General Data Protection Regulation Compliance in the Finnish Medical Association

Johanna Bremer

2021 Laurea

Laurea University of Applied Sciences

General Data Protection Regulation Compliance in the Finnish Medical Association

Johanna Bremer
Safety, Security & Risk Management
Thesis
June, 2021

Laurea University of Applied Sciences **Abstract**

Safety, Security & Risk Management

Bachelor of Business Administration

Johanna Bremer

General Data Protection Regulation Compliance in the Finnish Medical Association

Year 2021 Number of pages 25

The purpose of this thesis is to investigate does the Finnish Medical Association reach the requirements to be GDPR compliant. In the end this thesis reaches the changes that were made when GDPR came into force in 2018 and accuracy of these changes. Training process of the staff is also investigated. This thesis was done in cooperation with the Finnish Medical Association.

For scientific approach and research methods this thesis used literature review and an open interview. The interview was done with the Administrative Director, Jaana Heinonen, of the Finnish Medical Association.

The results of the research show that there is a need for improvement of the GDPR training in the organization. The purpose of the GDPR training is to ensure the knowledge base of the staff in the future and this way to ensure the compliance of GDPR in the Finnish Medical Association.

Keywords: General Data Protection Regulation, compliance, knowledge base

Laurea-ammattikorkeakoulu **Tiivistelmä**

Safety, Security & Risk Management

Bachelor of Business Administration

Johanna Bremer

GDPR:n noudattaminen Suomen Lääkäriliitossa

Vuosi 2021 Sivumäärä 25

Tämän opinnäytetyön tarkoituksena on tutkia, että kattaako Suomen Lääkäriliitto GDPR:n (yleinen tietosuoja-asetus) vaatimukset. Loppujen lopuksi tämä opinnäytetyö tutkii muutoksia, joita tehtiin Suomen Lääkäriliitossa silloin, kun GDPR tuli voimaan vuonna 2018. Samalla tutkitaan, että onko nämä muutokset tehty oikein. Työntekijöiden GDPR koulutusta tutkitaan myös. Tämä opinnäytetyö tehtiin yhteistyössä Suomen Lääkäriliiton kanssa.

Tässä opinnäytetyössä tutkimuksellisena lähestymistapana käytettiin kahta eri tiedonkeräysmetodia, jotka olivat kirjallisuuskatsaus sekä avoin haastattelu. Haastattelu tehtiin Suomen Lääkäriliiton hallintojohtaja Jaana Heinosen kanssa.

Tutkimuksen tulokset kertovat, että organisaatiossa on tarve parantaa GDPR-koulutusta. Koulutuksen tarkoituksena on varmistaa henkilöstön tietotaidon pysyvyys tulevaisuudessa, näin voidaan myös varmistaa, että GDPR:n noudattaminen tulevaisuudessa.

Contents

List of abbreviations

GDPR - General Data Protection Regulation
DPO - Data Protection Officer
EU - European Union
EDPD - European Data Protection Directive
EEA - European Economic Area
FMA - the Finnish Medical Association

1 Introduction

This thesis researches the compliance of General Data Protection (GDPR) in the Finnish Medical Association (FMA). The purpose of GDPR is to control processing of personal data and it's valid only in the European Union (EU) and in the European Economic Area (EAA). GDPR came into force in May 25th, 2018 and that's when FMA made some changes in their operations regarding GDPR. The objective of this thesis is to check the compliance and validity of these changes in the FMA. The results of this thesis are based on literature reviews, Interview with the Finnish Medical Association and other observations made by checking the documents and training material the FMA has. This thesis is written in cooperation with the FMA. The research objective for this thesis is to research how GDPR changes were made in FMA a few years ago and to verify the compliance of GDPR in the FMA. (Office of the data protection ombudsman, 2021)

1.1 Finnish Medical Association

This thesis was written in cooperation with the Finnish Medical Association. The FMA is a professional association for doctors practising in Finland, it was founded in 1910. The association takes part in developing the health care system in Finland. (The Finnish Medical Association, 2021)

The FMA has an office located in Helsinki, Finland. The decisions are made by the delegation and the board of the association. The subdivisions of the association bring together doctors by specialization. In addition, they have diverse regional activities. The FMA also provides training for doctors in a few days lasting big training event held in Expo and Convention Centre in Helsinki once a year, in the year of 2021 the training was held remote due to COVID-19 pandemic. (The Finnish Medical Association, 2021)

1.2 Research questions

This study focuses on two areas. First category is the present, to make sure that FMA reaches the requirements of GDPR. To understand how the current level is reached we need to research the history at first, meaning what measures were taken when GDPR came into force. The second category is the future, ensuring the correct level of GDPR in the Finnish Medical Association in the future.

The research questions for this thesis are:

"Is the FMA compliant with the requirements of the GDPR" also,

"How to ensure the GDPR knowledge base of the staff in the future?".

The above-mentioned categories will then answer the research questions.

2 General Data Protection Regulation

In this chapter GDPR is introduced thorough background and obligations of organizations. It is important to start with the background of GDPR to understand the reasons behind why GDPR was created. In addition, it is important to understand why GDPR is valid before understanding how GDPR works.

GDPR is also introduced by looking into the obligations of organizations which is relevant for this thesis to be able to check the compliance of GDPR in the FMA. Since GDPR was created to improve and to guard the protection of personal data it is important to know what is considered as personal data. Personal data is also described in this chapter. Obligations of organizations are explained in figure 2. The privacy statement of the FMA is also investigated at the end of this chapter.

2.1 Background

In 1995, a directive came into force called European Data Protection Directive (EDPD) which was created with the knowledge and technological situation at that time. In the next two decades a huge leap in technology happened where the EDPD couldn't keep up anymore. EDPD didn't meet the current data protection requirements, it only covered the minimum data privacy and security standards. In 2011 the change towards new GDPR took it's first step. European Parliament passed the GDPR in 2016 and after that GDPR came into force officially. From this day on the two-year transition period began and from May 25th, 2018 each organization in the EU an EAA area were required to be GDPR compliant. (Wolford, 2021)

The goals of GDPR are to improve the protection of personal data and data protection rights. In addition to respond to new data protection issues related to digitalization and globalization and to contribute to the development of digital single marketing. The GDPR changed the way that companies, organizations and authorities process personal data. How is GDPR different from the old Personal Data Act? GDPR could be considered as reinforced personal data law; as the Personal Data Act focuses more on how information is processed, the GDPR focuses more on how and why the information is collected. (Office of the data protection ombudsman, 2021)

2.2 Obligations of organizations

What is considered as personal information? Personal information is divided into three groups:

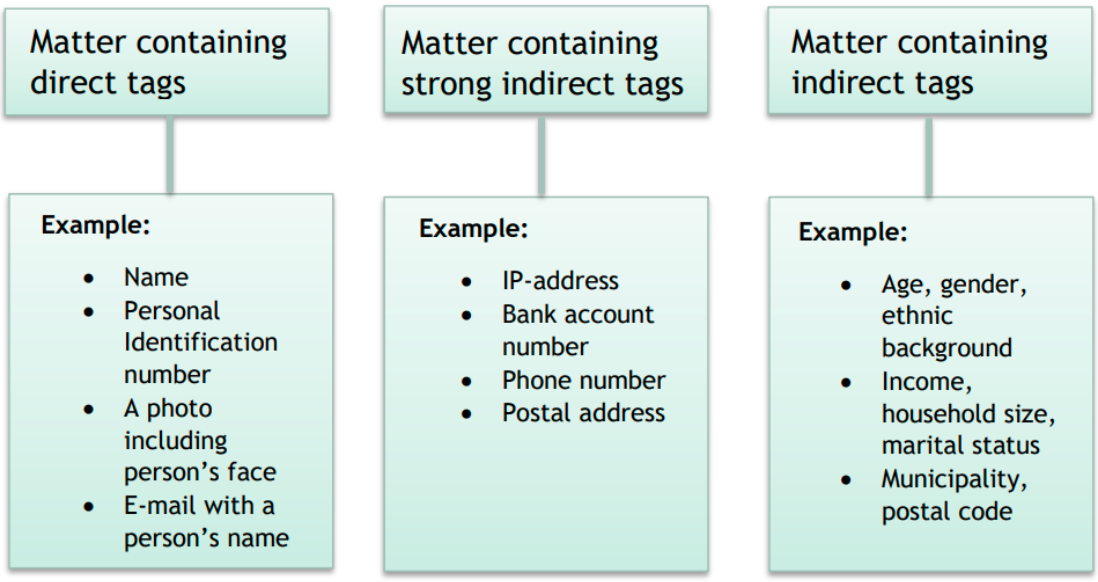

Figure 1 Personal information defined (HAMK, 2021)

According to GDPR companies and organizations should know the answers to the following: (koulutus.fi, 2021)

1. Why they have certain user-, personal- or other information?
2. Is the information relevant for the company?
3. What is the origin of the information?
4. Who has access on the data?

It is important to be able to answer the questions above especially in case the companies or organizations have websites with the possibility to register as a client or a member. It is important also in case the company or organisation has an e-mail register for carrying out customer mailings. (koulutus.fi, 2021)

The GDPR is a law, meaning in case companies and organizations are not following the law there is a fine. In case the law is not followed it can lead to significant fines. Fine can be even 20 million euros or a 4% of a company's turnover. Just by Googling "GDPR fine cases" many examples show up with big fines. In addition, the Data Protection Authority may determine other measure, which could mean that the company or organisation must stop the processing of personal data. (Office of the data protection ombudsman, 2021)

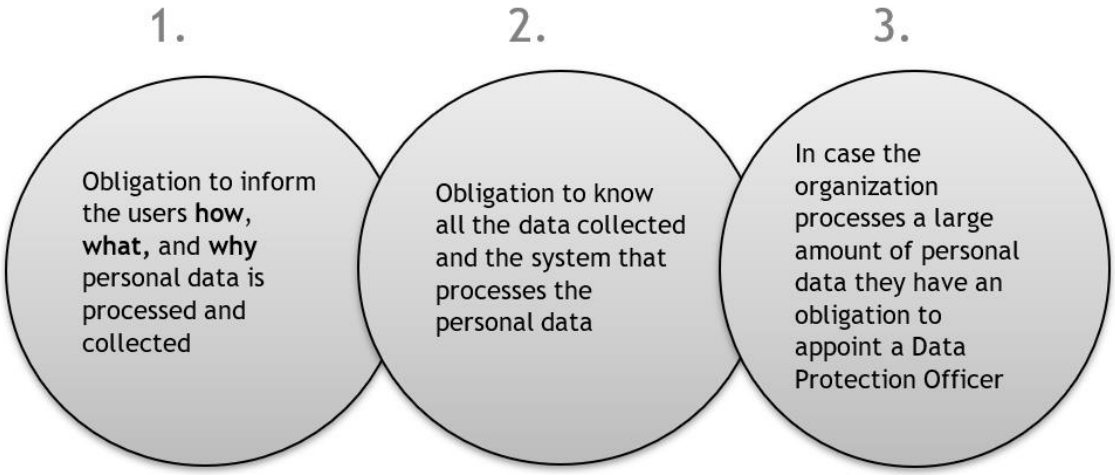

Figure 2 Obligations of companies and other organizations (Koulutus.fi, 2021)

In the FMA webpage a people can find a Privacy Statement where the how, what and why personal data is processed and collected. It says that FMA uses personal data for the maintenance and administration of the membership of the FMA and collection of membership fees for example. Each and every purpose for the use of personal data is explained clearly and thoroughly. User can find answers for the how, what and why personal information is processed and collected from the Privacy Statement. Personal data is gathered mostly from the member itself, but some information comes from other resources. Each resource is explained in the Privacy Statement. In addition, FMA has an appointed Data Protection Officer. (The Finnish Medical Association, 2021)

3 Research process

Research for this thesis started at the end of 2020. The purpose of the research was to gain knowledge on the subject and to gather enough research results to get valid results. The research process began with planning of the thesis. The next step was to gain a knowledge base of the subject. Creating a knowledge base included studying GDPR and investigating any possible case studies. Following the next step, open interview with the FMA, which expanded the created knowledge base and gave a good and realistic picture of GDPR in the FMA. The last steps, analysis and reporting, gave answers to the research questions. The research process is visualized in figure 1.

Figure 3 The research process

3.1 Literature review

A literature review is a research made from multiple reliable sources about the same subject. Literature review gives an overall picture on the existing written knowledge of the subject, which allows the researcher to identify theories and methods relevant to the study. When writing a literature review information must be researched from relevant sources. Information can be researched from printed sources such as books and from different electronic sources. Due to the COVID-19 pandemic this thesis uses only electronical sources. The purpose of literature review isn't only to summarize the information found from the sources, but to critically analyse, explain and evaluate the findings. (McCombes, 2019)

The purpose of this literature review is to investigate in case similar research has been done before and then study the possible research results found. In case similarities are found, the new study can be validated with the found data. In addition, the purpose is to gain a good level of understanding of the topic by researching the already existing material. In this thesis literature review was used as a knowledge base for the research topic.

When starting the literature review the first thing was to decide where to start the research. As said earlier due to COVID-19 pandemic decision was made to use electronical sources only. Thanks to internet information is found easily and widely. The internet also has a downside to it, the researcher must be critical on the source of information ja know which source is reliable and which is not. Therefore, when the information is similar from different sources the information can be found reliable. This literature review started with looking for similar theses from the internet. The exact same study hasn't been done before, where the compliance of GDPR changes made to an organization, has been studied after changes has been done. Therefore, literature review acts as a base of general knowledge in this thesis. After searching for the theses, I started to study what is GDPR. A lot of information was found and some of the information found wasn't relevant for this study, therefore I decided to focus more on the background of GDPR and the obligations of organizations regarding GDPR. The sources for creating the knowledge base where Theseus (for previous studies, no similarities found), the Office of the data protection ombudsman, the FMA's webpages, some articles

that provided reliable information and a few webpages that had information relevant for this study.

In addition, I conducted a research on GDPR fines. The purpose was to research how often do GDPR violations happen. According to a list of GDPR fines there has been more that 1500 recorded GDPR violations in the year of 2021. The list is kept as up to date as possible, but not all violations are made public therefore it doesn't give a full picture. There has been one recorded violation in Finland by June 2nd, 2021 and in the year of 2020, there has been 5 recorded violations. When considering the amount of organizations Finland has and compare that to the amount on recorded violations it is safe to say that GDPR violations don't happen often. But the impact of these violations can be financially remarkable, the biggest fine in Finland was in 2020 to Posti Group Oyj, the amount of the fine was 100 000 euros and the reason for that fine was insufficient fulfilment of data subjects' rights. (GDPR Enforcement Tracker - list of GDPR fines, 2021)

3.2 Interview

Interview is a conversation between two, or many people and the purpose is to gather information. Interview consists of interviewer, who leads the interview with questions and an interviewee of interviewees to respond the questions presented by the interviewer. Interview can be done face-to-face, via telephone or some other communication tool, such as Microsoft Teams. There are three types of interviews: structured interview, semi-structures interview and unstructured interview. In structured interview the interviewer asks a number of standard questions that are decided before the interview. The questions are about certain topics and are presented in a certain order. The interviewee or interviewees must select answers from a list of pre-determined answer options. In semi-structured interview the interviewer asks a number of predetermined questions from the interviewee or interviewees. The questions are answers are given openly in the respondents' own words. The interviewee can give more questions during the interview if needed. In an unstructured interview there are no specific rules or questions that are decided before the interview. The interviewer asks some questions from the interviewee or interviewees to get an open and informal conversation. (Easwaramoorthy and Zarinpoush, 2006)

Close to the end of my research, a semi-structured interview was conducted with the Administrative Director of the Finnish Medical Association, Jaana Heinonen. Interviewee was chosen based on the knowledge she has about the GDPR compliance of the company. The interview focused on the past-, present- and future compliance of GDPR. It was important to understand what has been done in the past, what changes were made when GDPR came into force, to get the understanding how the GDPR is at the level as it is today. And also, to know if the company has any plans for the future concerning GDPR. The results of the interview

have been translated from Finnish to English. The original interview answers can be found in Appendix 2. The interview was done via Microsoft Teams.

4 Research results

This chapter introduces the research results of literature review and interview. Literature review results were gained after a thorough research in the internet. Due to Corona I didn't visit any libraries during research, instead I researched many different sources on the internet. Sources were in example, articles, theses and Data Protection Act.

Interview results were gained after the semi-structured interview. The interview included many different questions with opportunity to answer them openly. Open interview formed the possibility for a more open conversation and made the interviewee more relaxed. After analysing the interview answers with the literature review results a good understanding of the compliance of GDPR in the FMA was created. Literature review- and interview results are explained in the following chapters 4.1 and 4.2.

4.1 Literature review results

Literature review started with creating a knowledge base on the subject. Starting of literature review needed some planning since internet is full on different sources and information. It was important to decide how extensively the matter would be investigated. The main focus was to understand what is GDPR, the reasons behind creation of GDPR and how does it affect organisations.

Knowledge base gained is explained more thoroughly in the chapter 2, where the GDPR is introduced. After my thorough research about GDPR I gained a good level of knowledge and understanding about history of GDPR, the reasons behind GDPR and obligations of organizations regarding GDPR.

During the literature review previous studies about the compliance of GDPR in organizations were researched, but without success. Most studies were about what companies must do when GDPR comes into force, there were no studies about the compliance after GDPR came into force. In other words, there are no studies examining whether a company complies with the GDPR after it came into force. There are a lot of similarities in some the studies found but they are still no the same. In literature review only electronic sources were used due to COVID-19 pandemic.

When starting the literature review the first thing was to decide where to start the research. As said earlier due to COVID-19 pandemic decision was made to use electronical sources only.

A part of the literature review was to collect information from various reliable sources. In addition, the statistics of GDPR violations was researched which led to a conclusion that violations don't happen often, but the severity of the violations can be financially remarkable. After the thorough literature review, I gained a strong scientific basis for my entire research.

4.2 Interview results

According to Jaana Heinonen the FMA had a massive check-up made by Eija Varma who is a data protection lawyer from Castrén & Snellman, which is a firm of solicitors, when GDPR came into force. Varma went through the whole GDPR process, what needs to be done and what kind of guidance needs to be done. In addition, Varma went through different documents that the FMA had, gave some instructions and with her help the Finnish Medical Associations was ready for GDPR. Heinonen also mentioned that before the GDPR came into force a lot of marketing calls were received where very expensive services were traded, a lot of intimidation around GDPR. Based on Varma's profession she was a reliable consult to ensure the validity of the GDPR transition of FMA.

Heinonen also stated that GDPR did not bring a massive change on the FMA, just documentation process and general focus. The Finnish Medical Association had something to be improved but mostly with documentation. To FMA the GDPR didn't bring a massive change because they don't have an online store, they don't profile any customers and they don't do international trade. Heinonen believes that employees know well what information is classified and how that information is handled.

According to Heinonen she doesn't have any bigger concerns regarding GDPR -safety of the FMA. Only problem is the deletion of unnecessary files. There should be a practice so that the unnecessary files would be deleted regularly. In addition, the GDPR induction video should be watched more than once, when starting the position. Heinonen states that there hasn't been any GDPR violations in the past. They have created a process in case a violation occurs, where and how to report the violation. The have had a small situation where a wrong message was sent to a wrong recipient by accident, it wasn't a serious case and the content in the message wasn't serious, but they checked the process again.

Heinonen thinks that the staff needs more training regarding GDPR, just to make it regular so that the staff doesn't forget GDPR rules. It should be brought up every 1,5 years because for some it's more familiar than others who maybe don't have to think about GDPR in their work as much. As a bonus someone could come up with better modes of operation and this could lead to change of processes and updating. All in all, Heinonen has a safe feeling about the compliance of GDPR in the Finnish Medical Association.

At the end of the interview Heinonen presented a request that I would create a process of GDPR training that would happen regularly. It is important to keep the employee's knowledge active.

The results of the interview show that the changes that were made were executed by a reliable source. The staff is aware on how to handle personal data and what information to share and not share. The staff completes a short GDPR -training video at the beginning of employment, but there is no follow-up training after that. It is important to keep the level of information active after induction.

5 GDPR compliancy in the future

How to ensure the GDPR compliancy in the future? New employees get a small GDPR training at the beginning of employment but there isn't any training following that. Therefore, the information the employee gains within the first weeks of employment regarding GDPR, doesn't get any verification or memory refreshment later. To ensure that the FMA is GDPR compliant in the future it is important to make sure that the staff has a strong knowledge base about GDPR. Good knowledge base can be reached with training, in addition someone might come up with better ways, new and improved processes that can be added in the training. In addition, the GDPR training could be used as a reminder for each employee to delete every unnecessary file as Heinonen mentioned this as an issue. Employees have a habit on saving unnecessary files and not deleting them from their computer or intranet folders.

5.1 Current training

The present training in the FMA is a part of induction when a new employee executes a small training session online with some text and questions about GDPR. The training includes a short presentation about GDPR. Introduction about what is personal data, which is important for the employees of FMA to know. We handle personal information basically every day. In addition, the disclosure of personal data is explained very well, to who you can't share personal and how. The training consists of written explanation and training with quick questionnaires in between subjects and in the end, there is game with randomly assorted questions with multiple choices.

The online training is executed very vell because it consists of written facts, questions in between to help the brain to absorb the information gained and the end game to test knowledge received.

5.2 Training in the future

When starting a new position there is a lot of induction and everything is new, and it is most likely hard to connect all the induction for own work tasks therefore it is important to repeat the training again later. People learn differently, usually through sight, hearing, movement, or touch. Studies show that repetition of learnt material is one of the keys in learning. (Oppiminen ja opiskelutekniikat, 2021)

The already existing training material could be used as the repetition training, but it needs to be done regularly. According to Heinonen employees carry out the training only at the beginning of the employment relationship. FMA has a designated data protection officer who could be the responsible one to make sure the training happens regularly. A training link could be sent via e-mail once a year, in the spring. In the same e-mail there could be a reminder of "spring cleaning", meaning employees need to clean all the unnecessary files from their computers, as according to Heinonen this an issue that people save unnecessary files in their computers and in their own intranet folders.

6 Conclusions

The purpose of this thesis was to research the compliance of GDPR in the FMA. The project started with planning of thesis and a literature review which provided a good knowledge base on the subject. Without a good knowledge base on the subject the thesis couldn't be valid. After the research process an interview was conducted with Jaana Heinonen from the FMA. The interview results showed that the GDPR changes to the company have been made under the guidance of a trusted party. Based on the results of this study the FMA meets the GDPR compliance but there is a need for GDPR training to ensure the continuity of knowledge base of the staff.

6.1 Answering the research questions

The first question was: is the FMA compliant with the requirements of the GDPR? After creating a knowledge base by literature review on the subject, a strong scientific basis for the entire research was gained. FMA uses personal information from all the three categories: direct tags, strong indirect tags and indirect tags. The Privacy Statement explains clearly how, what and why personal data is processed and collected in the FMA. It answers the questions why FMA has certain user-, personal – or other information, which is mostly for the maintenance and administration of the membership of the FMA and collection of membership fees. Personal data is relevant for the FMA for the membership register and the possibility to keep up different statistics. Without personal data the FMA couldn't run their daily work. Personal data is gathered mostly from the member itself, but some information comes from

other resources. FMA has an appointed Data Protection Officer (DPO), as it is required when a company or an organisation processes large amounts of personal data.

During the semi-structured interview with the FMA it was clear that GDPR changes were made under the guidance and supervision of a trustworthy party. Each document and instructions were made by a data protection lawyer. The staff was trained by the guidance of the same thrusted party. After the interview it was clear that GDPR situation was in a good level in the FMA, there hasn't been any prior GDPR violations and Heinonen doesn't have any concerns regarding the compliance of GDPR in the FMA. The staff is aware how to process personal data, and they have the knowledge to search for information from the intranet where a lot of information about GDPR can be found, all the information and guidance are created by data protection officer. In addition, the DPO helps with any concerns regarding GDPR.

After looking at many aspects and researching how a company is GDPR compliant, this research study shows that the FMA meets the requirements to be GDPR compliant. There isn't anything alarming in the processing of personal data and also, the FMA fulfils the obligations of companies and other organizations described in figure 3.

Second question was: how to ensure the knowledge base of the staff in the future? As it came up in the semi-structured interview a clear need for GDPR training is needed to keep up the knowledge base of the staff in the future. The level of knowledge must be maintained, and the training could be used as a reminder to clear the staff's computers and intranet folders from any unnecessary files. The current training could be used, or a new form of training could be developed. But in example the DPO, should be the responsible to lead these trainings and make sure the trainings happen regularly.

6.2 The validity of this thesis

This thesis used a two very effective and appropriate research methods for this thesis such as the literature review and interview. In addition, the GDPR files were examined during the literature review. These research methods created a mass of information which was analysed and processed. Each information can be traced from this thesis and each step of the research are described clearly in this thesis to help the reader to understand background this research and the reasons behind the conclusions. This research is valid and can be seen as a success. Literature review created a solid knowledge base combined with the whole research which then led to the possibility to answer the research questions presented at the beginning of this thesis.

This thesis was conducted in cooperation of the FMA to check the compliance of GDPR in the FMA. To conclude validity of this research, this research shows that FMA is compliant with GDPR. This research can be used in the future as a base for projects similar to this study.

References

Electronic

Wolford, B., 2021. What is GDPR, the EU's new data protection law? Accessed 3.3.2021. https://gdpr.eu/what-is-gdpr/

Office of the data protection ombudsman. Tietosuojavaltuutetun toimisto, 2021. EU:n tietosuoja-asetus - usein kysyttyjä kysymyksiä - Tietosuojavaltuutetun toimisto. Accessed 3.3.2021.
https://tietosuoja.fi/gdpr

koulutus.fi, 2021. Uusi tietosuoja-asetus – mikä, miksi ja miten? Accessed 4.3.2021.
https://www.koulutus.fi/oppaat/uusi-tietosuoja-asetus-12611

HAMK, 2021. Mitä ovat henkilötiedot ja erityiset (arkaluonteiset) henkilötiedot? - Digipedaohjeet. Accessed 4.3.2021
https://digipedaohjeet.hamk.fi/ohje/mita-ovat-henkilotiedot-ja-erityiset-arkaluonteiset-henkilotiedot/

Peda.net, 2021. Oppiminen ja opiskelutekniikat. Accessed 30.4.2021.
https://peda.net/kankaanp%C3%A4%C3%A4/ky/opinto-ohjaus/ojo

Finland. Data Protection Act 1050/2018, 2018. Accessed 30.4.2021.
https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf

Rossow, A., 2021. The Birth Of GDPR: What Is It And What You Need To Know. Accessed 29.4.2021
https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=37c1ecfe55e5

The Finnish Medical Association. laakariliitto.fi, 2021. Tietosuojaseloste. Accessed 5.5.2021.
https://www.laakariliitto.fi/tietosuojaseloste/

The Finnish Medical Association. laakariliitto.fi, 2021. Accessed 8.5.2021.
https://www.laakariliitto.fi/en/

The Finnish Medical Association. laakariliitto.fi, 2021. Association. Accessed 8.5.2021
https://www.laakariliitto.fi/en/association/

McCombes, S., 2019. The Literature Review | A Complete Step-by-Step Guide. Scribbr. Accessed 2.6.2021
https://www.scribbr.com/dissertation/literature-review/

Easwaramoorthy, M. and Zarinpoush, F., 2006. Interviewing for research. Sectorsource.ca. Accessed 2.6.2021
http://sectorsource.ca/sites/default/files/resources/files/tipsheet6_interviewing_for_research_en_0.pdf

Unpublished

Jaana Heinonen. The Finnish Medical Association. 2021. Open interview. 7.4.2021. Bremer, J.

Figures

Appendices

Appendix 1: Interview results in Finnish

Mitä muutoksia Lääkäriliitossa tehtiin silloin kun GDPR astui voimaan?

Jaana Heinonen: Silloin tehtiin iso tarkistus. Meillä oli Eija Varma (tietosuojajuristi) Castrén & Snellmanila ja hänen johdollaan käytiin läpi koko GDPR prosessi, eli mitä kaikkea pitää tehdä ja mitä kaikkea ohjeistusta pitää tehdä. Eija kävi myös läpi meidän dokumenttejamme, antoi ohjeita ja hänen avustuksellaan saatettiin Lääkäriliiton GDPR valmiuteen. Ennen kuin GDPR tuli voimaan tuli paljon markkinointi puheita missä kaupattiin kalliita palveluita ja sanottiin, että kaikki menee aivan uusiksi. Eihän se sitä olemassa olevaa tilannetta muuttanut sisällöllisesti paljoa, ainoa oli vain tämä dokumentaatioprosessi ja yleinen skarppaaminen. Tuntui, että silloin oli pelottelevaa viestintää. Ihan selkeä markkinarako. Oli Lääkäriliitolla jonkun verran skarpattavaa, mutta lähinnä siinä dokumentoinnissa. Lääkäriliiton kaltaiselle organisaatiolle, kun meillä ei ole verkkokauppaa, me emme profiloi asiakkaita, ei tehdä kansainvälistä kauppaa, tämä ei ollut iso muutos. Kyseessä on kuitenkin järjestö, meillä on jäsenet ja me ymmärretään hyvin mikä tieto on salassa pidettävää ja miten niitä käsitellään. Ei isoa muutosta.

Onko sinulla nyt tai onko aikaisemmin ollut jotain huolia liittyen Lääkäriliiton GDPR-turvallisuuteen?

Jaana Heinonen: Ei ole varsinaisia huolia. Huomattiin aikaisemmin se, että hyvin käsitellään tietoja ja tiedetään mitä tietoja saa luovuttaa. Ainoa ongelma on turhien tietojen tallettaminen Torille (intra). Pitäisi ottaa turhien tietojen poistaminen käytäntöön, kun jokin tiedosto ei ole enää tarpeellinen niin sen voisi poistaa. Toisin sanoen pitäisi muuttaa toimintatapaa, jotta turhat tiedostot tulisi poistettua säännöllisesti. GDPR -perehdytysvideo katsotaan yleensä vain kerran työsuhteen alussa, olisi hyvä katsoa myöhemmin uudelleen.

Onko Lääkäriliitossa tapahtunut jotain rikkeitä aikaisemmin?

Jaana Heinonen: Ei ole tapahtunut. On luotu prosessi, että mihin tietoturvapoikkeamat ilmoitetaan. Yksi ainoa pieni viesti joskus lähetetty väärään paikkaan, viesti ei kyllä sisällöltään ollut vaarallinen, mutta silti prosessi tarkistettiin uudelleen. Ei ole tapahtunut mitään tietoturvaloukkauksia.

Oletko sitä mieltä, että henkilökunta tietää riittävästi GDPR:stä, vai tarvitaanko lisää koulutusta?

Jaana Heinonen: Lisää perehdytystä tarvitaan. Toivoisin, että koulutuksesta tulisi joku systemaattinen n. 1,5 vuoden välein tapahtuva koulutus. Asia pitäisi nostaa säännöllisesti esiin. Joillekin se on tutumpaa ja toisille vieraampaa. Toisten työhön GDPR liittyy päivittäin

ja toisten työhön harvemmin. Joku voi myös keksiä uusia ja parempia toimintatapoja ja näin prosesseja voisi muuttaa ja päivittää.

Mikä on sinun arviosi Lääkäriliiton kokonaisvaltaisesta GDPR-turvallisuuden tilanteesta tällä hetkellä?

Jaana Heinonen: Mielestäni tilanne on tällä hetkellä hyvä. Minulla on turvallinen olo.

Onko sinulla jotain tiettyä osa-aluetta, jota haluaisit minun tutkivan?

Jaana Heinonen: GDPR koulutuksen kehittäminen, sen säännöllistäminen. Henkilöstön tietoisuuden ylläpitäminen, prosessien luominen.