **Controller** is the person, organization or other body that determines the purposes and means of the processing of personal data. **Processor** is the one who processes the data on behalf of the controller. (European Parliament and Council of the European Union, 2016, pp. 111-112)

The main principle in the GDPR is listed in Article 5. It clearly states that personal data has to be processed lawfully, fairly and in a transparent manner. It can be used only for the purpose it is collected to (purpose limitation) and only the information that

is needed can be collected (data minimization). It has to be kept accurate and up to date. The data has to be stored in a way that it is protected against unlawful usage and entry and it has to be protected from accidental loss or damage. (integrity and confidentiality). The information cannot be stored if it is not needed anymore for the original purpose, however the information can be stored if needed for example for research purposes (storage limitation). The controller of the information has to be able to demonstrate that they have done everything accordingly. (European Parliament, Council of the European Union, 2016, pp. 117-118)

4.1 Rights of the data subject

The data subject has to give their consent to use and collect the information unless it is done because of a public interest or other legitimate reason. This permission to use the information has to be stated in such a clear way that the person is able to understand it and it can and it cannot be for example a pre-ticked box on a Web site. The controller has to be able to demonstrate that they have been given the right to collect the information. A person can withdraw the consent whenever they want. A child under 16 cannot give their permission to this but the guardian can. (European Parliament and Council of the European Union, 2016, pp. 118-123)

Collecting and processing of so-called sensitive information is forbidden. This information includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, health related issues or data concerning a natural person's sex life or sexual orientation. This information can be processed and stored only on specific cases and then special care has to be taken. The information can be obtained and processed for example when dealing with employment and social security issues. (European Parliament and Council of the European Union, 2016, p. 124)

The data subject has the right to know what information the controller has and how it is being processed and stored. He also has the right to get the information corrected if it is flawed, pseudonymized, anonymized or deleted. A person has also the right to refuse the usage of automated profiling if alone that is used in decision making, in this

case the decision has to be checked and made by a human. (European Parliament, Council of the European Union, 2016, pp. 138-141,147)

4.2 Controllers' responsibilities and the supervision of the regulation

The controller is responsible for the material collected, its storage, processing, and removal. This is described in detail in the regulation. If there should be a data breach that would have a significant impact on a person, the supervising body and the data subject have to be informed as soon as possible and not later than 72 hours. (European Parliament, Council of the European Union, 2016, pp. 162-163)

The regulation states that each member state shall appoint a supervisory authority. It lists the competences, tasks, and powers that this authority would have. It also describes how the European Data Protection Board will be formed. (European Parliament, Council of the European Union, 2016, pp. 199-212, 228)

The supervisory authority can issue a fine for infringements up to 20 000 000 euros or 4 % of the annual turnover, whichever is higher. (European Parliament and Council of the European Union, 2016, p. 246) The controller or the processor has to compensate the damage inflicted to an individual if he suffers from an infringement unless they can prove that they have taken the necessary precautions. (European Parliament and Council of the European Union, 2016, p. 92)

4.3 Conclusions

The GDPR lists in detail the rights each person has, what data can be collected, how to process and protect it. It also gives detailed information on what the controllers' responsibilities are and what to do. The formidable fine is to act as a serious deterrent for the controllers. What might be overlooked is the fact that this regulation is to be followed by all organizations, the only exception is private households. This means that each company despite the size or field, every association, club, and trust including the public operators are to obey these rules.

Previously private persons did not have such a possibility to check their information, deny its collection and usage. Now if the person chooses, they have the opportunity to do so. All companies operating in Europe have the same rules. This will have an effect on the market, unifying the ways companies operate.

5 OVERVIEW OF THE NEW DATA PROTECTION ACT

The Data Protection Act (1050/2018) was created to specify and supplement the GDPR. One of its major purposes is to define the supervisory authority on data protection matters. (Office of the Data Protection Ombudsman, n.d.) The GDPR says that the information must be kept coherent. It means that the information should not change uncontrollably. This can be obtained by controlling the access to the information and by defining the rules of what can be done and how.

The scope of application of The Data Protection Act states that this act does not apply to parliamentary activities. It means that matters like processing of personal data in criminal matters and how to maintain national security are excluded from this act. Otherwise the act states that GDPR is applied. (Ministry of Justice, Finland, 2018)

5.1 Processing personal data

The act specifies when and by whom personal data can be processed. It can be processed by a person or entity to fulfil duties. The processing of data must be proportionate and necessary for the performance of a task carried out. The data can be also processed and saved while conducting a study or for statistical reasons. Processing and gathering information of a child who is under 13 is prohibited. (Ministry of Justice, Finland, 2018)

The Data Protection Act lists cases when the information can and must be processes and gathered even though they are considered to be sensitive. This kind of information can be handled if they are linked for example to health care of social benefits or insurances, or the information is needed to fulfil duties listed elsewhere in legislation like providing information of union membership. The act also lists the means and measures on how to control and process this sensitive information. The usage of data has always to be justified. If a person has gained information while processing the data, this information may not be passed on to a third person or to be used in advantage of the recipient of the information nor in disadvantage of anyone. (Ministry of Justice, Finland, 2018)

The act also defines the cases when the personal identity code can be recorded and processed. In most cases the code can be a part of the register if a statutory duty is fulfilled of if the code is needed to absolutely identify the person while performing a monetary issue like issuing a credit or loan. Otherwise it can be recorded if address information is being updated or to prevent redundant postal traffic and the registrar already has the code. Apart from the above mentioned, the personal identity code can be recorded only if the data subject has given consent to it. The code should not be in printed copies of a filing system. (Ministry of Justice, Finland, 2018)

5.2 The supervisory authority

The supervisory authority is the Data Protection Ombudsman who works under the auspices of the Ministry of Justice. This Ombudsman has at least two Deputy Data Protection Ombudsmen and can hire additional staff if needed. The Ombudsmen are appointed for five years and have to have a master's degree of Law and additional degree in International and Comparative Law. In addition, the office has an expert board of five members and each of them also have a deputy. This board of experts is appointed by the government for three years at a time. (Ministry of Justice, Finland, 2018)

A person that feels that his rights are being violated can refer that matter to the Data Protection Ombudsman. This person must be kept unanimous when investigating the

matter and the personality should not be revealed. The Ombudsman has the right to refuse to investigate the matter if it is already being processed in a court. The Data Protection Ombudsman can pass a conditional fine if there has been a violation. These fines cannot be imposed to a natural person as these matters would be then handled as a criminal offence. The punishment for a data protection offence is laid down in the Criminal Code. (Ministry of Justice, Finland, 2018)

5.3 How does the national act differ from the GDPR?

The European Union operates on the principle of conferral of powers. This means that its members have disclosed their power to the EU on certain levels. It can operate only on matters enclosed in the treaty and on other matters the highest power is in the hands of its member states. EU has three legislative levels: regulation, directive and ruling. The regulation is to be in force in all the member states, the directive gives legislative guidance on national level and the ruling is binding only to them who it is demonstrated to. This means that the General Data Protection Regulation is then automatically in force in all the member states and it can be only elaborated nationally. (Ulkoministeriö, Eurooppatiedotus, 2019) The regulation was originally designed in a way that it will be completed with national acts like was done in Finland with the Data Protection Act.

The purpose of the national Data Protection Act is to answer some of the questions left open by the GDPR and to define certain topics. The Data Protection Act gives information on the following points:

- the age limit for of a child in this context
- the processing of special categories of personal data
- defines the processing of personal data for journalistic purposes or the purposes of academic, artistic, or literary expression
- the processing of personal identity codes
- certain situation in which the public interest constitutes a legal basis for processing personal data and
- restrictions of the right of the data subject.

But first and foremost, it defines the supervisor roles and the means of exercising the supervisory rights. (Office of the Data Protection Ombudsman, n.d.)

The table in Appendix 1 compares the GDPR and the Data Protection Act in more detail.

5.4 Conclusions

Even if amendments and clarifications are given in the national act, at least few matters still stay unclear. The article published in the Official Journal of the European Union about General Data Protection Regulation strives to explain the regulation in detail. In the preface the journal states the following: "*The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum*" (European Parliament, Council of the European Union, 2016, p. 22). The time or retention period is not defined in the regulation itself nor in the national act. This forces the collector to either use their own estimation on how long the information is needed or to refer to other legislation to see what is stated there. Specific retention times are listed for example in Accounting Act and several acts concerning employment.

Also, the compensation for the data subject in case of infringement is not defined in detail in either legislation. GDPR states that it will be a matter of court of justice. (European Parliament and Council of the European Union, 2016, p. 92) This matter could have been defined in the national act.

6 MONITORING THE DATA PROTECTION ACT AND GDPR

Most companies and organizations need to comply with the GDPR and the Data Protection Act, only households and private persons are ruled out. A lot falls in the hands of the private person as they are usually the ones who notice that their rights are

being infringed or they make the initiative to have their data checked. Data protection rights are there to help individuals to manage the data.

First the person needs to contact the company or organization, the controller. The controller is to answer without delay and no longer than one month. If they deny answering or do not give the information asked, the person can then contact the authority which in this case is the Data Protection Ombudsman. (Office of Data Protection Ombudsman, n.d.)

6.1 Data Protection Ombudsman

The post of the Data Protection Ombudsman was established in 1987 by Act 474/1987 of Data Protection Board and Data Protection Ombudsman. (Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta, 1987) Its role has changed many times after that when new legislation has come to force. The latest update was when the Data Protection Act came to force in January 2019. With that law, the Data Protection Ombudsman who works under the auspices of the Ministry of Justice was appointed as the national supervisory authority referred to in the GDPR.

The government points the Data Protection Ombudsman every five years. Reijo Aarnio was the Data Protection Ombudsman since the post was established in 1987. From 2019 to 2020 he had two deputies, Anu Talus and Jari Råman. On 1.11.2020 Anu Talus was appointed to the chair of Data Protection Ombudsman while Jari Råman acts now as her deputy. The Data Protection Act states that the Data Protection Ombudsman and the Deputy Data Protection Ombudsman must have a master's degree in Law and additionally other than a master's degree in International and Comparative Law. (Ministry of Justice, Finland, 2018)

The Office of the Data Protection Ombudsman has also an expert board that is appointed every three years. The board has a chairperson, deputy chairperson and three other members and each of them has a deputy. The expert board has the same qualification requirements than the Ombudsmen. (Ministry of Justice, Finland, 2018)

6.1.1 Powers and tasks listed in the GDPR

The tasks of the Data Protection Ombudsman are listed in Article 57 in the GDPR. The tasks include for example the following:

- monitor and enforce the application of the regulation
- promote public awareness on the rights and understanding the risks data processing has
- promote the awareness of controllers and processors of their obligation
- advice the data controllers of the regulation and the proper handling of data
- advice government and other institutions of the regulation
- handle the complaints launched by the individuals
- conduct investigations also without a complaint when necessary
- encourage the establishment of data protection certification mechanisms and of data protection seals and marks and approve the criteria of certification
- approve corporate rules (European Parliament and Council of the European Union, 2016, pp. 205-208)

The powers of the Data Protection Ombudsman are listed in Article 58. There are both investigative and corrective powers. The powers include for example:

- to order the controller and the processor to provide any information it requires for the performance of its task
- carry out investigations, data audits
- access to the information collected and handled by the controller and the processor
- to issue warnings to a controller or processor on operations that are likely to infringe the data subjects' rights
- order the controller or processor to give the data subject their information if they have refused
- to order the controller to communicate a personal data breach to the data subject
- order a temporary or permanent ban to process data if the regulation has been infringed

- to withdraw the before mentioned certificate if the regulation has been breached
- to prescribe an administrative fine (European Parliament and Council of the European Union, 2016, pp. 209-212)

Both the tasks and powers of the supervisory authority are listed in detail in the GDPR. Many of the tasks are preventive aiming to provide information and guidance to all parties. The powers are comprehensive. The regulation also states that each EU member state can list additional tasks and powers for their appointed authority. This is now done in Finland with the Data Protection Act.

6.1.2 Powers and tasks listed in the Data Protection Act

In Finland, the Data Protection Ombudsman has also other tasks and powers than the ones listed in the GDPR. The Ombudsman has the right to obtain information also if it is classified secret when it is needed to fulfil his duties. They can also search the premises of the controller if a punishable infringement is suspected. The Data Protection Ombudsman may use external experts when needed. They may also request assistance from the police if necessary. Even though the data subject has the right to lodge a complaint for the Data Protection Ombudsman, it may be dismissed if it is already pending in a court. The Data Protection Ombudsman also represents Finland in the European Data Protection Board. Some limitations are set too. For example, the Data Protection Ombudsman does not monitor Chancellor of Justice of the Government or the Parliamentary Ombudsman. (Ministry of Justice, Finland, 2018)

6.1.3 Administrative fine

The administrative penalty payment listed in Article 83 is imposed by a collegial body. The collegial body consists of The Data Protection Ombudsman and the deputies. The penalty has to be given prior to a ten-year expiration period. This fine cannot be implemented on central government authorities, state enterprises, municipal authorities and other similar parties and organizations listed in the Act. (Ministry of Justice, Finland, 2018) The board has the right to impose administrative fines for data

protection violations. The maximum amount of the administrative fine is 4 % of the company's turnover or EUR 20 million whichever is greater. (Office of the Data Protection Ombudsman, 2020)

The first fines have been now implemented in Finland for data protection violations. The Office of the Data Protection Ombudsman's sanctions board has given these penalties on 18.5.2020 for three companies; Posti Oy (100 000 €), Kymen Vesi Oy (16 000 €) and a unanimous company (12 500 €). Posti failed to give information to its customers about how the collected data would be used. The data was passed on to other parties that then sent communications and direct marketing. This had happened after making change-of-address notifications to Posti. Kymen Vesi processed the location data of its employees by tracking vehicles with a vehicle information system. The information gained was used to monitor the working hours. The company had not done an assessment on the impacts of using the data. In addition, it created high risk to the rights and freedoms of data subjects. The company which name was not revealed collected unnecessary data like religious beliefs, state of health, possible pregnancy, and family status of their job applicants. (Office of the Data Protection Ombudsman, 2020)

6.2 European Data Protection Board

European Data Protection Board is a joint board of applying to police and criminal justice authorities in the European Union. The Board was established in 25.5.2018 when the GDPR came to force. (Office of the Data Protection Ombudsman, n.d.) The European Data Protection Board (EDPB) is an independent European body which consists of members sent and appointed by each member state of European Union. It has members also from EFTA EEA States, but they are not allowed to vote, and they cannot be appointed to any of the chairs. (European Data Protection Board, n.d.)

EDPB's goal is to ensure similar and unified application of the GDPR. They are making general guidance to clarify the terms of European data protection laws and they can make binding decisions towards national supervisory authorities to ensure the consistency. EDPB also act as an advisor in the European Commission. Their role is

not to answer specific, individual cases but rather to issue general guidance. They are active on cases which have cross-border effects (more than one state is affected by either the decision or the processor is present in more than one states). Each authority is to share the draft decision and EDPB will give their opinion on them before adoption. If this opinion is dismissed, they may adopt a binding decision. So far, they have not issued any binding decisions. (European Data Protection Board, n.d.)

7 METHODOLOGY AND IMPLEMENTATION OF THE STUDY

This study is a case study using mixed data collection methods. A case study is often used when researching a particular phenomenon, in this case the legislation and its adaptation. Case study is an inductive method that is often exploited when an efficacy of a theoretical framework is tested. It is often linked to mixed data collection approach utilizing observation, surveys, and interviews. This method typically answers questions How? and Why? and the research question often evolves as the study progresses. Case studies can include both qualitative and quantitative research and so does this one. (Adams, Khan, & Raeside, 2014, p. 98)

Quantitative research is often seen as the beginning of the research as it is based on methodological principles. This data is often in numerical form. It is a method of collecting data which then later can be analysed further. Qualitative research uses several methodical methods to collect and study non-quantitative issues like history or behaviour of people. (Adams, Khan, & Raeside, 2014, p. 6)

7.1 Implementation of the study

In this study we can list two major research problems: familiarizing and comparing the national act to EU's regulation and how do the companies see and understand them. The additional research problems are: has anything improved, what would the

companies do now differently and what kind of security issues have there been if any. The following chapters focus on actualizing this research.

7.2 Reliability and validity

Several methods can be used to process collected data in quantitative research. This survey uses nominal scale. In the survey the respondents are given several options where to choose from, for example where is the company operating, but they are not asked to rank anything which would be the case if ordinal, interval or ratio scale would be used. Simple random sample is used in data collection as the sample is a known unit, the entrepreneurs of a preselected group. (Adams, Khan, & Raeside, 2014, pp. 71, 73) The sample for the survey was 730 which can be seen already as a significant amount.

It is debatable what should be an acceptable response rate. Adam, Khan and Raeside state that a 20 percent response rate is acceptable. (Adams, Khan, & Raeside, 2014, p. 118) However, Yehuda Baruch has made several studies about response rates in academic studies. He has calculated that an average response rate in academical studies is 55,6. Never the less, this is not the only criteria to a successful study, the target group has to be also wide enough to represent the group under the study in a sufficient level. (Baruch, 1999, pp. 421-422) In this case the target group was fairly large. This study is not intended to rely on the survey alone, but the matter is meant to be deepened with interviews. These interviews will give the study the reliability and validity it would have otherwise lacked based on the survey alone.

8 SURVEY OF RAUMAN YRITTÄJÄT-MEMBERS

Different surveys and queries can be a great way to obtain large amounts of data and to gather information anonymously. Rauman Yrittäjät ry agreed to help on this task. In this case Microsoft Forms was used as it is easy for the participants to use and access

and it can be done anonymously. Forms has also built-in analytics which can be used and a possibility to export the information for example to Excel. The president of Rauman Yrittäjät sent the author's introduction and the link to the survey to their members first in a group email on 23.4.2019 and a reminder again on 29.5.2019. The emails and members were privileged information in which the author did not had access to. The link to the survey was sent to 730 members from which nine answered making the response rate 1,23 percent.

There are two main reasons why not to answer the questionnaire – either they did not receive it or did not want to answer. The first alternative the writer could not control as the distribution was done by a third party. If a questionnaire is sent to CEO's, their response rate is typically lower than the average, typically 21 percent. Also, if the questionnaire is sent to several firms, the average response rate is 20 – 30 %. Even in academical studies the response rate is often left out. This can be due to several reasons but one of the reasons is to be able to use the collected data in cases when the response rate is low. (Baruch, 1999, pp. 423, 425-426) The studies also show that the response rate declines year by year. (Carley-Baxter, Hill, Roe, & Twiddy, 2009) (Baruch, 1999, pp. 432-433) Apart from that, the response rate also varies by the field of study. (Carley-Baxter, Hill, Roe, & Twiddy, 2009, p. 3) Nevertheless, the response rate is too low in this case to be used for making conclusions.

8.1 Results of the questionnaire

Even if the questionnaire's response rate does not allow any interpretation, some points will be studied here.

The figure below shows that most of the respondents work in a company that operates locally. Six companies operate only locally on Rauma region, two in whole Finland and one also abroad.

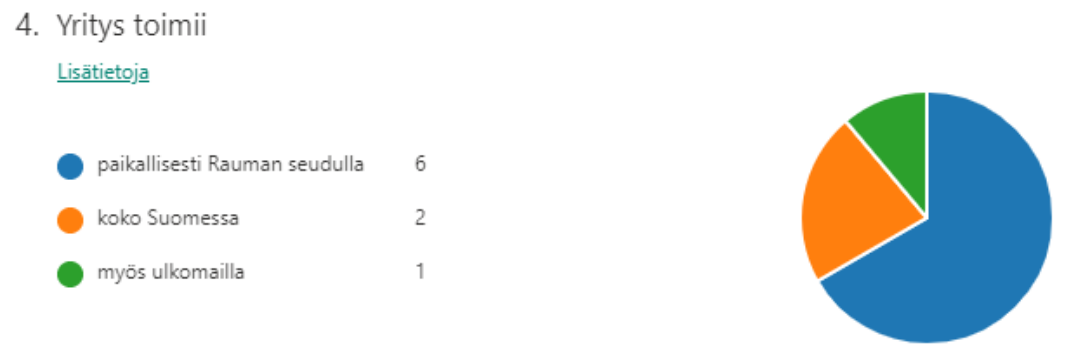

Figure 3. Where does the company operate? (Valavuo, GDPR, 2019)

Most companies have also private persons as customers and only one company has a webstore. Most of the companies have 1-4 persons working for them (5 out of 9) but three companies have more than ten people.

In question five the respondents were asked how they gathered information from GDPR in beforehand. This is shown in figure 4.

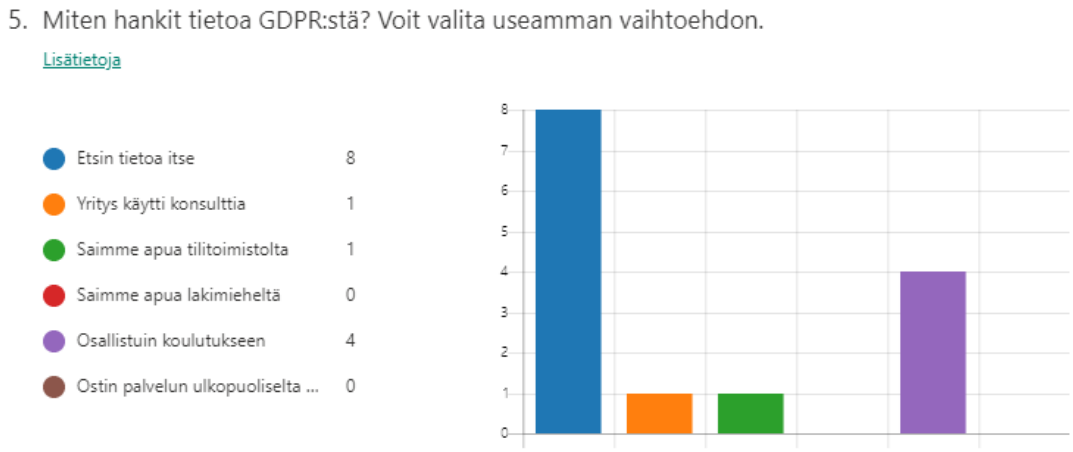

Figure 4. How did you acquire information from GDPR? (Valavuo, GDPR, 2019)

The respondents were able to choose more than one option but eight out of nine sought the information themselves, four took a training but only one used a consult or an accounting office. None used the help of lawyer and none outsourced gathering the information to an outside organization.

The respondents were given eight option for question which changes they did either to the companies' operations or operation style. Figure 5 shows the variance of the answers.

6. Mitä muutoksia yrityksen toimintaan tai toimintatapoihin tehtiin ennen GDPR:n voimaantuloa? Voit valita useamman vaihtoehdon.

8 Vastaukset

Tunnus ↑	Nimi	Vastaukset
1	anonymous	["Teimme ohjeistuksen henkilökunnalle toimintatavoista","Yrityksessä on nimetty henkilö, joka vastaa tietoturvasta"]
2	anonymous	["Ei mitään"]
3	anonymous	["Laadimme rekisteriselosteen","Teimme ohjeistuksen henkilökunnalle toimintatavoista","Pidimme koulutuksen henkilökunnalle","Päivitimme kotisivut","Muutimme verkkokaupan toimitusehtoja","Kysymme asiakkailta nyt luvan tietojen keräämiseen","Yrityksessä on nimetty henkilö, joka vastaa tietoturvasta"]
4	anonymous	["Laadimme rekisteriselosteen"]
5	anonymous	["Laadimme rekisteriselosteen","Yrityksessä on nimetty henkilö, joka vastaa tietoturvasta"]
6	anonymous	["Laadimme rekisteriselosteen"]
7	anonymous	["Laadimme rekisteriselosteen","Teimme ohjeistuksen henkilökunnalle toimintatavoista","Pidimme koulutuksen henkilökunnalle","Päivitimme kotisivut","Kysymme asiakkailta nyt luvan tietojen keräämiseen","Yrityksessä on nimetty henkilö, joka vastaa tietoturvasta"]
8	anonymous	["Ei mitään"]

Figure 5. The variance of different tasks the companies did to adapt to the requirements of GDPR. (Valavuo, GDPR, 2019)

Two of the companies did not do any changes. Two companies made only a Privacy Policy. Several companies chose to do more actions than one. In total, five companies made a Privacy Policy, and four companies named a person to be responsible for data privacy.

Six respondents consider data privacy to be very important to them. Seven respondents state that even though GDPR is included in the company culture, it does not show in the daily operations. One respondent thinks that the operation is now more difficult, yet one sees that the operation is now easier. The companies report that only few customers have contacted them in GDPR related matters, and few have used their

opportunity to check their information. Seven respondents state that they have not confronted any problems. One respondent says that the personnel information has now been stored in a locked storage with a limited access. Seven companies have their own policy on how to handle security breaches.

Figure 6 shows that even though the respondents were given several options on what they would do now differently they seemed to be unanimous on their answers.

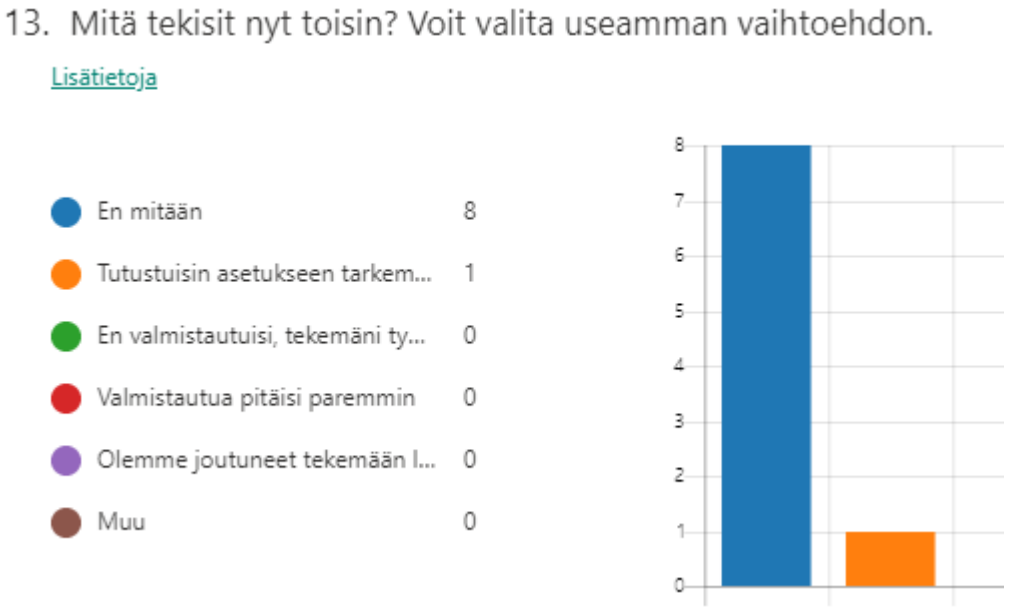

Figure 6. What would you do now differently? (Valavuo, GDPR, 2019)

Eight out of nine would not change their preparation and one would get more familiar with the regulation. None seem to think that the preparations were in vane nor would they see a need to prepare better. None have made additional changes later. Also, one respondent made a comment in the free text section that GDPR is bureaucratic and not relevant for a small company.

8.2 Conclusions

It seems that the respondents are from small companies operating mostly locally. This may have had an impact also to the response rate – if all the companies were small, perhaps they were not so familiar with the regulation and are maybe more likely to see it irrelevant. Also the ones who did answer say that they find data privacy to be

important, that may be the reason they chose to answer unlike the others. GDPR does not play a big role on the companies or their daily operations. Still they would not do anything differently.

9 INTERVIEWS OF THE CASE COMPANIES

In order to gain more information on this matter, interviews are conducted to a selected group of companies and organizations. The companies were selected so that they would represent either a same field of operations or size. There are also two larger companies involved in the fields of telecommunications and insurance. Two organizations from public sector are also studied. The interviewees are asked to answer the questions as they personally see them, and they are not necessarily experts of this particular matter even though all work in expert positions. All were also asked about their usage of Social Media because there has been a lot of debate on their safety. Two persons declined to be interviewed and so seven case companies were represented.

Overview of the key features of the interviewed companies are shown in table 1 below.

Company's field of operation	**Number of employees**	**Number of customers**
programming (ERP), accounting, and payroll	32	1 400
programming (ERP)	9	120
accounting and payroll	5	information not given
public sector, a municipality	3 000	about 40 000 if the whole population is seen as a customer
public sector, social and welfare	1 000	about 24 000 if the whole population is seen as a customer
telecommunication	4 000	2 800 000
insurance	4 000	450 000

Table 1. Key figures of the case companies.

Due to the pandemic, all the interviewees were given a choice of interview via email, phone, or Microsoft Teams. All the interviews were done eventually via email. Therefore, the interviews were done as a structured interview. The same questions were sent to each participant. The questions for the public sector organizations differed a bit from the ones sent to companies. The questions used can be found in appendices 2 and 3. Using this kind of method does not allow the interviewer to interact with the respondent but generates uniformed data which is then easy to compare. (McLeod, 2014)

9.1 Interview of an ERP programming company representative

The first interview was done to the same programming company to which the Author did her previous thesis to. The interviewee works as the Support and Training Manager. The ERP program is designed for construction companies and is especially used in HVAC (heating, ventilation, and air conditioning) companies. Apart from that the company also offers its customers payroll and accounting services. The company has 32 employees and about 1 400 customers. Most of their customers are SME companies (small and medium sized enterprises). The company or its operation have not significantly changed from the previous allowing comparison to the previous functions.

While preparing for the implementation of GDPR, the company used a law firm to consult and to set the boundaries on how to operate and what to take into consideration. These rules and ways of work were defined rather strictly yet they are now followed as such also today. They have increased the internal supervision and are regularly reminding the employees on ways of work. Otherwise the daily operations have not changed. The company has written instructions on what to do in case of security breach, but they have not had any issues.

The respondent sees the data privacy very important and considers himself to be very careful especially in private. He uses Facebook personally but none of the Social

Media channels as a company representative. The interviewee expresses his concern about identity thefts. He also works as a Data Protection Officer of the company.

Some customers have contacted the company to get information on how to delete information. He estimates that only 25 percent of the changes done to the program have been used. They implemented several features to the program including different searching options, pseudonymization, anonymization, and deletion function. He states that many of the customers do not care for example about the retention times at all. None of their customers have contacted them to see how they are handling the GDPR issues. He is not aware of any problems occurred for the customers either. In general, he says that their customers see GDPR and data privacy as unnecessary fuss and nuisance. Even though he now feels that they could have done less preparations, he says he most likely would have done the same as he personally sees this matter important.

9.2 Interview of an ERP programming company representative

The interviewee works as a Business Manager for a software company that designs an ERP program mainly used by construction companies. The company is a part of a larger group that operates not only on software but also on media sector. Many of the support functions, like in this case training and data privacy are handled and regulated by the group.

The software company also offers its customers payroll and accounting services via a third party. Their software can be linked to its services as requested by the customer forming a package. Some payroll and financial functions are done by using this program, some information and functions are transferred.

The software company itself employs 9 people and they have 120 customers. The company has now private consumers as customers and they do not have a web store. The company operates in the whole Finland.

The interviewee has taken part in various trainings organized by the group. In some of them there has been an external specialist but in most cases the Data Protection Officer has given the trainings. She has knowledge also on the national act. The respondent has searched information also on her own. GDPR has been taken into consideration in the development of the program and is an ongoing function for the company.

Before the GDPR was in force they gathered information, defined the data flows and where information is saved and how it is handled. They draw flow charts from the processes to understand them better. After this they were able to see what needed to be changed and how to preserve and delete the information. They also defined who can handle information and how it will be transferred making sure that it is not transferred if not needed.

All request for information, checks on what information is saved from a person or marketing bans are handled by each company and not on the group level. She says that some questions or comments come to them occasionally. The users for example inform them if they see some part of the program to be problematic, for example revealing information like social security numbers. In many cases this is a matter of finding the correct user rights which can be defined in detail in the program itself. They have not had data breaches or bigger issues neither on company nor on group level. The group has appointed a Data Protection Officer and have done Data Protection Notice for each service. All security issues would be handled by the Data Protection Officer.

The interviewee sees data privacy to be important but says that it is not visible in her daily life. She uses Facebook and LinkedIn but not as a company representative. She has contemplated on how much work GDPR and the changes require and whether the time and money used was worth it. By this she means that there was so many resources used that was it necessary.

9.3 Interview of an accounting company representative

The interviewee is a co-owner of an accounting company where she works as a CEO and an accountant. The company has five employees and serves mainly local

customers in Rauma area in accounting and payroll related services. They have appointed a Data Protection Officer and their Data Protection Notice is available on their web site.

The employees trained themselves in external trainings before the GDPR came into force. Their goal was to offer to take care of related issues for their clients. Most of the clients are small business and they did not see the need for this kind of service or expertise.

The interviewee seems to be disappointed on how the public and their clienteles reacted to the legislation. Even though she finds data privacy to be important especially in her line of work, she thinks that the legislation is too complex and distant for the smaller companies.

9.4 Interview of a public sector organization representative

The interviewee works as a Data Protection Officer of the public sector organization, a municipality. The organization has about 3 000 employees in group services, educational sector, social and welfare and technical services. Because of her work, the interviewee is well aware of both GDPR and the Data Privacy Act. She has obtained information from national instructions and from instructions provided by the Data Protection Ombudsman. The organization has provided several trainings to the employees by both national and private trainers. They have also trained the workers on how to work remotely.

Before the GDPR only the health and welfare sector had an appointed Data Protection Officer. Now this position is elaborated to cover all the functions. The organization also updated their internal instructions and created privacy statements and procedures. All the contracts were examined and updated. Some negotiations are still ongoing as not all the contract changes were agreed by the other parties. This updating process and trainings are still ongoing.

The whole chain of handling personal data has changed: the collecting, recording, disclosure, preserving and saving and deleting. This affects daily operations. Also the cyber threats are taken into consideration. The organization has been contacted by people to check the information recorded and the log-in information. They have also received hints of how to do things differently. The organization has also established an internal channel where to report data breaches and deviations.

The organization has done an Information Final Statement and their Data Protection Notice (all together 21 different Statements for different purposes) are available on their web sites. They have also taken Accessibility Directive into account. This directive handles the accessibility of websites so that the services would be available for everyone even if they would be for example visual impaired. At the moment this directive is valid only for public organizations. (Poutapilvi, n.d.)

The interviewee wants to lead by example, both in work and leisure time. She uses the latest updates, changes passwords, uses encrypted email and secure Internet connections and keeps her knowhow up to date. She uses LinkedIn, Facebook and Twitter. All in all, she sees data privacy and security very important.

9.5 Interview of a public sector organization representative

The respondent works as a Home Care Coordinator for a municipality. The social and welfare sector offers work to about 1 000 people. The interviewee has taken part on several trainings organized both by external and internal organizations. All the municipality employees need to do a specific online training. She has also obtained more information herself. The municipality has a Data Protection Officer, but the interviewee thinks that more dedicated personnel would be needed on this function, for example a specialist on operational level or support.

Even though the welfare services have professional secrecy and the information they collect and handle have been kept private, the interviewee still sees many problematic issues. For example, if something is not written down the assumption is that it is not done. She thinks that this is something they need to consider and change in a larger

scale. They have earlier used calendars and notebooks to document their work. Now these are archived and locked away. It has been a habit to have work shift tables visible along with contact information, these are no longer present. They have also restricted the areas where for example relatives and other outsiders can enter. They have also defined how long information is held and how to delete and destroy it. Unnecessary information is not to be obtained and saved.

They have received questions of what information is collected from the patients and customers and to whom it can be given to. The organization has done an Information Final Statement and Data Protection Notice. They have also rules on how to handle data breaches and other problems.

The interviewee sees data security important. She uses only WhatsApp personally. The welfare sector has Facebook pages which are updated centrally.

9.6 Interview of a telecommunication company representative

The interviewee works as an Account Manager working with corporate customers, not private consumers. The company in question has about 2,8 million customers both on private and public sector and employs about 4 000 people. The company has also a webstore and serves international customers as well.

The company offers training about data privacy and all the employees need to pass a test regularly in order to serve their customers. Due to the size of the company, many of the matters are handled by specific teams. Therefore, the interviewee was not able to answer many of the questions. The company has profound and well written information about data privacy for their customers to see. It explains in detail but in an easily understandable way the rights the customer has, the handling of data and so forth. The company has also provided its employees instructions on how to handle data security issues and breaches.

The interviewee sees data privacy very important and as an only way to control the information given. She also emphasizes the possibility to have her information deleted if she wishes so. She uses Facebook, LinkedIn and Instagram.

9.7 Interview of an insurance company representative

This interviewee works as a Customer Manager for one of the largest insurance companies in Finland. The company has about 1 000 employees and 450 000 customers. They have both private and company customers. They also have a webstore. The company operates in whole Finland.

The company has provided several trainings for its employees by both internal and external experts. The interviewee has also taken part in online trainings and follows this issue constantly. The company has made changes to several procedures after the GDPR and they have for example renewed the customer recognition process accordingly. New implementations have been introduced and the claims procedure renewed. The changes were done to fulfil the requirements in the legislation. The interviewee thinks that operating and working is now more difficult even though she sees this matter important.

To her knowledge there has not been many inquiries about the data privacy or GDPR related issues by the customers. She brings the subject up herself in the annual meetings she has with them. The organization has done an Information Final Statement and their Data Protection Notice is available on their website. They also have named a Data Privacy Officer. They have established internal procedures on how to handle data breaches.

The company has also introduced a new insurance type, a cyber insurance. It has proven to be useful also in Finland.

The interviewee uses mainly Facebook but has an account in LinkedIn and Instagram. In general, she sees data privacy and data security very important.

9.8 Comparison of interview results

All the represented companies have adapted their ways of work to the GDPR and they have appointed a Data Protection Officer and created Data Protection Notices. In most cases the interviewees say that the company has rules on how to handle deviations. All the companies have also provided training to their employees and some of them need to be taken annually or otherwise regularly.

All the respondents say that data privacy is important. They may see it important also because they operate and work in field where it is seen important or critical. Data privacy can also be seen as a tool to create trust towards the customers. Only two persons clearly state that they wish that security and privacy issues would be taken more seriously. Many respondents question the preparations done before GDPR thinking if they all were necessary or in proportion. Some also state that things are now more complicated and difficult even if they are at least partly satisfied with the changes and legislation.

The respondents were asked about their usage of social media. For example the German competition authority Bundeskartellamt has ruled that Facebook has to ask for permission to use information collected from its users on WhatsApp and Instagram. Facebook has filed a complaint against the decision saying that the information is needed to fight its competitors. Facebook says that it follows GDPR and criticises why the matter was handled by competition authority and not the data protection authority. (Linnake, 2020) Several services have similar issues, and it is debatable if these can be seen as safe to use. Even though this matter can be seen as a separate issue, it can be seen relevant as it gives information on how much information the respondents are willing to share themselves. Many of the respondents use more than one social media platforms and only one respondent lists WhatsApp as a form of social media even though we can assume that also the others use it.

10 INTERVIEW OF THE DATA PROTECTION OMBUDSMAN

The author had the opportunity to interview Deputy Data Protection Ombudsman Anu Talus who was later appointed to be the next Data Protection Ombudsman. She will take the office in November 2020. The interview was conducted by the phone.

The Office of the Data Protection Ombudsman is contacted about 10 000 times in a year, which means several contacts every day. Most of the contacts come from private persons, but also from companies. However, companies can only be advised at a general level, the authority cannot for example pre-check any Data Protection Notices. Reports of security breaches come directly from companies, individuals contact the office mostly regarding removal requests. They also receive so many lecture requests that they have to decline some of them.

The biggest workload comes from different control measures and hearings. Inspections are carried out either based on a public debate or because of notifications. Security breaches employ the office most, but these do not require a cumbersome procedure and thus do not take up a lot of resources. Anu Talus considers the control of the data subject's rights to be the most important task the office has. All notifications are processed, but if necessary, tasks can and will be prioritized. For example, reports of incorrect credit information are processed first, as this has major impact on the individual level. She emphasizes the all the tasks that have direct impact on a person’s daily actions and rights are the most important and urgent ones.

Now there are about 5 500 cases open. Before the GDPR they received only about 3 000 contacts per year, and it tripled when GDPR came in force They have been now able to clear the bottleneck with a separate project. Handling a case will take months because the company in question have to be heard and given 1-2 months’ time to respond already after the first contact. After this the Office will assess the case and start necessary actions and guide the company or organization.

The Data Protection Ombudsmen are also involved and employed by European co-operation. European Data Protection Board, EDPB has meetings monthly and in

addition to that thirteen work groups where the Finnish Data Protection Ombudsman's Office is also represented. Also the national legislation projects need to be orientated in. At the moment there are 100 legislation projects that involve data protection or security.

Without the Data Protection Act, fines could not be imposed. The General Data Protection Regulation alone would not be enough. According to Anu Talus, there could not be a better law or regulation than the current ones we have, even if they would be now redesigned and reworked. The regulation must be unified and work in the same way in every EU country and therefore cannot be very specific or detailed. It has also been the intention that the regulation will be supplemented nationally, just as has now been done in Finland. According to her, the procedures could work better and more harmonized in the EDPB, but this is still an ongoing process.

The feedback both for the Office and the legislation have been positive. The decisions have been seen good and fair.

11 CONCLUSIONS AND DISCUSSION

On 24th of June 2020, after two years the GDPR came into force, European Commission released an assessment on the GDPR and its effects. The assessment confirms that most of the objectives set have already been fulfilled. EU citizens have gained more rights and possibilities to monitor their data processing. Yet they state that procedures and execution need to be unified. The regulation has increased openness. People's awareness needs to be still increased so that they would be able to exercise their rights. The regulation has proved its flexibility also during the Covid-19 pandemic at hand. (Office of the Data Protection Ombudsman, 2020)

The commission states that in future they need to promote the issues of SME companies making the regulation easier to follow. Also the cases that are not national only need to be handled in an unified and more efficient way. Co-operation between

EU members and third parties must and will be developed further. (Office of the Data Protection Ombudsman, 2020) For example, the "Data Free Flow with Trust" initiative has been introduced to G20 and G7 leaders and in 2019 a mutual EU-Japan Adequacy Decision has been signed creating the largest area for safe data flows in the world. (European Commission, 2020)

The statistics are impressive: 4,3 million people and organizations have used the Commission's online portal on GDPR over the two years. 275 000 complaints have been launched over the infringements during the first 18 months. 69 percent of EU citizens have heard about GDPR and 71 percent are aware of their local data protection authority. Between May 1998 and November 2019, 785 fines were issued. (European Commission, 2020)

This thesis project begun from the interest to see how the companies see GDPR, how they prepared originally and whether they needed to make more changes or adaptation on how they handle data. At the early stages the survey was conducted to 730 companies from which most of them are small or middle sized. It soon became obvious that the matter was not seen important nor interesting. Unfortunately, the response rate for the survey was only 1,23 percent. That is not enough to make conclusions based on the material unless the response rate is considered to be a conclusion of its own – the matter was not seen important. The validity of the study could be enhanced with the interviews of the case companies. However, the same themes and end results were raised up in the interviews. As can be seen from the answers received, GDPR played a very small role for the companies even if it would be seen as important. The interviews confirmed this conclusion. It seems that the bigger the company is, better they have prepared, and these matters seen more important. This matter could be studied further – is there a correlation in between the company size and the importance of data protection.

The recent unfortunate happenings, the data breach of Vastaamo and news about other data protection problems and spying, hopefully increase the vigilance and help people and also the companies to realize the significance of both data protection and security. Companies and other organizations must react and make their systems better and more

secure. Handling security issues could become also a valuable asset in marketing, a way to distinct a company from its competitors.

Already at this stage it is clear that Vastaamo did not fully follow the GDPR. With the information we have we cannot say with certainty whether the protective measures were sufficient or if their impact assessment was done according to the legislation, this is under investigation by the Office of the Data Protection Ombudsman and other responsible parties. However, they failed to inform the data subjects personally about the data breach. This should have been done within 72 hours from the breach or of the date they gained the information. They should have informed the persons also of the actions they can do themselves to mitigate the harm done as well as the actions Vastaamo was to take. Health issues are the most sensitive ones, one's people do not want to reveal, and companies need to protect. They are also especially cared for in the legislation. Yet Vastaamo failed to protect this information.

This unfortunate case can teach a valuable lesson for all: we, as consumers and data subjects need to take care of our information but foremost the organizations need to take these issues seriously and enhance security. Organizations would need to pay attention to the following:

- Evaluate and estimate the collected information: is it needed, how long should it be saved, do we need to do a deeper evaluation of the above
- How the information is saved and protected and who has access to it.
- How is the information disposed?
- Inform the customers and other people about the above in a clear manner.
- If something should happen, act immediately, prevent further damage and inform the relevant parties of what has happened.

As what comes to us all, we too should take more active and caring role and to learn to protect our information. It can be done for example by following these steps:

- Read through the agreements before entering or disclosing information.
- Think carefully what information the organisation needs and are you willing to give it and what possible risks there might be if misused.
- Do not use same usernames and passwords in all applications and services you use. Change the password every once in a while and use MFA or other strong identification methods when possible.

As we can see from the interview of the Data Protection Ombudsman in Finland and from the Commission's evaluation, there had been a clear need for this legislation. It is seen as a clear improvement yet changes still need to be made. In Finland the Office of the Data Protection Ombudsman has not issued yet many fines or decisions. We can assume that when they do, also companies' awareness on the legislation, its requirements and data protection in general will increase. It is also clear that people's awareness of their rights still needs to be increased.

According to the interview, The Office of the Data Protection Ombudsman is contacted about 10 000 times in a year now when previously they received about 3 000 contacts. There is a steep increment yet companies that replied had not had any data breaches or security issues. This could also be worth of studying – what is the cause of the increase and what are the reasons why people contacted them. Could it be that they just waited for the regulation to be in force and then raised all the issues that were bothering them or is there more to it.

While collecting research material for the theory part, it became obvious that there are no books written about GDPR only even though there are plenty of data security and data protection. Hence, there is huge number of other sources of material available. There is limited amount of case law and practise. This study focuses on material that is most reliable, from selected and trusted sources only. Also law is studied as such without interpretation from third parties.

It seems that so far, that the companies are under the impression that they do not need to do anything or that they are doing enough as is. The recent incidents prove otherwise. Companies would need to be proactive and anticipate all possible scenarios. Companies and other organizations need clear information that is easy to comprehend and follow. The most important things to remember from the legislation are:

- the GDPR applies to everyone and to all personal data collected
- companies have the burden of proof on what comes to fulfilling the obligations
- in addition to the possible fine from the officials in case of data breach or misuse, organizations may need to compensate the damage to the data subjects

It is said that not even the strictest laws cannot protect us if we do not allow it to. If we are free willingly giving our information away, the protection is more difficult. People are willing to give their information for personal gain like promotions and discounts or to shop online, for example. It is rare to read the consent notices or information, it is easier to click yes on all the accounts. Like European Commission stated, the awareness needs to be increased. The author hopes that this study also increases the awareness of the companies on this important matter making the world a bit safer for all of us.

REFERENCES

Adams, J., Khan, H. T., & Raeside, R. (2014). *Research Methods for Business and Social Science Students.* SAGE Publications. Retrieved June 4, 2020, from https://uoasl.alma.exlibrisgroup.com/view/action/uresolver.do?operation=resolveService&package_service_id=1023236680005968&institutionId=5968&customerId=5965

Baruch, Y. (1999). Response Rate in Academica Studies - A Comparative Analysis. *Human Relations, 52*(4), 421-438. Retrieved August 16, 2020, from https://journals.sagepub.com/doi/pdf/10.1177/001872679905200401

Carley-Baxter, L. R., Hill, C. A., Roe, D. J., & Twiddy, S. E. (2009). Does Response Rate Matter? Journal Editors Use of Survey Quality Measures in Manuscript Publication Decision. *Survey Practise, 2*(2). Retrieved August 16, 2020, from file:///C:/Users/Riitta%20Valavuo/Downloads/CarleyBaxter-et-al_Does-Response-Rate-Matter_Survey-Practice-v2-n7-2009.pdf

Chen, J. (2020, October 21). *Investopedia*. Retrieved October 21, 2020, from Group of Seven (G-7): https://www.investopedia.com/terms/g/g7.asp

European Commission. (2020, June 24). *GDPR: the fabric of a success story.* Retrieved October 16, 2020, from Press corner: https://ec.europa.eu/commission/presscorner/api/files/attachment/865834/GDPR_factsheet-08.pdf.pdf

European Data Protection Board. (n.d.). *About EDPB*. Retrieved June 1, 2020, from European Data Protection Board: https://edpb.europa.eu/about-edpb/about-edpb_en

European Parliament and Council of the European Union. (2016, May 4). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and

on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*, p. 261. Retrieved May 25, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1

European Parliament, Council of the European Union. (2016, May 4). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*, p. 88. Retrieved May 25, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1

Järvinen, P. (2010). *Yksityisyys - Turvaa digitaalinen kotirauhasi.* Jyväskylä: WSOYPro Oy.

Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta, 474/1987 (April 30, 1987).

Linnake, T. (2020, February 12). Facebook valittaa Saksan kilpailuviranomaisen määräyksestä ja selittää siihen syyt. *Digitoday*.

McLeod, S. (2014). *The Interview Research Method*. Retrieved October 4, 2020, from SimplyPsychology: https://www.simplypsychology.org/interviews.html

Ministry of Justice, Finland. (2018). *Data Protection Act, Translation from Finnish.* Ministry of Justice, Finland. Retrieved May 24, 2020, from https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf

Ministry of Rights. (2018, December 5). *Ajankohtaista.* Retrieved December 11, 2019, from Uusi tietosuojalaki voimaan vuoden 2019 alusta: https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta

Office of Data Protection Ombudsman. (n.d.). *Have your data protection rights been infringed?* Retrieved May 27, 2020, from Private person: https://tietosuoja.fi/en/have-your-data-protection-rights-been-infringed

Office of the Data Protection Ombudsman. (2020, May 22). *Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for*

data protection violations. Retrieved June 1, 2020, from Currrent issues: https://tietosuoja.fi/en/article/-/asset_publisher/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista

Office of the Data Protection Ombudsman. (2020, June 25). *Uutiskirje*. Retrieved October 6, 2020, from Euroopan komissio julkaisi arvioinnin EU:n yleisestä tietosuoja-asetuksesta – uusi lainsäädäntö on parantanut kansalaisten oikeuksia: https://tietosuoja.fi/en/-/euroopan-komissio-julkaisi-arvioinnin-eu-n-yleisesta-tietosuoja-asetuksesta-uusi-lainsaadanto-on-parantanut-kansalaisten-oikeuksia

Office of the Data Protection Ombudsman. (n.d.). *Data Protection*. Retrieved May 24, 2020, from What is personal data?: https://tietosuoja.fi/en/what-is-personal-data

Office of the Data Protection Ombudsman. (n.d.). *Data Protection Legislation*. Retrieved May 24, 2020, from Office of the Data Protection Ombudsman: https://tietosuoja.fi/en/legislation

Office of the Data Protection Ombudsman. (n.d.). *Guidelines of the European Data Protection Board*. Retrieved June 1, 2020, from Current Issues: https://tietosuoja.fi/en/guidelines-of-the-european-data-protection-board

OneLogin. (2020). *What is Multi-Factor Authentication (MFA) and How Does It Work?* Retrieved November 10, 2020, from OneLogin: https://www.onelogin.com/learn/what-is-mfa

Poutapilvi. (n.d.). *Saavutettavuusdirektiivi edistää yhdenvertaisuutta*. Retrieved September 18, 2020, from Saavutettavuusdirektiivi.fi: https://saavutettavuusdirektiivi.fi/

Rousku, K. (2014). *Kyberturvaopas, tietoturvaa kotona ja työpaikalla.* Viro: Talentum.

Ulkoministeriö, Eurooppatiedotus. (2019, July 31). *Suomi ja EU*. Retrieved May 24, 2020, from EU-lakien suhde Suomen lakiin: https://eurooppatiedotus.fi/suomi-ja-eu/eu-lakien-suhde-suomen-lakiin/

Valavuo, R. (2018). *Tietosuoja-asetus ja sen aiheuttamat muutokset case-yrityksessä.* Rauma: Satakunnan ammattikorkeakoulu. Retrieved May 25, 2020, from https://www.theseus.fi/handle/10024/148607

Valavuo, R. (2019). GDPR. Retrieved from https://forms.office.com/Pages/AnalysisPage.aspx?id=165bUOHcWUWoORV9Fv_-b9Azk5jtzXBCttEnSWtJ5dlUOVM1T0ZUT1ZQWkNLTUYzRllYSjVCNjhCTy4u&AnalyzerToken=eRR6ViqojX5vGxBYk476Su3V1pr7kmx9

APPENDIX 1

	GDPR	Data Protection Act
Definition of a child	*… the processing of the personal data of a child shall be lawful where the child is at least 16 years old.*	*…processing of the personal data of the child is lawful where the child is at least 13 years old.*
Processing of special categories of personal data	*Article 9* *1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.* After this, nine exceptions are listed.	*Article 9(1) of the Data Protection Regulation does not apply:* *1) when an insurance institution processes data, it has received in the course of insurance activities* *2) to any processing of data that is provided by law* *3) to the processing of data concerning trade union membership as defined in employment law* *4) when a healthcare or social welfare service provider in the course of arranging or producing services* *5) health and genetic data can be processed when necessary to enable anti-doping work or sports for persons with disabilities or long-term illness* *6) to the processing of data for scientific or historical research purposes or for statistical purposes*

		7) *to the processing of research and cultural heritage materials for archiving purposes*
The definition processing data in means of academic, artistic, or literary expression	Article 85 states that each member state is to lay down a law where this is defined.	The act lists clearly which articles of GDPR do not apply if they would infringe on the right to freedom of expression or information.
Processing of personal identity codes	Personal identity codes are not mentioned in the GDPR as such but Article 4 states the following: *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name**, an identification number**, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person* This means that the GDPR also applies to processing of these codes	A personal identity code may be processed if the data subject has given consent to it or if so provided by law.

Certain situation in which the public interest constitutes a legal basis for processing personal data	Section 2, Articles 13 and 14 relate to information and access to personal data whether the data is collected with or without the consent of the person. These articles list the cases when the data can be collected, if the person has the right to forbid this or would have access to this information.	*Articles 13 and 14 of the Data Protection Regulation may be derogated from, if this is necessary for national security, defense or public order and security, for preventing or investigating offences, or for a supervisory task relating to taxation or public finances.*
Restrictions of the right of the data subject	Article 15, Right of access by the data subject: *1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data…* Article 23 lists the restrictions of the right of the data subject comprehensively.	The data subject does not have the right of access to data which have been collected concerning him or her, referred to in Article 15 of the Data Protection Regulation, if it is a matter of national security, if the data would seriously endanger the health of someone or if the refusal would hinder supervisory and inspection tasks in an important economic or financial interest of Finland or the European Union.
Definition of the supervisor roles and the means	Article 40 Codes of conduct encourages the member states to draw up of codes of conduct intended to contribute to the proper application of GDPR. Article 41 urges to form a supervisory authority. Chapter VI	Chapter 3, section 8: *In Finland, the national supervisory authority referred to in the Data Protection Regulation is the Data Protection Ombudsman, who works under the auspices of the Ministry of Justice.*

	handles the formation of a supervisory board of EU, its competences, and functions.	The act also defines the competences and roles the Data Protection Ombudsman has.

Table 2: Comparison of the national act and GDPR. (European Parliament, Council of the European Union, 2016) (Ministry of Justice, Finland, 2018)

APPENDIX 2

Questions used in company interviews are as follows:

1) Yrityksen henkilöstön määrä ja arvio asiakasmäärästä.
2) Onko yrityksellä yksityisasiakkaita?
3) Onko yrityksellä verkkokauppaa?
4) Toimiiko yritys paikallisesti yhdellä seudulla, koko suomen alueella vai myös kansainvälisesti?
5) Miten hankit tietoa GDPR:stä?
6) Oletko tutustunut myös tietosuojalakiin?
7) Mitä muutoksia yrityksen toimintaan tai toimintatapoihin tehtiin ennen GDPR:n voimaantuloa?
8) Miten GDPR näkyy yrityksen toiminnassa?
9) Mikä on tietoturvan merkitys sinulle henkilökohtaisesti tai työssäsi?
10) Käytätkö sosiaalista mediaa?
11) Ovatko yrityksen asiakkaat ottaneet yhteyttä GDPR:än liittyen? Jos on, mitä asia on koskenut?
12) Onko yrityksellä tullut vastaan ongelmia GDPR:än liittyen? Jos on, minkälaisia? Miten ne on korjattu?
13) Onko yrityksellä selkeät ohjeet siitä, miten tietoturvaongelmat hoidetaan?
14) Onko yrityksellä nimetty tietosuojavastaava?
15) Onko yritys laatinut tietosuojaselosteen tai tehnyt tietotilinpäätöksen?
16) Mitä tekisit nyt toisin?
17) Mitä muuta haluaisit kertoa aiheeseen liittyen?

APPENDIX 3

Questions used in public organization interviews are as follows:

Miten hankit tietoa GDPR:stä?

Oletko tutustunut myös tietosuojalakiin?

Mitä muutoksia toimintaan tai toimintatapoihin tehtiin ennen GDPR:n voimaantuloa?

Onko tämän jälkeen pitänyt tehdä lisää muutoksia? Olivatko kaikki muutokset tarpeellisia?

Miten GDPR näkyy toiminnassa? Vaikuttaako se esimerkiksi päivittäiseen työskentelyyn?

Onko henkilökunnalle järjestetty koulutusta tietosuojaan liittyen? Jos on, kuka on toiminut kouluttajana (onko palvelu ostettu ulkopuoliselta toimijalta, onko sisäinen koulutus jne)?

Ovatko asiakkaat ottaneet yhteyttä GDPR:än liittyen? Jos on, mitä asia on koskenut?

Onko vastaan tullut ongelmia GDPR:än liittyen? Jos on, minkälaisia? Miten ne on korjattu?

Onko yhteisöllä selkeät ohjeet siitä, miten tietoturvaongelmat hoidetaan?

Onko yhteisöllä nimetty tietosuojavastaava?

Onko yhteisö laatinut tietosuojaselosteen tai tehnyt tietotilinpäätöksen?

Mitä yhteisön pitäisi tehdä nyt toisin?

Mikä on tietoturvan merkitys sinulle henkilökohtaisesti?

Miten tietoturva näkyy juuri sinun päivittäisessä työssäsi?

Käytätkö sosiaalista mediaa joko itse tai yhteisön viestinnässä? Mitä kanavia käytät?

Mitä muuta haluaisit kertoa aiheeseen liittyen?