Linnea Nyberg

The Economic Value of Data and the General Data Protection Regulation

School of Accounting and
Finance
Master's thesis in Business Law
Master's Programme in
Business Law

Vaasa 2022

UNIVERSITY OF VAASA
School of Accounting and Finance
Author: Linnea Nyberg
Title of the Thesis: The Economic Value of Data and the General Data Protection Regulation
Degree: Kauppatieteiden maisteri
Programme: Business Law
Supervisor: Shakila Bu-Pasha
Year: 2022 **Pages:** 77

ABSTRACT:

The aim of this thesis is to find out how the economic value of data affects the need for regulation of personal data and how the businesses need to address this in their operations. This is done through EU data protection law, the General Data Protection Regulation (GDPR). The GDPR is as the name states about data protection and regulates how personal data should be handled. Data protection aims to protect individuals' personal data and how it can be used. Whereas economic value of data means that personal data is of economic value, and it is seen as something that has value to businesses and their operation.

The GDPR came into force in May 2018. Therefore, it is a fairly new legislation. The GDPR applies to a large number of individuals since it is applied to not only the citizens of the European Union but also to those companies that have customers that are citizens of EU. This adds to the diversity as well as the global aspect of the subject.

The main research question is whether or not the economic value of data is the aspect that makes the main difference between privacy and data protection. The economic value of data is inspected through the businesses side of view. Research is also done through comparing the concepts of privacy and personal data protection.

The thesis is done as a literature review meaning that it should be seen as a collection of relevant sources of the topic and the combination of them in a way that the sources are viewed in a critical manner. Since the GDPR is a fairly new legislation, there is a variety of sources available. The sources used in the thesis are in addition to the written ones, different kinds of articles, websites, and legal sources. The most important legal source is the General Data Protection Regulation, and it is considered as the guideline throughout the thesis.

It was found through the study that the hypothesis and research question of the economic value of data does create the main difference and is the reason why such personal data protection regulation needs to be. The GDPR causes additional work for companies and the need to take into consideration data protection aspects in their everyday work. However, the GDPR also has brought benefits to companies by giving them the guidelines that they can obey in order to process personal data lawfully.

KEYWORDS: General Data Protection Regulation, Data Protection, Personal Data, Economic value of data, Privacy

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen akateeminen yksikkö
Tekijä: Linnea Nyberg
Tutkielman nimi: The Economic Value of Data and the General Data Protection Regulation
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Talousoikeus
Työn ohjaaja: Shakila Bu-Pasha
Valmistumisvuosi: 2022 Sivumäärä**:** 77

TIIVISTELMÄ:
Tutkielman tarkoituksena on selvittää, miten datan taloudellinen arvo vaikuttaa tietosuojalainsäädännön tarpeeseen ja miten yritysten tulee ottaa tämä huomioon toiminnassaan. Tämä tehdään Yleisen tietosuoja-asetuksen kautta. Tietosuoja pyrkii suojelemaan yksilöiden henkilötietoja ja sitä, miten näitä henkilötietoja voidaan kautta. Datan taloudellinen arvo puolestaan tarkoittaa sitä henkilötiedoilla voidaan nähdä olevan taloudellista arvoa ja niiden voidaan nähdä olevan hyödyllisiä yrityksille ja heidän toiminnalleen.

Tutkimuskysymyksenä tutkielmassa on se, onko taloudellinen arvo suurin ero yksityisyyden käsitteiden ja tietosuojan välillä. Datan taloudellista arvoa tarkastellaan yritysten näkökulmasta. Tutkielmassa käytetään myös vertailua yksityisyyden käsitteiden ja tietosuojan välillä.

Yleinen tietosuoja-asetus (GDPR) tuli sovellettavaksi toukokuussa 2018. Näin ollen se on suhteellisen tuore asetus. Aiheen monipuolisuuden puolesta puhuu se, että GDPR koskettaa laajaa ryhmää yksilöitä, sillä sitä sovelletaan kaikkiin Euroopan Unionin kansalaisiin, sekä myös kaikkiin niihin yrityksiin, jotka tekevät yritystoimintaa Euroopan Unionin sisällä ja sen kansalaisten kanssa.

Tutkielma toteutetaan kirjallisuuskatsauksena, tarkoittaen että se tulisi nähdä kokoelmana aiheeseen liittyviä relevantteja lähteitä ja niiden yhdistelmää siten, että lähteitä tarkastellaan kriittisesti suhteessa toisiinsa. Koska kyseessä on suhteellisen tuore asetus, löytyy siitä monipuolisesti lähteitä. Lähteinä tutkielmassa on käytetty kirjallisten lähteiden lisäksi myös erilaisia artikkeleita, nettisivuja sekä virallislähteitä. Virallislähteistä tärkein on ymmärrettävästi Yleinen tietosuoja-asetus, joka toimii punaisena lankana läpi tutkielman.

Tutkielman lopputuloksena voidaan todeta se, että tutkimuskysymys ja siinä esitetty hypoteesi datan taloudellisesta arvosta luo suurimman eroavaisuuden yksityisyyden käsitteen ja tietosuojan välillä. Voidaan todeta sen olevan myös se syy, miksi kyseiselle tietosuojalainsäädännölle on tarve. GDPR aiheuttaa ylimääräistä työtä yrityksille sen kautta, että yritysten tulee huomioida tietosuojaan liittyvät aspektit jokapäiväisessä elämässään. Siitä on kuitenkin myös hyötyä yrityksille, sillä se luo ne raamit, joiden mukaan yritysten tulee toimia käsitellessään henkilötietoja.

ASIASANAT: Yleinen tietosuoja-asetus, Tietosuoja, Yksityisyys, Henkilötieto, Datan taloudellinen arvo

Contents

ABBREVIATIONS

the Charter	The Charter of Fundamental Rights of the European Union
EU	The European Union
FISMA	The Federal Information Security Management Act
GDPR	General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act
ICCPR	International Covenant on Civil and Political Rights
PIPL	Personal Information Protection Law
UDHR	Universal Declaration of Human Rights
UN	The United Nations

1 Introduction

1.1 Purpose, hypotheses, and motivation

Personal data is every data that can be related to either an identified or identifiable individual. These include data such as a telephone number, IP address and patient record. [1] Personal data is a vast concept, and it is a part of every individual's everyday life. No matter how anonymous one would desire to be, there is still always some personal data of an individual online. Therefore, it is very important for the legislation of personal data to be up to date. Regulation (EU) 2016/679 of the European Parliament and of the Council, the European union's new General Data Protection Regulation (GDPR) was legislated to serve this exact purpose.

Nowadays it is nearly impossible to not use the internet since our society is so vastly based on the usage of it and nearly everything happens online. More than half of the world's population use the internet every day. [2] When using the internet, you leave marks of yourself and your usage, many times unintentionally. Around 2,5 quintillion bytes of data is generated by the users of the internet daily. [3] This data that is collected on the internet has become a mean of business for many companies and the economic value of data is much bigger than many people come to think of.

Even if you do not use the internet yourself, there is a lot of personal data collected online in different databases. Therefore, it is important that the legislation is up to date and protects individuals so that their personal data is not used without their knowledge

---

[1] Office of the Data Protection Ombudsman (n.d. A). What is personal data? Retrieved March 15, 2022, from https://tietosuoja.fi/en/what-is-personal-data

[2] Hofmann, P., Kiyomoto, S., Nakamura, T., Serna, J. & Tesfay W.B. (2018) PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation Retrieved March 29, 2022, from https://www.researchgate.net/profile/Shinsaku-Kiyomoto/publication/323787516_PrivacyGuide_Towards_an_Implementation_of_the_EU_GDPR_on_Internet_Privacy_Policy_Evaluation/links/5b3ebbb3aca272078519c3fa/PrivacyGuide-Towards-an-Implementation-of-the-EU-GDPR-on-Internet-Privacy-Policy-Evaluation.pdf, p. 15

[3] Hofmann et al. (2018) p. 15

and that companies cannot financially benefit from individuals' personal data without the individual's permission. The financial benefit is not the only thing to take into consideration when talking about data regulation. If personal data is not handled correctly, it could also lead to crimes such as stolen identities and could bring great harm to individuals. The EU data protection law, General Data Protection Regulation, more well known as the GDPR, came into force in May 2018. It consists of regulation that determine the guidelines which companies and businesses need to obey if they handle personal data as a part of their business and this considers all collected personal data even if the main purpose was not to use to financially benefit from it. This binds all companies that work inside the European Union or have customers that are inside the European Union. Therefore, it is not only binding in EU but also in other areas since many companies nowadays have customers all over the world no matter what the company's country of origin is.

Main theme and idea in the thesis can be defined by a quote that reflects how in this world the economic value of data is the most important reason why such regulation needs to exist.

"If the product is free, you are the product" [4]

This quote can be seen as rather controversial and, in this thesis, it is not used to accuse companies of using individuals' information rather than it is used to implicate how individuals themselves are able and allowed to use their personal information as a mean of payment. One gets something in return of letting the company use one's personal data and either use it themselves or pass it on to a third party. This happens for example when you give a website your e-mail address in order for you to get a discount for something and in return, they are able to send you messages of topics of their choosing. It could mean that these messages come from the company themselves, but also sometimes

[4] Lynskey, O. (2016). The foundations of eu data protection law. Oxford University Press. p.3.

other companies can pay them to be able to get the e-mail addresses, personal data, to use in their own marketing and advertising.

1.1.1 Purpose

The purpose of this thesis is to examine the economic value of data and how that has affected the need for personal data protection regulation. It is also inspected how this affects companies and what they need to do in order to comply to the GDPR. Because the thesis is made from business laws point of view, it is based more on the economical side of the GDPR and how it can be viewed from the business's point of view. However, data protection can't be dealt with without taking into consideration the individual also so the thesis will combine these two.

The ways in which GDPR affects business and individuals are rather different because they are usually on different sides of the legislation. Businesses are often the ones using and collecting the data therefore they are the ones that the regulation legislates whereas the individuals are the ones who the regulation tries to protect and whose data the businesses are collecting and using. Privacy in traditional human rights law is often based more on the individuals' rights but in GDPR the businesses are mentioned more, and it is defined what is the businesses' role in protecting individuals' data. The main point of view in the study is how the economic value of data makes the main distinction between the right to personal data protection and right to privacy. The aim is to find out how big of a role the economic value of data plays and whether or not the legislation would be needed without it.

1.1.2 Motivation

The GDPR is a fairly new legislation. The motivation for this study is not about trying to find out whether or not the GDPR has been implemented the way it is supposed to or

how it is working in general. The main motivation is to find out if the economic value of data has a big impact on the need of personal data regulation and also how that is from the companies' point of view.

As stated previously in this chapter, nowadays it is next to impossible to avoid using internet even a little bit. It is very much a part of our society and therefore it is also important to protect data. Therefore, the motivation to this thesis also comes from a personal point of view. Being a user of the internet comes with its perks naturally but there are also side effects to it and not all of them are positive. No matter what webpage you open or what application you use, you are always asked if you approve of the collecting of your personal data through for example cookies that are on websites. Every webpage also has a privacy policy from which every individual can check what personal data they are sharing by using said webpage.

What is motivating about this subject is also the global aspect of it. Since GDPR is a regulation that companies both inside the EU and with customers inside the EU need to comply, the regulation covers a large area geographically and also in the number of companies. Such legislation needs to be well organized among the different operators that are subjected to it. With forever globalizing world, it is interesting to study how such legislation compares to concepts of personal data protection in different legislations and also in the global ones.

1.1.3 Research question

The research question is as follows:

> Is the economic value of data the main distinction between the right to personal data protection and right to privacy?

The research question is made from the hypothesis that the economic value of data would make the main distinction between the right to personal data protection and the right to privacy.

Not all aspects or articles of GDPR are handled in this thesis. Therefore, the GDPR is not handled in full but only taking the aspects of it that are applicable for this thesis. Also left outside of this thesis is more detailed comparison of how the EU data protection law compares to concepts of traditional human rights in different Member States. This limitation is done due to word limit, and it is done with the writer's nationality in mind.

1.2 Structure

The structure of a literature review, in this case a thesis, plays a crucial part in how readable the thesis or study is. By having a logical structure, the reader is able to see that the approach to the study has been methodical. A thorough carefully presented thesis will give the impression that the writer has been careful with his or her writing. [5] This will also create a more trustworthy impression which is important especially in a literature review where the main key of the text is made by combining already existing sources.

The structure of the thesis is planned so that it starts by defining the basics in both GDPR an**d** privacy in traditional human rights law. By defining the basics, it is easier to move on to more specific sides of the matter. The basics form a base for the thesis and through them the research questions are answered. It is in the interest of this thesis to be able to reflect back on the chapters before and to link different chapters with each other. This also makes it easier for the reader to be able to keep up with what is studied in the thesis. After defining the basics comes the comparison of the two subjects that are handled.

[5] Aveyard, H. (2010). Doing a literature review in health and social care : A practical guide. McGraw-Hill Education. p. 147

The first actual chapter of the thesis begins by presenting the GDPR, what it is, how it came into consideration, how it was implemented and what it means to businesses. The second chapter presents the concept of privacy in traditional human rights law by giving a few examples of different countries and how privacy is considered in their legislation**.** The main emphasis is in Finnish legislation and law, and this is studied in more detail than the other examples. Then moving on to the third chapter which compares the two presented in previous chapter**.** It is centred mostly on how the economic value of data makes the biggest difference between the two. The fifth and last chapter before the conclusions looks into the future and ponders on how the GDPR could be in the future and what could be something that influences it. It focuses on social media and globalization. The last chapter is conclusions, so it brings together all the findings and it also presents some further study ideas considering the subject.

1.3 The method and sources

Because the field of study is business law, most of the sources are based on law. The method of study in this thesis is forensic dogmatic. It is a jurisprudence that aims to answer the questions in existing law by systemizing, pondering, and interpreting the norms of law. Therefore, the aim is not particularly to find anything new or to figure out a new solution rather than trying to find the answer by combining already existing laws and literature.

In the Finnish legislation system, sources of law are divided into three groups that are strongly binding, weakly binding and permitted sources of law. Strongly binding laws are norms of statutory law and also customs that have been established. Weakly binding laws are those that come from legislative drafts and Supreme as well as Supreme Administrative Court decisions. The permitted sources of law are ones that are not written and are legal principles and arguments. It is possible for rules to have a normative conflict

between them in which one law forbids what the other requires to do. In these situations, it is the principles that come in and give balance. [6]

The thesis subject is studied from the point of view that the economic value of data makes the main difference between the EU data protection law and conceptions of privacy under traditional human rights law. This comparation is done by combining different sources and legislation inside the EU and inside it's Member States, especially Finland.

The thesis is very much based on EU-law therefore EU-law plays a big part in reference material. Other point of view is traditional human rights and these are studied through national laws and by comparing different countries and their human rights law. Finland is naturally the subject that is studied the most which is rather self-explanatory given the writers nationality. The sources used in this thesis are both in English and Finnish. A part of the thesis is based on Finnish legislation and implementation and therefore it is natural that the most comprehensive sources on that aspect are found in Finnish.

This thesis is a literary review so that brings some limitations, and this thesis should be seen as more of a combination of different sources rather than a study that makes new revelations. In addition to this, also some limitations come from the fact that it is a master's thesis and not a longer dissertation therefore the word count is also limited and not every point of view from GDPR can be taken into consideration. The GDPR is a vast subject and the page count in this thesis is only a starting point into the world of GDPR.

By doing a literature review it is possible to identify not only the areas that there is research from, but also those areas in which research hasn't been done yet and where it would be beneficial. [7] It is not possible to cover all these areas in a restricted word count,

---

[6] Raitio, J. (2012) The Source of Law – Doctrine and Reasoning in Finland. US-China Education Review B 11. Retrieved from: https://helda.helsinki.fi/bitstream/handle/10138/42078/Raitio_Source_of_Law_Doctrine_and_Reasoning_in_Finland.pdf?sequence=2

[7] Oliver, P. (2012). Succeeding with your literature review: A handbook for students. McGraw-Hill Education. p. 6

but these could benefit the subject by giving ideas for wider research. Since the subject of the thesis is very much based on the internet and that in turn is a very quickly transforming area, gives this many opportunities from areas in which there isn't that much research on yet.

There are various reasons why a research study is influential, and these reasons include aspects such as changing the way the subject area is seen and developing new widely applicable concepts. [8] These are key features when considering these articles from a thesis point of view. One part of a literature review is to also identify when writers disagree on an issue and this aspect is a very informative part. [9] For example, before looking into the GDPR more one could think that all aspects of privacy are taken into account similarly to in human rights law and therefore articles that are contrary to that idea prove to be the most beneficial in regard to this thesis. Since this is a master's thesis it is somewhat expected to use various sources and find differing opinions in the sources used.

[8] Oliver (2012): p. 10
[9] Oliver (2012): p. 9-10

2 EU data protection law

Eu data protection law consist of The General Data Protection Regulation, more commonly known as GDPR. The GDPR is valid legislation in the whole European Union, and it is a binding law to those countries in the European Union and also to business that do business and have customers inside the European Union. This is defined in recitals 22 and 23, and article 3 in the GDPR. In recital 22 it is defined that regardless of where the processing takes place, if the controller or processor operates in the Union the processing of personal data needs to be in accordance with the GDPR. In recital 23 it is defined that *"the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation*". [10] In this chapter it is presented what the GDPR essentially is, how it became to be, how it is implemented in different countries, especially Finland and what it means to businesses.

2.1 How the General Data Protection Regulation came to be

The European Parliament had already in 1970s called for the protection of data in legislation. However, it was forty years later, in 2012, when the European Commission published a data protection reform package that led to General Data Protection Regulation, commonly known as GDPR. [11] It came into force on May 25th, 2018. The regulation was given first on the 27th of April 2016 meaning that the operators had 24 months and 29 days to prepare for the implementation of the GDPR. [12]

Before the GDPR, the EU had made Directive 95/46/EC of the European Parliament and of the Council, the 1995 Data Protection Directive. This was made in a time where

[10] General Data Protection Regulation (2016/679) Article 3, recital 22 & 23
[11] Lynskey (2016): p.3-5
[12] Sankari, V. & Wiberg, M. (2019) GDPR ei toimi: Tietosuojakäytännöt eivät noudata asetusta. Yhteiskuntapolitiikka 84 (2019): 3. https://www.julkari.fi/bitstream/handle/10024/138277/YP1903_Sankari%26Wiberg.pdf?sequence=2&isAllowed=y p.340

internet was understandable not nearly as developed or widely used geographically or systematically as it is today or as it was when the GDPR was legislated. The Data Protection Directive was created in order to protect personal data which makes sense it being the predecessor to GDPR. [13] Therefore, when the GDPR was created it was not an entirely new phenomenon and legislation rather than a more defined version of the previous legislation and something that was more binding and involved more operators than its predecessor.

The need for a stricter regulation on personal data collection was born because the previous regulations were made in a time where smart phones, and all the data they collect, were not yet a major part of society. [14] According to the EU, over 90 percent of Europeans want to have the same rights when it comes to protecting your personal data despite the location of where their personal information is being handled. [15] There are 447.7 million inhabitants in the European Union [16] so wanting to have similar rights is not a small aspect. Most of the Member States in European Union consist of welfare states and therefore also the internet is used extensively throughout the whole Union. This also increases the amount of personal data stored of the Member States and their citizens. Having legislation that protects this large number of people is important for the individuals as well as all of the Member States.

If an internet user was to read all the privacy policies, they needed to accept in order to use the internet, this would take on average nearly 250 hours every year. [17] This is not beneficial for either the user or the business providing the service because there just simply isn't time to read that number of policies. The result of having to read all the

[13] Lord, N. (2018, September 12) What is the Data Protection Directive? The Predecessor to the GDPR. Retrieved March 2, 2022, from https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr
[14] Wall Street Journal. (2018, May 21) GDPR: What Is It and How Might It Affect You? [Video]. Youtube. Retrieved February 21, 2022, from https://www.youtube.com/watch?v=j6wwBqfSk-o
[15] European Commission (n.d. E). Data protection in the EU. Retrieved March 17, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[16] European Union, estimated in 2020
[17] Hofmann et al. (2018): p. 15

privacy policies could be that either the user would sign and accept something that they actually did not know they were signing up for or that the business would lose users or customers because the individuals would not sign the privacy policies without reading them. Having such legislation enables one to trust that what is said in the privacy policy follows the law. Should there be something that is not in accordance with the GDPR, this would be considered unlawful and such policies would not comply.

The GDPR fines are designed so that not complying to the regulation is costly for a business regardless of it being a large or a small company. The fines are defined in article 83. Rather than the size of the fine depending on the size of the company, it depends on the size of the violations. There are some violations that are more severe than others. The less severe violations are ones that lead up to a fine of 10 million euros or a 2% amount of the worldwide annual revenue of that firm from the preceding financial year. Whichever sum is larger is the one that is used. These less severe violations include violations that are made governing for example articles that define the role of controllers and processors. The more serious violations can lead up to a fine of 20 million euros or 4% of the annual revenue with same limitations as mentioned before in the less severe violations. These more serious violations are the ones that work against what is at the core of GDPR; the right to personal data protection and the right to be forgotten. [18]

According to EU, about 85% of people feel that they no dot have complete control over their personal information and how it is used online. [19] Not having control over one's information could hinder the usage of internet and all the services on it. As mentioned earlier, having access, and using internet is a big part of being a member in the society these days. Therefore, not having control or the feeling that you don't have it could lead to not having the courage to use internet and that could make it so that businesses don't get as many customers online. GDPRs goal is to protect the abuse of personal data from

[18] Wolford, B. (n.d.) What are the GDPR Fines? Retrieved April 14, 2022, from: https://gdpr.eu/fines/
[19] European Commission (n.d. D). Data protection – Better rules for small business. Retrieved March 17, 2022, from https://ec.europa.eu/justice/smedataprotect/index_en.htm

not only humans but also machines that have the ability to act upon their surroundings and make decisions by themselves. [20] Automation is nowadays happening in many industries, and it is a growing phenomenon. The fact that GDPR already is takin into consideration the machines that are not controlled my humans, makes it easier for the developing of automation also happen in such a direction that is safer for the individuals and for the protection of their data.

There have been arguments that protecting data is broader in protecting individual rights than the right to privacy. Data protection has the ability to offer individuals more control when it comes to their personal data. [21]

2.2 What is the General Data Protection Regulation

The General Data Protection Regulation's fundamental achievement is for the individual to recognize their control over their personal data. The GDPR can be seen as an answer to the trends of being transparent, accountable, and reducing bureaucracy.

The GDPR has a set of rights that have been well defined in order for the individual to execute these rights. These rights include

> "*the right of transparency and modalities, the right to be informed, the right of access, the right to rectification, the right to be forgotten, the right to restrict processing, the right for notification obligation, the right to data portability, the right to object and the right in relation to automated decision making and profiling*". [22]

[20] Kocarev, L. & Sokolovska, A. (2018, June 5) Integrating Technical and Legal Concepts of Privacy. IEEE Access, vol.6. pp.26543-26557, 2018, DOI: 10.1109/ACCESS.2018.2836184 p. 26545
[21] Lynskey (2016): p. 90
[22] Gunathunga, S. (2017, September 11). Individual's rights under GPR. Retrieved February, 28, 2022 from https://sagarag.medium.com/individuals-rights-under-gdpr-3256fb3f356c

In article 5 of the GDPR the principles relating the processing of personal data are defined as following.

" personal data shall be

1. *processed lawfully, fairly and in transparent manner in relation to the data subject*
2. *collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*
3. *adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed*
4. *accurate and where necessary kept up to date*
5. *kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*
6. *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage* " [23]

These principles are in the same order as previously; *"lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality as well as accountability*." [24]

In order for the processing to be lawful, it should apply at least one of the following aspects: consent from the data subject or that the processing is necessary for performance of contract, compliance with legal obligation, for protection of vital interest of the data subject or another natural person, for performing a task that is of public interest or for purposes that have legitimate interests by the controller or by a third party. [25]

[23] General Data Protection Regulation (2016/679) Article 5
[24] General Data Protection Regulation (2016/679) Article 5
[25] General Data Protection Regulation (2016/679) : Article 6

2.2.1 Personal data

In GDPR the definition of personal data is made in the article 4 paragraph 1. Any information that is about an identified or identifiable individual is considered personal data. Personal data can be one singular piece of information or a collection of pieces of information that together combined lead to an identifiable or identified individual. In the eyes of GDPR it does not matter in which form the data is collected. It applies to all personal data that can be identified to a person whether it is stored in paper, in video form, inside a system or any other form. [26] Therefore, in addition to having a large scope company wise, the GDPR also handles about personal data that is in multiple different forms.

The most basic examples of personal data are name, both first and surname, address, both home and email address and an identification card number. These pieces of data can easily be led to an identified individual. For example, a company registration number and a company email number that is not identified to a certain individual, are examples of data that are not personal data and to which the GDPR would not apply to. In order for personal data to no longer be personal data, it needs to be fully anonymized in a way that is not reversible. If the anonymization is reversable, this is considered personal data since it can be tracked back to an identified individual. [27]

2.2.2 Basic concepts in GDPR

GDPR refers to a person as someone who is a natural person and not a legal person or a system. Personal data on the other hand is something that can be identified to a person.[28] If you are considered a legal person or a system, there is no such data available that would be considered your personal data. As previously mentioned, personal data is

[26] European Commission (n.d. A). What is personal data? Retrieved March 15, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
[27] European Commission (n.d. A).
[28] Sankari & Wiberg (2019): p. 341

something that is possible to be tracked back to an identified individual and this is not the case if the individual is a legal person or a system.

In the Regulation collecting means the either manual or automatic actions that are targeted in personal data. These actions include such actions as collecting, storing, using or distributing personal data. This data is collected in a register which is any formed group of personal data. [29]

There is a difference in whether a company or organisation is considered a controller or a processor. According to GDPR article 4(7) data controller is someone who determines the purposes that for which purpose and by what means the personal data is collected. A controller answers the questions why and how. It is also possible for a company to be a joint controller, meaning that two or more organisations together decide and determine answers to the previous questions. [30]

The definition of a data processor is made in the article 4(8) in GDPR . A data processor is a company or an organization that works for the controller and is the one that processes the personal data. This entitles that the details and actions required from the processor need to be specified in a contract. A processor is often a third party meaning that it is not from inside the company. [31] However, this does not rule out the possibility of a processor being from inside the company.

There are some situations in which an operator can be both controller and processor. This can happen for example if you are a processor whose job is to process data for other controllers. It is possible that you work as a processor in favour of the controller and

[29] Sankari & Wiberg (2019): p. 341
[30]European Commission (n.d. B). What is data controller or data processor? Retrieved March 15, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en
[31] European Commission (n.d. B)

simultaneously work as a controller for other data. The demarcation is not absolute and there are different possibilities.

2.3 Applicable articles in GDPR

The GDPR contains 11 chapters and 99 articles. It is not in the interest of this thesis to go through all the articles in GDPR so only the most applicable ones are chosen into more specific review. These articles are article 13 "*Information to be provided where personal data are collected from the data subject*", article 15 "*Right of access by the data subject*", article 15 "*Right to erasure*" and article 20 "*Right to data portability*".

Article 13 handles the information that the data collector must provide to the individual whose data is being collected. In the first paragraph it is defined what is the information that the controller should provide to the subject whose data is being collected. These include information such as "*the identity and the contact details of the controller and, where applicable, of the controller's representative*", "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*" as well as "*the recipients or categories of recipients of the personal data*".

Paragraph two has additions to the first one as to what information should be provided to the data subject in order for the processing to be fair and transparent. This means that the controller should provide information about for example "*the period for which the personal data will be stored or … the criteria used to determine that period*" and "*the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability*".

This article serves this thesis because it is about what the data collector's obligations are towards the individual whose data is being collected. Therefore, it is important that both the collector and the one whose data is being collected are informed of what the

collector's responsibility is here and what should the individual whose data is being collected know about the data collection. It increases the feeling of having control over one's privacy when one is aware of how their data is being used and for what purpose.

In the third paragraph of article 13 it is defined that if the controller intends to process the collected data for some other purpose than what it was originally collected, prior to that the same information should be provided to the data subject of the other purpose as well as any other relevant information. This increases the control of one's personal data because by giving permission to use it for one purpose does not mean that you would give the permission to use it for other purposes as well at the same time.

Article 15 is about the right of access by the data subject. In the first paragraph of said article it is defined what are the information that the data subject has the right to obtain from the controller the confirmation that his or her personal data is being processed and also information such as "*the purposes of the processing*", "*the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations*" and "*the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing".*

It is also stated in the article 15 paragraph 3 that the controller needs to provide a copy of the personal data to the data subject and if this request is done by electronic means the information should also be provided in the same form.

An important aspect to privacy is knowing how and why your personal data is being stored, used, or collected. Because of this, the article 15 is important when considering the privacy angle of data protection. Privacy is not only about having your personal data to yourself but also having the feeling that you are in control of your personal data and how it is used.

This is much linked to the previously presented article 13. The difference between the two is that article 13 presents the rights and obligations from the controller's point of view whereas in article 15 these are presented more from the individual's point of view. it could be said that article 13 is more important to the business and article 15 more important to the individual when considering the rights.

Article 17 in the GDPR is about the right to erasure or more commonly known as the right to be forgotten. It defines the ground rules to which the data subject has the right to ask for his or her personal data to be removed by the controller as soon as possible. The grounds that need to apply include aspects such as "*the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed*" and "*the personal data have been unlawfully processed*".

If the controller has made public of the personal data, it is the controller's obligation to inform the controllers processing the data that the subject has requested for his or her data to be erased. At its core the article 17 means that if an individual asks for their data to be removed, then the controller is forced to do so.

In the paragraph 3 there are mentioned some exceptions to the previously mentioned grounds. If for example the processing is necessary for exercising the right of freedom of expression and information or for the establishment, exercise or defense of legal claims then in these cases the right to be forgotten does not apply.

Article 20 in GDPR is about the right to data portability. The first paragraph of the article defines that the data subject has "*the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided,*

where: a. the processing is based on consent pursuant or on a contract pursuant b. the processing is carried out by automated means".

In the second paragraph it is said that the data subject has the right to have their personal data transferred between controllers if it is technically feasible. The third paragraph defines that the actions mentioned in the first paragraph of this article should be without prejudice to the previously mentioned article 17.

This article is the most coherent when thinking about the economic value of data. Because of what is stated in this article, the data subjects have the ability to know what data is collected of them and how it has been used. Therefore, it is not possible for companies to sell out individuals' data without them knowing about it or at least without the big risk of getting caught and having to deal with consequences.

2.4 Implementation

EU has supported the implementation of GDPR by giving its State Members funding total of 6,3 million by the end of 2020. For example, Finland has gotten funding to raise awareness about GDPR and how it opens doors to the digital markets. [32]

In Finland the new requirements brought on by GDPR were addressed by introducing new legislation, Finnish Data Protection Act and Act on Protection of Privacy in Working Life. [33] Prior to the GDPR and the Data Protection Act, there was Personal Data Act in the Finnish legislation. Therefore, protection of individual's data was already taken into consideration in the Finnish legislation before the GDPR was implemented. This is understandable because the use of Internet and data collection that comes with using it

[32] European Commission (n.d. C). Eu funding supporting the implementation of the General Data Protection Regulation (GDPR). Retrieved March 15, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

[33] White & Case (2019, November 13) GDPR Guide to National Implementation: Finland. Retrieved March 3, 2022, from https://www.whitecase.com/publications/article/gdpr-guide-national-implementation-finland

was already very much in full force before the GDPR came to be. The Personal Data Act is much like the Data Protection Act as both of these laws handle about the same subject. The Personal Data Act will be presented in more detail in chapter three of this thesis where it is applicable when considering privacy in legislation in Finland.

According to Saarenpää, the GDPR has transformed the individuals' obligation to find out what they are registering to, to the controller's obligation to inform the individual of the same aspects. Therefore, the controller, if needed, has to inform the registered individual about the register keeping and how their personal data is being handled if this is not already known to the registered party. This has made it possible for people to know how and where their information is being handled. The obligation to inform also includes that upon request the controller needs to submit all the information they have of the individual to the individual themselves. [34]

2.5 What it means for businesses

The GDPR regulates all the companies in European Union but also all those companies who are dealing with the personal data of individuals living in the EU area. Therefore, it affects companies all around the world, even though it is legislated in the European Union. By covering such a large area, this means that most major companies around the world are affected by the GDPR. [35] The GDPR affects especially the business and industries that are to do with banking and finance. This is because typically in this industry large amount of personal data is collected and stored. [36]

---

[34] Saarenpää, A. (2015). Henkilö- ja persoonallisuusoikeus. In: Oikeus tänään. Part II, pages 203-430. 3.revised, 2015. Ed. Marja-Leena Niemi. Rovaniemi: University of Lapland.

[35] Gruschka, N., Jensen, M., Mavroeidis, V. & Vishi, K. (2018) Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. https://arxiv.org/pdf/1811.08531.pdf p.1

[36] Larsson, A. & Lilja, P. (2019) GDPR What are the risks and who benefits? in Larsson, A. & Teigland, R. (Ed.) The Digital Transformation of Labor. Routledge. p.193

For a company GDPR meant some changes in how they present themselves online. The GDPR craves that companies use plain language and tell customers who they are requesting the data, why it is processed and for how long and where it is stored. It also means that the companies must have customers consent in order to process their data and this consent should be given as clearly as possible. According to the GDPR consent is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". [37]

In addition to this consent is also mentioned in the article 7 that is about the conditions of consent. In this article 7 it is defined that the controller has to be able to demonstrate that the consent has been given by the data subject. This applies when consent is what the processing is based on. It is also mentioned in this same article that the data subject has "*the right to withdraw his or her consent at any time*". The process of withdrawal should be as easy as giving consent. [38]

Customers should also have the ability to both access their own data and also to give it to other companies. In case of a risk of a data breach, customers should be informed. [39]

In order for a business to comply with the GDPR, the need to change their internal procedures as well as their processes. The measures businesses need to do in order to implement the GDPR in their everyday process include for example maintaining a record of their activities concerning processing and data. [40] The GDPR can be used by companies as a tool to ensure that they collect, use and destruct data correctly and carefully.

[37] General Data Protection Regulation (2016/679) : Article 4(11)
[38] General Data Protection Regulation (2016/679) : Article 7
[39] European Commission (n.d. D)
[40] Teixeira, G., Mira da Silva, M. & Pereira, R. (2019). The critical success factors of GDPR implementation - a systematic literature review. Digital Policy, Regulation and Governance. 21 (4), 402-418, DOI: 10.1108/DPRG-01-2019-0007

Companies can also use it as a tool to estimate the value of their own data and use it as a strategic asset. [41]

The GDPR makes it so that companies take the laws that are addressed with it more seriously, meaning laws that deal with privacy and personal data. Upon taken into action the GDPR's practices, many companies have only then for the first time evaluated how they handle personal data. [42] Implementing the GDPR also craves the companies to have privacy officials amongst their organization whose job is to survey that data is handled in a correct way. [43] This of course will mean that the company will need to hire or educate someone to do this line of work. In the beginning this will mean additional costs but in the long run this will benefit the companies work. The GDPR should be seen more as a process rather than an accomplishment. [44]

A study conducted by a reporter from the Finnish Broadcasting Company YLE, Joni Nieminen, put the GDPR into practice by having an IT-worker and master student of communication Emilia Laurila to ask from several companies that she had been in contact with either as a user of the service or as an employee, to get a listing of all the information that these companies have of her. There were both Finnish and international companies involved. From most of the businesses the information was fairly easy to get. A few of the international companies deleted Laurilas information instead of doing what she asked them to which was to deliver the information to her. This brings up the doubt that these companies have something to hide and whether you are able to trust that they delete the information fully upon request. It was also an interesting find in the study that one of the Finnish companies had the information only printed on a paper and in order

---

[41] Hoofnagle, C., Van der Sloot, B. & Borgesius, F. (2019) The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law; 28(1), 65-98, DOI: https://doi.org/10.1080/13600834.2019.1573501 p.67

[42] Hoofnagle et al. (2019) p. 67-68

[43] Hoofnagle et al. (2019) p. 68

[44] Edwards, J. (2021, January 14) 6 business benefits of data protection and GDPR compliance. Retrieved April 15, 2022, from https://www.techtarget.com/searchdatabackup/tip/6-business-benefits-of-data-protection-and-GDPR-compliance

to get to see the information, Laurila had to travel 300 kilometres. This is against regulation since in the same article it is stated by data protection ombudsman Reijo Aarnio that if the information is requested electronically, they should also be delivered in the same way. [45]

As mentioned previously in this chapter, the fines for actions against the GDPR can lead up to a fine of 20 million euros or more. This is a significant fine and the amount of the fine entails the importance of data protection. Such fines would not be issued if the subject was not of high interest. In Finland by September 2021, there had been issued fines due to breaking the GDPR rules in total amount of hundreds of thousands.[46] The biggest fine has been issued to the Finnish company Posti. The fine was in total 100.000,00 euros because they had broken the GDPR by not informing the registered their right to deny giving their information to third parties when they did a moving notice. This right was only informed to those individuals who bought additional services in addition to giving this moving notice. [47]

Even though complying to the GDPR means that companies need to take some extra things into consideration, by no means is the meaning of the GDPR to hinder businesses but quite the contrary as one of its goals is to make customers trust especially small businesses more. [48] Article five in the GDPR lists the seven fundamental principles that are in the base of the regulation. These are "*lawfulness, fairness and transparency,*

[45] Nieminen, J. (2019, August 22). Emilia Laurila, 25, halusi selvittää, mitä tietoja hänestä on kerätty – paljastui hämmentävän tarkkaa raportointia ja yllättäen tuhottuja tietoja. Yle. Retrieved March 13, 2022, from: https://yle.fi/aihe/artikkeli/2019/08/22/emilia-laurila-25-halusi-selvittaa-mita-tietoja-hanesta-on-keratty-paljastui

[46] Pietarinen, H. (2021, September 10th) Parkkipate ja Posti saivat kymmenienthuansien eurojen gdpr-sakot, joita suomalaisyrityksille on tulossa lisää. Helsingin Sanomat. Retrieved March 4, 2022, from https://www.hs.fi/talous/art-2000008247280.html

[47] Office of the Data Protection Ombudsman. (2020, May 22nd) Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations. Retrieved March 4, 2022, from https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista?languageId=en_US

[48] European Commission (n.d. D)

purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality as well as accountability". [49]

This means that when a company operates following the regulation to the GDPR, said company is all of these qualities. Knowing that the business, even small ones must work by certain rules according to data protection, makes the customers feel that they are able to trust the business more. It has been researched that not following the regulation can cause mistrust in the company. Over half of the interviewed people in the research were of that opinion. [50] The GDPR also benefits businesses by giving both the business and individual clear instructions and guidelines in how to act. If you know how your personal data is going to be handled, you are more responding towards giving it to use to a company because you know that you are able to trust how they handle your personal information. If they were to do something wrong or criminal with it, you are also able to trust that they will be prosecuted accordingly.

Also having an even privacy regulation means that also the competition between companies needs to be even. Prior to the GDPR the competition was unfair between those companies that paid attention to the ethical aspects of business and the companies that did not mind the ethical side.[51] Since privacy is a human right, it is important that the businesses are required to obey protecting privacy.

Privacy in organizations can be defined with two principles, the first of which is privacy by design. This means that privacy should be included from very early on in the developing of new products, services, or such. This is an easy way to make sure that the GDPR's regulations are being followed when privacy is considered very early on in the planning process. The second principle is privacy be default. This means, as the name states, that

---

[49] Edwards (2021)
[50] Asaolu, H. (2020, March 16) GDPR Compliance Implementation: all the requirements and things to do. Retrieved April 13, 2022 from: https://leadsbridge.com/blog/gdpr-compliance-implementation-for-dummies- all-the-requirements-and-things-to-do/
[51] Edwads (2021)

when organizations offer either a system or a service and this system or service allows customers to have the choice of how much of their personal data they want to share, it should be the default option that gives the most protection to said individual. [52]

Data protection by design and by default is also defined in the article 25 of the GDPR. It is legislated that the controller should "*implement appropriate technical and organisational measures … which are designed to implement data-protection principles*" and also that "*the controller shall implement appropriate technical and organisational measures for ensuring that … only personal data which are necessary for each specific purpose of the processing are processed*". [53]

A benefit to companies that comes with the GDPR is, in addition to previously mentioned features, that it favours relationships that combine data subjects and companies directly without third party advertising or content networks. Before the GDPR it was cheaper to companies to buy data from third parties instead of buying it from the data subject themselves. [54] Not having a third party who delivers the information, this gives companies the ability to form a relationship with the customers themselves and, they are able to tell that the personal data has been retrieved lawfully.

[52] Edwards (2021)
[53] General Data Protection Regulation (2016/679) Article 25(1-2)
[54] Hoofnagle et al. (2019) :p. 68-69

3 Privacy as a right and in legislation

Privacy is seen as a fundamental right and something that is part of every individual's basic human rights. This emphasises the importance of privacy and the need to protect privacy. This chapter will first present what privacy in general is, how it can be defined and whether it should be seen as an individual right or something that has a common goal. After this will be presented privacy in legislation, in global context as well as privacy more defined in the Finnish legislation.

3.1 Privacy in general

The Cambridge dictionary defines privacy as a right to keep your personal matters a secret. [55] Privacy is something that is recognised by most countries in the world either in their constitution or in other ways in their legislation. It is also considered to be a fundamental right, this originating from the fact that privacy comes from human dignity. [56] This means that every human being has a value, and they should have respect. Human dignity also means that individuals should have self-worth thus meaning that they believe that they have the worth that human dignity entitles. Privacy being something that originates from human dignity emphasises even more the role of it as a human right.

The boundaries of privacy can't be defined clearly, and it is not a fixed condition. [57] Therefore, it can occasionally be rather difficult to define clearly or to identify those boundaries in which privacy is protected. Privacy can't be defined with a purely legal or

[55] Cambridge Dictionary (n.d.B). Privacy. Retrieved April 20, 2022, from https://dictionary.cambridge.org/dictionary/english/privacy)

[56] European Data Protection Supervisor (n.d.) Data Protection. Retrieved March 30, 2022, from https://edps.europa.eu/data-protection/data-protection_en#Interaction

[57] Cohen, J. E. (2013, May 20). What Privacy Is for. Harvard Law Review, 126(7), 1904–1933. https://harvardlawreview.org/2013/05/what-privacy-is-for/ p.1906

philosophical definition. [58] This applies also when the point of view is law. There isn't one legislation that covers all areas of privacy rather than privacy is a part of many different legislations and has been the starting point to legislations, for example the GDPR.

When thinking about what privacy actually is, one could come to the conclusion that privacy has a value or that privacy in itself is a value. [59] Privacy is commonly held to a great value and something that should be a right that everyone has. Privacy can also be defined through norms of exclusivity meaning that it is established by a group of norms that regulate the access to individual or the group of them. [60]

Privacy rights are as the name states, rights that aim to protect individuals' privacy. Even though privacy rights protect individuals, privacy is not an individual right. Privacy has a meaning also in public policy through innovation and human flourishing. [61] Privacy has a crucial role in social interaction and an invasion to privacy happens if someone's personal barriers of privacy are breached. [62]

Privacy is considered to be a basic right and something that people automatically have. However, privacy should not only be considered from the individual's point of view. It should be seen through the fundamental role it plays in social interaction between individuals. [63] The European Data Protection Supervisor follows along the same lines by defining privacy as something that is not just an individual right but should be seen as something that has social value. [64] Privacy has a significant role in establishing those

[58] Hughes, K. (2012, September 13) A Behavioural Understanding of Privacy and its Implications for Privacy Law. The Modern Law Review. 75(5) p. 806-836. [Resticted availability] https://doi-org.proxy.uwasa.fi/10.1111/j.1468-2230.2012.00925.x p.806
[59] Taylor, M. (2012) Genetic data and the law: A critical perspective on privacy protection. Cambridge University Press. p.15
[60] Taylor (2012): p. 25
[61] Cohen (2013): p. 2013
[62] Hughes (2012): p. 807
[63] Hughes (2012): p.823
[64] European Data Protection Supervisor (n.d.)

conditions that enable public life. [65] It is in the public's interest as well to have a proper privacy protection.

According to Hughes, privacy can be something that is experienced in different ways. This includes such states as solitude and anonymity. There can be also different behavioural ways that individuals show and experience privacy. These include verbal behaviour as well as non-verbal one. [66] The need to privacy can be expressed with words or it can also be expressed by a gesture such as turning away.

The concepts of privacy in traditional human rights law are based on it being a basic human right rather than a mean of business. It is the economic value of personal data that has created the need to have legislation on it and how one can use it. If privacy and the protection of it were merely only for people to be able to keep their anonymity, such data protection regulation would possibly not even need to exist.

From lawmakers' point of view privacy can be invaded in different ways. There can be for example threats against one's personal information or attempts to break one's privacy barriers. [67] This thesis is focused on privacy on personal data therefore these threats or attempts to break privacy barriers would be to either threat to get individuals personal information and used in an unlawful way or then if by some way the data would already be at the hands of the invader, they could make threats as to how they will handle already existing personal data. Attempt to break a privacy barrier would be to perform such actions that would enable you to get a hold of information that does not consider you or be your personal data.

There are companies that provide services in order to even more enhance one's privacy or security, but majority of people do not use these services because they feel that

[65] Taylor (2012): p. 13
[66] Hughes (2012): p. 808-809
[67] Hughes (2012): p. 815-817

privacy is something that should be protected even without the use of these kind of services. It can be quite contradicted that at the same time people consider privacy to be a right that is of great value in their life but also feel that privacy is such a right that everyone should have it without needing to especially do anything for. Privacy is seen as something that is self-evident.

3.2 Privacy in legislation

Privacy is a part of multiple legislations. This is rather self-explanatory because as mentioned previously in this chapter, privacy is considered as a basic human right. People hold privacy in a great value and in order to keep your privacy in a level that you want, there is the need to have it in legislation also.

This part of the chapter under this subtitle will deal with how privacy is considered first in global legislation and then more detailed in Finnish legislation.

3.2.1 Privacy in global legislation

According to the United Nations Conference on Trade and Development, 71 % of the world's countries have legislation on privacy and data protection. In Europe alone almost all the countries have legislation on these issues, and this is largely due to the GDPR that is implemented to countries that are in the European Union. In comparison, in Africa only 61 % of countries have legislation on privacy and data protection issues. [68]

What made the legislation complicated before the GDPR was implemented was the fact that the law that is the EU Member States origins from not only the national and

[68] United Nations Conference on Trade and Development (n.d.) Data Protection and Privacy Legislation Worldwide. Retrieved March 13, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

international orders but also European Union orders. [69] Prior to the GDPR there was the Data Protection Directive that was enacted in 1995. It is a directive that handles about the protection of individuals in regard to the processing of personal data and the free movement of that data. [70]

The main global legal instrument in protection of privacy is The International Covenant on Civil and Political Rights (ICCPR). [71] It is an international human rights treaty that was adopted in 1966. [72]

Article 17 in the ICCPR is about privacy and the first part of the article states that

> *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. "* [73]

The Universal Declaration of Human Rights, also known by its abbreviation UDHR, was declared by the United Nations in 1948. There are 193 member states currently in the United Nations (UN), including all EU countries. [74] The Universal Declaration of Human Rights mentions privacy in at least two of its articles. Article 3 defines that "*everyone has the right to life, liberty and security of person*". In article 12 one part of the article is that *"no one shall be subjected to arbitrary interference with his privacy".* [75]

---

[69] Dörr, D. & Weaver, R. (2014). Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries. Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110338195 p.22

[70] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

[71] DigWatch (n.d.). Privacy and data protection. Retrieved April 12, 2022, from https://dig.watch/topics/privacy-and-data-protection

[72] Equality and Human Rights Commission (n.d.A) . International Covenant on Civil and Political Rights (ICCPR). Retrieved March 15, 2022 from https://www.equalityhumanrights.com/en/our-human-rights-work/monitoring-and-promoting-un-treaties/international-covenant-civil-and

[73] International Covenant on Civil and Political Rights: Article 17

[74] United Nations (n.d.B) Member States Retrieved March 13, 2022 from https://www.un.org/en/about-us/member-states

[75] United Nations (n.d. A) Universal Declaration of Human Rights. Retrieved April 2, 2022 from https://www.un.org/en/about-us/universal-declaration-of-human-rights

The fact that privacy is mentioned in such a global declaration confirms the position that it has and the importance it holds as a basic human right. Since there are so many member states in the UN, the UDHR holds an important place in how the concept of privacy is considered in different countries. Notable is that the UDHR was declared in a time where the internet was not yet invented since the internet was created in the mid-70s. [76] Therefore, the concept of privacy has broadened during the years after the declaration but still the articles apply because personal data that is handled in the internet falls very much under the category of privacy.

Inside the European Union the Charter of Fundamental Rights of the European Union is the legislation that defines the fundamental rights of those individuals living inside the EU. The goal of the Charter was that the rights across EU Member States would be consistent and clarified. it became legally binding in December 2009 when the Treaty of Lisbon was entered into force. [77]

In the Charter privacy is defined in article 7 stating that "*everyone has the right to respect for his or her private and family life, home and communications*". [78] The Charter also considers personal data and the protection of it in its article 8 and in the first paragraph it is defined that "*everyone has the right to protection of personal data concerning him or her*". [79] The fact that these two rights are defined in separate articles creates a distinction between the rights. This is notable because the Charter is, as mentioned, legally binding in the EU.

---

[76] Tarnoff, B. (2016, July 15) How the internet was invented. The Guardian. Retrieved March 23, 2022, fromhttps://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf

[77] Equality and Human Rights Commission (n.d. B) What is the Charter of Fundamental Rights of the European Union? Retrieved May 22, 2022 from https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union

[78] Charter of the Fundamental Rights of the European Union (2012/C326/02) article 7

[79] Charter of the Fundamental Rights of the European Union (2012/C326/02) article 8

3.2.2 Privacy in countries' legislation outside the EU

In Australia privacy is legislated in the Privacy Act 1988. It controls and protects the privacy of individuals as well as regulates how different organisations need to handle personal information. The Privacy Act goes further than just regulating the privacy and it has similar aspects to the GDPR. However, it does have more limitations than the GDPR when it comes to for example who the act regulates and which kind of organisations fall under its process. In the core the Privacy Act is a regulation that is about how the individuals' personal information should be handled. It has similarities to the GDPR since it regulates how individuals' data should be handled and what information should the individual be given when handling said data. There is also Information Privacy Act 2014 that applies to the public sector agencies, and it covers the area of amongst others collecting, using and storing personal data. [80] Even though the GDPR applies to countries inside the European Union and to companies that have customers inside the European Union, there is also similar legislation in Australia for example as presented before.

In addition to Australia, there is also privacy law in China's legislation. The Personal Information Protection Law (PIPL) is a fairly new legislation since it has only been effective from the beginning of November 2021. PIPL was created in order to regulate data online and protect individuals' personal information. According to article 3 the PIPL applies to "*the processing of the personal information of natural persons within the territory of the People's Republic of China".* [81] Therefore, it is not as wide-ranged as the GDPR. Although when compared by populations, there are 1, 449 billion people in China [82] and that

[80] Office of the Australian Information Commissioner (n.d.). The Privacy Act. Australian Government. Retrieved April 9, 2022 from https://www.oaic.gov.au/privacy/the-privacy-act

[81] China Briefing (2021, August 24) THE PRC Personal Information Protection Law (Final): A Full Translation. Retrieved March 15, 2022 from https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

[82] As of 30th of April 2022

compared to the population in EU that is around 477 million people. [83] This means that the PIPL actually considers a much higher amount of people than the GDPR. The PIPL, like the GDPR covers all companies that have customers inside the Peoples Republic of China. This also makes the number of individuals that the regulation protects a lot higher since it is also binding to companies that are not from the Peoples Republic of China but have customers inside it making it globally a significant law.

The United States have a slightly different approach to privacy and data protection compared to for example the GDPR. In the US, privacy and data protection regulation are more sector specific. The regulations about privacy in the US include such as The Health Insurance Portability and Accountability Act (HIPAA) and The Federal Information Security Management Act (FISMA). In the US, data protection is addressed into more importance and privacy is mentioned more in segmented privacy laws. Most essential difference when comparing the US privacy and data protection regulation to the GDPR is the emphasis that the US legislation has on data as a commercial asset whereas the GDPR's main goal is to protect individuals and their rights before companies. [84]

3.2.3 Privacy in Finnish legislation

Finland is considered to be a welfare country and it is a part of the European Union. The concept of privacy in Finland is seen quite similar as in those countries that are also situated inside Europe. As stated, Finland is a part of the European Union meaning that some of the laws such as Treaties or Regulations of European Union are binding also in Finland.

---

[83] European Union (n.d.) Facts and figures on life in the European Union Retrieved March 30, 2022 from https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en

[84] Coos, A. (2021, April 23) EU vs US: What Are the Differences Between Their Data Privacy Laws. Retrieved March 19, 2022, from https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/

The European Convention on Human Rights was joined by Finland when it became a member of the Council of Europe in 1989. It is a part of the Finnish legal order. [85] In the article 8 of the European Convention of Human Rights it is ordered that everyone is entitled to have a right to respect both in their private and their family life. The first part of the article states that:

> "*Everyone has the right to respect for his private and family life, his home and his correspondence*. " [86]

Privacy in Finnish legislation is included in the Constitution of Finland. Section 10 in the Constitution defines the right to privacy in a quite similar way that is defined in the previously mentioned European Convention on Human Rights.

> "*Everyone's private life, honor and the sanctity of the home are guaranteed." [87]*

The Constitution forms the base to all legislation and exercising of government power in Finland. [88] Therefore, it can be interpreted that privacy holds an important position in the Finnish legislation. Since the definition of privacy is the act of keeping something secret, the importance of privacy can also be interpreted as a cultural thing. Finns are often seen as reserved people and privacy is an important aspect.

According to the legislation everyone's private life is guaranteed, and this includes also all the personal data that is collected of that certain individual. Therefore, the aspects

---

[85] Viljanen, J. (n.d.) The European Convention on Human Rights and the Transformation of the Finnish Fundamental Rights System: The Model of Intepretative Harmonisation and Interaction. Retrieved March 4, 2022, from https://www.scandinavianlaw.se/pdf/52-16.pdf p.305

[86] European Convention on Human Rights: article 8

[87] Constitution of Finland (731/1999) 10 §

[88] Ministry of Justice Finland (n.d.) Constitution. Retrieved March 11, 2022, from https://oikeusministerio.fi/en/constitution-of-finland

that are ordered in the GDPR are in Finnish legislation an expansion to what has already been legislated in the Constitution.

Privacy is also included in the Act on the Protection of Privacy in Working Life (2004/759). Since people use a large amount of their life working, also a lot of their data is being collected and used during the years of labour. Therefore, it is important to define regulation for privacy in the workplace as well. The legislation on privacy and personal data is defined in the section 3 of said Act.

> *" The employer is only allowed to process personal data directly necessary for the employee's employment relationship, which is connected with managing the rights and obligations of the parties to the employment relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned."* [89]

Privacy and the importance of it in the workplace is not often considered as important as it should be. Especially nowadays when it is not that common anymore to stay on the same workplace and work under the same employer one's entire career, there can be a lot of personal data collected of an individual by different employers. Therefore, it is important that all this personal data is handled correctly and in a way that the individuals can trust that their privacy is secured. It is quite clearly defined in the section above that an employer is strictly only allowed to handle personal data that is connected to the individual's employment. This means that the employer is not allowed to collect or store any kind of personal data of their employees without the employee's consent.

The importance of privacy in the working life can also be presented through discrimination or the prevention of it. Because personal data that is collected by employers needs to be connected to the employment relationship, the employer doesn't have a right to

[89] Act on the Protection of Privacy in Working Life (2004/759) 3 §

either ask or find out whatsoever personal information about the employee. These include personal data such as gender, sexual orientation, or political views. Especially information that is considered sensitive should not be collected without permission form the employee.

As well as in the previously presented regulations, privacy is also mentioned in the Personal Data Act (532/1999). As mentioned in the second chapter of this thesis, this act has been replaced by the Data Protection Act. It is in the interest of this thesis to present this Act also since it presents how privacy, especially in data protection has been handled in the Finnish legislation even before the GDPR came into action.

In the Personal Data Act the word privacy is mentioned fourteen times, and the most significant is the first section which defines the objectives of the Act.

> "*The objectives of this Act are to implement, in the processing of personal data, the protection of private life and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice.*" [90]

Also, section 5 that handles the duty of care is quite telling in how the context of privacy is considered in the Finnish legislation. This mirrors quite well to the GDPR and therefore not much has changed in this sense after the implementation of the GDPR.

> *"The controller shall process personal data lawfully and carefully, in compliance with good processing practice, and also otherwise so that the protection of the data subject's private life and the other basic rights which safeguard his/her right to privacy are not restricted without a basis provided by an Act. Anyone operating*

[90] Personal Data Act (523/1999) 1 §

on the behalf of the controller, in the form of an independent trade or business, is subject to the same duty of care. " [91]

3.2.3.1 Cases on privacy in the Finnish legal system

Privacy is an issue that when breached, sometimes needs a decision from the court. The examples presented in here are linked to the GDPR for the sake of this thesis.

The adjudication made by the Finnish Supreme Administrative Court, KHO: 2018: 112, handled about if the individual or common benefit should be taken more into account when considering the right to be forgotten. The case was about a situation where the data ombudsman had ordered Google Inc as a register to delete two certain search results that contain certain individuals' information. The results that were requested to be deleted lead to a forum on the internet and the other to a news site. Both of these links lead to information that was delicate and it considered of the individuals medical details as well as the sentences they had gotten. The question that was being reviewed was whether or not these search results would be such that could be ordered to be removed or if they were necessary for the handling of such individual's personal information. The individual in question had committed a violent crime and therefore the search results could be justified with the common benefit in mind. The Supreme Administrative Court came into the decision that it was justified that these search results were deleted because even though it is in the public interest to get this information, this public interest is not greater than the individual's right to privacy. [92]

In these cases, one could wonder if the individual's right to privacy is in fact greater than the public interest. Having this information online could lead to hindering similar crimes when it would be known how public the information is going to be. On the other side it

[91] Personal Data Act (523/1999) 5 §
[92] KHO: 2018:112

can be argued on the individual's side that why a person who has committed a crime but has not brought it to the public eye by themselves and the search results lead to forums were other people are discussing of the matter, should need to suffer for it possible for the rest of their lives.

Another case handled in the Finnish Supreme Court, KKO: 2015: 41, was about the discrimination of an applicant in a job interview. The discrimination happened when the applicant was asked whether or not her spouse was politically active. The applicant had declined and therefore answered in an untruthful matter. In the interview it was also implied that the spouse of such applicant was a male when in fact the spouse was female. The employer had prior to the beginning of the employment relationship terminated the management contract made with said applicant. The Supreme Court ruled that discrimination had happened. The case is linked to privacy by previously showcased Act on Protection of Privacy in Working Life. The question about whether or not the applicant should reveal their spouses gender falls under the pretense of protection of privacy. Therefore, it should be something that doesn't have an effect on when considering if the applicant is suitable for the job or not. According to article 3 in the Act on Protection of Privacy in Working Life, an employer is only allowed to handle such personal data that is connected with managing the job. Therefore, the knowledge of whether or not the applicant's spouse was politically active or not is not something that is directly connected to managing the job and should not be taken into account in a job interview or as part of personal data that is collected of the applicant or afterwards possibly an employee. [93]

A recent case in the Finnish legal area considering privacy and especially data protection is a center for psychotherapy Vastaamo and the breach in their data protection. In the breach the hackers got the personal data of multiple individuals including their Finnish social security numbers. This led to extorsion attempts made by these hackers towards

[93] KKO: 2015: 41

those individuals whose personal data they had stolen. [94] In this case the data ombudsman issued a fine of 608 000 euros to the company for breaking the GDPR regulation. According to the data ombudsman the company had not followed the correct protocol in order to shield the personal data from unlawful use. [95] This is a good example of why personal data needs to be protected and what kind of consequences it could bring if the data protection is not done in a correct way. Not only are the consequences faced by the company in form of the fines and also in the form of its reputation going bad but also the individuals whose personal data has been leaked due to the hackers being able to get their hands on it.

What is interesting in such cases is that a person who buys personal data from an operator who has gotten this data in an unlawful way, could themselves commit a crime against data protection because they are buying information of individuals that have not given the permission to use their personal data. The fact that the personal data has been breached is in itself a bad enough fact but what makes it even worse is that one of the rights ordered by the GDPR, the right to be forgotten may be forever lost on these individuals whose data has been unlawfully used because it is next to impossible to know how widely the hackers have spread the data. This could lead to decades worth of trouble to the victims. Therefore, the legislation is truly made for a reason and the sometimes harsh fines are there also for a good reason.

[94] Niinistö, M. (2020,October 27). Mistä tiedän onko tietoni vuodettu? Uskaltaako terapiassa enää puhua? Haimme vastaukset 31 kysymykseen Vastaamon tietomurrosta. Yle. Retrieved April 2, 2022, from: https://yle.fi/uutiset/3-11615408

[95] Ikävalko, K. (2021, December 16) Tietosuojavaltuutettu määräsi Psykoterapiakeskus Vastaamolle 600 000 euron seuraamusmaksun erittäin vakavista tietoturvallisuuspuutteista. Yle. Retrieved March 30, 2022, from https://yle.fi/uutiset/3-12232962

4 Comparing data protection and privacy

Comparing means the action of examining two or more things and trying to find the difference between the two. Another definition for the word is also the act of suggesting or considering that two or more things are of equal quality. [96] In this chapter the two main aspects of this thesis, EU data protection law and concepts of privacy will be compared, and this comparison will be happening in a way that is defined in the latter definition of the verb compare.

Since privacy plays a big part in the EU data protection regulation, it would not be in the interest of this thesis to try and find major differences in the two since the hypothesis is that no such big differences would be found. Instead, it is beneficial to compare the two by finding out what is similar in them and also the possible differences between the two in case those are to be found.

4.1 Basics

There are many ways in how one could compare data protection and privacy. They could be seen as separate rights but also both complementary to each other, data protection could be seen as a subset to privacy or that the data protection is seen as an individual right that has a purpose to serve, among others, the right to privacy. [97] No matter from which point of view you compare the two it is evident that they both are similar rights and therefore complement each other. There is also need to separate data privacy and data protection from one another. Data protection contains the tools and policies that can be used to restrict the access to data whereas data privacy is the one that defines the operators who have access to the data. [98]

---

[96] Cambridge Dictionary (n.d. A). Comparing. Retrieved April 29, 2022, from https://dictionary.cambridge.org/dictionary/english/comparing

[97] Lynskey (2016): p.90

[98] Cloudian (n.d.). Data Protection and Privacy: 12 Ways to Protect User Data. Retrieved April 10, 2022, from

If data protection and privacy are seen as complementary rights, this means that they both serve the same common goal which would be to ensure that human dignity is ensured. [99] Data protection can be seen as the legal mechanism that is designed in order to ensure the right to privacy.

Privacy is a right that you voluntarily can give away. Having the GDPR does not make it so that you cannot give your personal data away at all. It just creates the guidelines as to which the operators who wish to benefit from your data or want to use it somehow need to follow and makes sure that you as an individual are informed about what and how your personal data is being handled. Therefore, data protection and privacy should not be seen as rights that exclude each other rather than something that complement each other. The concepts of privacy that are taken into account in the GDPR are there for a reason and still even with the data protection regulations there is need for legislation in privacy matters.

It can be argued that data protection is broader than just a modernized right to privacy that is brought to the modern, more digitalized, age. Data protection laws aim to protect individuals from their data being manipulated and the protection of this can be seen as something that goes beyond the right to privacy and should more be seen as a proactive right. Its proactive side shows in how it aims to give every individual the right to manage their own personal data. [100]

The fundamental and human rights concerning privacy can conflict with values such as the right to information and transparency in making decisions. [101] The conflict between the right to information comes in conflict between privacy and data protection so that personal data is regulated to cover a big area of all data, but it still leaves out some

---

https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
[99] Lynskey (2016): p. 94
[100] Lynskey (2016): p. 130
[101] Dörr & Weaver (2014): p.22

personal information that are not considered personal data. This is information that can't be traced back to an identified person but from the point of view of privacy, such data that is not considered personal could be considered private anyways.

4.2 The economic value of data

It is the collection and storage as well as disclosure of information that relates to private life that is in interference with the right to personal data protection. [102] It has been established previously that data protection legislation is needed because personal data needs to be stored and collected so that it can be used. In traditional privacy rights privacy is considered something that is kept a secret or something that is private to an individual. Personal data is something that has value to companies in different ways. Here it is considered for the economic value that it has.

As stated previously in this thesis, the economic value of data in short means that personal data can also be seen as a mean of payment. You become the product by providing the company your personal data in return to getting something from the company. The economic value of data is also the main reason in which data protection regulation needs to exist. It can also be seen as the main difference between the concepts of privacy in traditional human rights law and data protection.

If the data had no economic value, then companies would have the interest in it that they nowadays have. Personal data would not then also be the subject to criminal activity, at least not in a sense where someone would then sell the data onwards to a third party and therefore benefit from someone else's personal data. If it had no economic value, companies would not be interested in it and would not offer you their services free of charge in exchange to it. Conceptions of privacy in the traditional human rights law are

[102] Kokott, J. & Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Volume 3, Issue 4, November 2013, Pages 222–228, https://doi.org/10.1093/idpl/ipt017 p.224

more based on how individuals' privacy can be protected, and it does not focus much on personal data and how it can be protected while still being in ordinance with the legislation. What is also notable about personal data and privacy is that privacy in traditional human rights law is about the individual and considers every individuals privacy to be of equal value. Data protection legislation of course also value every individual's data the same but with personal data it is the quantity more than the quality. One individual's personal data doesn't make the need for the legislation rather than multiple personal data collected that are of relevance to each other.

For example, Google uses the economic value of data in their business. Most of the services Google provides look like they are free, and it seems that way to the consumer but actually how they are able to keep their services without cost is the data that individuals provide to the company. Another common quote that would be applicable when considering the economic value of data is "*There's no such thing as a free lunch*". This means that most of the times when a company is offering a service or an application or such for free, this means that they are wanting to benefit from you in some way.

4.3 Data invasion

There are multiple ways that personal data can be invaded. The invasion of privacy can happen for example via identity theft, stalking or trespassing. Identity theft is the most common way or at least the most well-known of the different options. Identity theft can lead to serious trouble for the individual who it is targeting. In comparing privacy and data protection law one could wonder how the data protection law answers to these questions of identity theft or other violations against individuals' privacy.

Privacy and data protection are something that are recognised as separate rights. These both rights have a vital meaning in having a sustainable democracy in Europe. [103] The difference between privacy and data protection is also the fact that privacy is more recognised as a human right while data protection is not. [104] This does not mean that data protection would not be recognised at all rather than it is not as widely recognised around the world as the right to privacy. There is growth in data protection legislation around the world and many of these can be seen as influenced by the GDPR. [105]

4.4 Freedom of speech

One thing that should be taken into consideration while talking about the GDPR and human rights is the freedom of speech and whether or not the GDPR might work against the freedom of speech. At first one could think that the GDPR is a good thing and has only positive side effects, but it could actually hinder freedom of speech. According to Reventlow EU states take their GDPR obligations seriously but the efforts on how to combine both data protection and freedom of speech have been uneven and that is making the GDPR compromise another important value, freedom of speech. [106] Privacy and freedom speech have been rights that have had tension between them even before the GDPR. Therefore, since privacy walks well hand in hand with the GDPR, it is only natural that the GDPR also has some tension between the right of having the freedom of speech. This has been seen in cases where it has been clear that data protection laws have been used in a way that is meant to silence or hinder those journalistic stories that are based on personal data. [107]

What is also closely attached to privacy and data protection is the right to be forgotten which means that if a person asks for their data to be removed this should be done. The

[103] European Data Protection Supervisor (n.d.)
[104] European Data Protection Supervisor (n.d.)
[105] European Data Protection Supervisor (n.d.)
[106] Reventlow, N. J. (2020) Can the GDPR and Freedom of Expression Coexist? AJIL Unbound 114:31-34 https://doi.org/10.1017/aju.2019.77 p.31
[107] Reventlow (2020): p. 31

only exception to this can be when erasing the personal data would compromise freedom of expression or the ability to research. [108] The collision with freedom of speech and data protection happens when considering whether or not an information is relevant for the processor to handle. With privacy this problem would not arise at this level because with privacy the problem with freedom of speech lies in what information is thought to be personal to an individual and what is not. Whereas nowadays with data protection regulation the aspect of relativeness comes to question, and it is easier to hinder the freedom of speech than in the privacy aspect of the case.

[108] European Commission (n.d.D)

5 In the future

According to Masse, in 2021 the GDPR had currently passed the settling phase and it was moving onto a phase that would determine whether or not the GDPR would turn out to be the success it was promised to be. [109] The success of the GDPR has an effect on citizens of the European Union but it can also have a bigger impact also in for example the United States of America and how data protection and privacy is handled in there. The more successful the GDPR is, the more successful is data protection seen in other parts of the world also. [110]

In order to look into the future and find out what kind of problems or issues the GDPR could face in the future, there is a need to look into the past and evaluate how the GDPR has been implemented and how successful this has been. The goal in this chapter is to evaluate what might be the problems in the GDPR also from privacy's perspective as well as in general. The main focus is on the problems that the Regulation might face in the future and how the GDPR would be able to answer them.

According to a report made by European Commission in the summer of 2020, the GDPR has been a success in its area and has met many of the expectations set for it. [111] There are some improvements mentioned that GDPR has already made after its implication. It has made the citizens of EU feel more empowered and they are more aware of the rights that they have. Because of GDPR, citizens are taking a more active role on their data and what is happening to it. [112] Being aware of the rights that you have increases privacy because you have the knowledge of what is information that you can lawfully keep to yourself and what in turn is the information that is not considered personal data and what could be collected of you.

---

[109] Accessnow (2021, May 25) GDPR: Three years in, and its future and success are still up in the air. Retrieved April 20, 2022 from https://www.accessnow.org/gdpr-three-years/
[110] Coos (2021)
[111] European Commission (2020, June 24) Two years of the GDPR: Questions and answers. Retrieved March 21, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166
[112] European Commission (2020)

Taking an active role in protecting your data and knowing what is happening to it, benefits not only the individual but also the whole society. As presented in the previous chapter, information breaches concerning personal data can affect many individuals and therefore the harm done can be significant in a much larger level. Having many citizens personal data breached and personal data such as social security numbers used in criminal activity can cause financial harm to the individual. Also having companies that are known for not complying to the GDPR causes harm to the company's image amongst other EU countries.

For businesses the GDPR has worked in favor of creating common ground rules and therefore helped to harmonize the framework for those companies that are operating in the EU. [113] Having common ground rules make it easier for businesses to know what is expected of them. Harmonizing regulation works in the businesses favor because they do not need to adopt multiple legislations of the same subject. They know that by complying to what the GDPR has stated, they are able to work lawfully in how they handle personal data.

Due to the economic value of data, there has already risen the need for operators that are designed to help people protect their rights. An example of these is MyData Global which is a non-profit association. Its goal is to combine the need of data that industries have with the digital human rights. The core idea is that there should be an easy way to be able to see where your personal data goes, who uses it and also easily alter these decisions. It aims to help and empower individuals so that in the future the digital society would be more fair and sustainable. One of its goals is also to create a more balanced relationship between the individuals whose personal data is being used and the organizations that use the individuals' personal data. [114]

---

[113] European Commission (2020)

[114] MyData (n.d.) How we operate. Retrieved May 26, 2022, from https://www.mydata.org/about/purposes-principles/

5.1 Differences in Member States

There seems to be some inconsistency between how the different Member States and their data protection authorities handle data protection. The main differences are on how much fines there were issued in different countries on the first three years. The biggest number of fines were issued in Italy, where the number was until 2021, 76 million euros. [115] This compared to for example previously mentioned fines in Finland that are in hundreds of thousands and not in millions. This of course also depends on the size of the country and the number of businesses that operate inside of it. Also, one could wonder if something would be to do with the different culture in the two example countries.

Since the GDPR is a legislation that was created to make the data protection law across Europe more unitary, there should not be big differences in how the Member States have implemented the regulation in each of their national laws. As has become clear in the thesis through previous chapters, privacy is a human right and therefore data protection, should be handled in a similar manner naturally all over the world but especially in all the Member States that it obliges.

5.2 Social media

Social media is and has been a growing phenomenon and with all the good that comes with it, comes also all the possibilities to do harm. One can wonder if there is a possibility to be able to identify all the cases which may be breaking GDPRs rules from all the thousands of posts floating in and to different social media platforms every day. Social media is a working platform for many people, and they don't always have a business behind

[115] Accessnow (2021): p.9

them, and they are not aware of how they should be taking GDPR into consideration in their work.

In the future there might be a need for a new stricter regulation regarding data protection especially when considering about individuals that are not part of a company but who still might operate as a processor or a controller. Many social media influencers have for example competitions in which their followers can take part in different ways. This occasionally means that they need to collect personal data such as email addresses or full names. The General Data Protection Regulation might need to specify their regulation so that it applies better to social media influencers also.

As brought up in a previous chapter, GDPR exempts purely personal and household activities and for example tagging your friend in a photo in social media or emailing them does not violate the GDPR even if you don't have the other person's consent. It is not considered that you are a controller. In the future there could be need for some clarification considering this aspect of GDPR as to who in fact can be considered a controller and how to differ the individuals who are considered controllers to the ones who are exempted due to personal and household activities.

5.3 Globalization

Globalization and the breaking of countries barriers, in a figurative sense, also brings up things to consider when talking about the GDPR. A lot of business work globally around the world and with the GDPR comes certain responsibilities even to countries not in the European Union but who work with customers within the EU. In article 3 of the GDPR it is defined that the Regulation applies "*to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*" as well as the processing of personal data of data subjects "*who are in the Union by a controller or processor not established in the Union*". In addition to the previously mentioned, the Regulation also

applies if the controller is "*not established in the Union, but in a place where Member State law applies by virtue of public international law*". [116]

One could wonder if there would be a need for a worldwide data protection law in the future or if something like that would even be possible. It would at least require years possibly decades of planning and counselling before it would be able to be implemented and taken into consideration in every country of the world. Difficulties in such a plan would be the different legislation in different countries. Inside the European Union, all the countries are fairly close to each other and there aren't big differences in how their legislation is compared to one another. Of course, belonging to the European Union is already a facture that is affecting so that all of the countries have a pretty similar way of thinking when it comes to legislation.

in the article 50 of the GDPR it is defined that the Commission and supervisory authorities need to take steps towards developing "*international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data*". [117] Therefore, it can be seen that the GDPR also takes into account the global aspect of data protection.

As said in the motivation chapter of introduction earlier in this study, the GDPR is a fairly new legislation, and it has the potential and also the need to grow in the future. The use of internet is only going to expand in the upcoming years, meaning that legislation will need to transform also.

5.4 Pandemic

The pandemic caused by the coronavirus that started in 2019 has tested the rights to data protection as well as to privacy. Since the coronavirus is by no means the last

[116] European Data Protection Regulation (2016/679) Article 3 (1-3)
[117] European Data Protection Regulation (2016/679) Article 50 (1a)

pandemic to happen during our lives the legislation trying to shield data protection and privacy needs to be up to date. [118] Since the epidemic is still ongoing, it is not yet fully clear whether the GDPR has been able to respond to the threats that have coming to its way.

The question regarding the GDPR and coronavirus is that how does health data match when considering about private data in general and whether or not it is allowed in the regulations sphere that health data and statistics of the individuals who have gotten sick are shared. Health data is something that is information about the individual regarding their health or disability as well as diseases and the treatment of those. Health data is considered to be a special category of personal data meaning that the protection of it also needs to be specific compared to personal data that is considered more basic.

Health data is mentioned in article 9 of the GDPR. It is defined that the processing of personal data that concerns health shall be prohibited. There are some exceptions mentioned in the paragraph 2 of said article. For example, in case the "*processing is necessary for reasons of public interest in the area of public health such as protecting against serious cross-border threats to health*" [119] it is considered that the processing of such personal data containing health data would not be prohibited.

The questions regarding health data during the epidemic can be such as if it is possible for an employer to share that a co-worker has gotten sick and maybe infected colleagues or that are the statistics that are being shared of the virus every day on the news and every possible media action that are against the regulation in the GDPR. According to Office of the Data Protection Ombudsman, starting with the latter question, it is possible to share statistics and health data about the virus if said data is anonymous so that no

[118] Smith, J. (2021, December 16) Q&A: Future pandemics are inevitable, but we can reduce the risk. European Commission. Horizon. The EU Research & Innovation Magazine. Retrieved March 17, 2022, from https://ec.europa.eu/research-and-innovation/en/horizon-magazine/qa-future-pandemics-are-inevitable-we-can-reduce-risk

[119] General Data Protection Regulation (2016/679): Article 9 (2)(i)

individuals can be identified based on it. If the data can be identified by combining it with other information, this kind of data can't be shared without the permit of said individuals. An employer on the other hand is not allowed to inform the sickness of their employee by naming the employee who has gotten sick. It is however allowed that the employer informs of the infection without naming the individual it is about. Processing the health data of employees is subjected to confidentiality. [120]

5.5 Smart watches and other devices that use tracking

First there were computers, then mobile phones, then smart phones and nowadays technology is so evolved that nearly every device we have is connected to the internet and in many cases also tracks our everyday movements. There are smart watches, smart rings, fitness bracelets, chips that you can put in your shoes and even data glasses. These can be grouped together as wearable computing devices meaning that they are worn on your body and the small sensors in them track for example your physical activity or other aspects. [121]

A lot of people are interested in finding out what their performance is and what can be found out about their health through different devices. What one probably does not come to think of is all the details these devices collect of us. Take for example a smart watch. It is used around the clock every day of every week and it tracks us even when we are sleeping. Therefore, the amount of data it collects of us is large. For a company to get a hold of this many data would be beneficial for them.

For example, one's health data would be very important to insurance companies. Some insurance companies have already offered rewards to those of its members who provide

[120] Office of the Data Protection Ombudsman. (n.d. B) Frequently asked questions on data protection and the coronavirus. Retrieved April 2, 2022, from https://tietosuoja.fi/en/coronavirus-covid-19
[121] Petermeier, D. (2020, February 18th) How the Wearable Market Deals With Sensitive Data. Wearables and Data Protection – What Providers Know About You. Retrieved April 22, 2022 from https://www.ispo.com/en/trends/wearables-and-data-protection-what-providers-know-about-you

their data to said insurance company. [122] In this aspect it would seem for the individual that they are benefitting from the discount they have gotten more than the insurance company of the data, but it is actually the other way around. The data provided to the insurance company is worth a lot more than the discount that they are giving to their customers. This makes sense, because insurance companies are doing business too and it is in their interest to make profit with their business.

If technology keeps evolving with the same speed that it is now evolving, only time can tell what kind of wearables will be invented or introduced to the market in the next twenty or even ten years. There has been talk of sensors in clothing and sensors that could detect diseases or work as a prevention of them. [123] Positioning data is considered to be personal data therefore this data coming from wearables is subjected to obey the GDPR. Patient records are also considered personal data, but calorie consumption or blood pressure are not information that could necessarily be traced back to an identified person. In the future one could wonder if the General Data Protection Regulation would benefit from some additions to it regarding for example health data.

[122] Petermeier (2020)
[123] Petermeier (2020)

6 Conclusions

"Personal data is the new oil of the Internet and the new currency of the digital world." [124]

This final chapter of the thesis begins with a quote from Meglena Kuvena in 2009. The quote emphasises the economic value of data by comparing it to oil of the Internet meaning that similar to oil, data by itself is not considered valuable but it is the connection and gathering of data to other relevant data that makes it valuable. The new currency references in turn means that data has become a mean of payment in the digital world. You are able to get services or even products by handing your personal data as payment.

In this thesis the aim was to find out if the economic value of data is the main distinction between the right to personal data protection and the right to privacy. The thesis began by defining the basics of the EU data protection law, main focus being on the General Data Protection Regulation because that is the most important piece of legislation when considering data protection inside the EU. Alongside with the basics it was also presented what was the history behind the regulation, what was the need for it to be made, how it has been implemented and what it means for businesses. This point of view was chosen because the thesis is made from business law's angle and the understanding of how companies are affected by such regulation is important in the field of business and as a future expert of business law. Then the thesis moved on to presenting privacy as a concept first in general and then more detail in different legislations as well as more detailed in the Finnish legislation. This chapter also presented some legal cases in the Finnish legislation that were connected to the GDPR. Fourth actual chapter in the thesis was about the comparison of privacy and data protection. No major differences were

[124] Meglena Kuneva as a keynote speeker at Roundtable on Online Data Collection, Targeting and Profiling in Brussels on March 31st, 2009.

found between the two aspects therefore instead of a black and white comparison the chapter more tried to explain how the two come together and also presented the possible differences the two had. In a field that is as changing as data protection, the fifth chapter was brought in the thesis to present and make assumptions about how the data protection and privacy could be in the future and what kind of problems they might face.

6.1 Answering the research question

The research question was presented in the beginning of the thesis. The research question is as follows:

Is the economic value of data the main distinction between the right to personal data protection and right to privacy?

In this thesis it has been found that the EU data protection law compares quite well to personal data protection and what it craves in order for it to be protected. As expected, the economic value is what makes the main distinction between the right to privacy and the right to personal data protection. If the data had no economic value there would not be the need for the legislation of personal data protection, at least not in the extent that it is now.

An aspect that is also taken into account in this thesis is privacy. Privacy is something that should not be seen as an individual right rather than something that has value for the whole community. The same could be said about the General Data Protection Regulation also. It aims to give all citizens of European Union the same rights when it comes to their data protection. Therefore, it is a regulation that aims to protect the individual but at the same time has a goal to service a bigger community as well.

6.2 Further study ideas

Because this is more of a literature review rather than an actual study, this thesis should be considered as a broad introduction into the GDPR and the economic value of data as well as how data protection is seen from the businesses point of view. A literature review comes with limitations. The main point of this thesis was not to find out anything new or spectacular rather than by combining different sources find out if the economic value of data makes the main difference between concepts of privacy and personal data protection. The word count gave its own restrictions and therefore while writing this thesis some broader aspects of how the EU data protection law as well as privacy could further studied came to mind.

Some ideas for a broader more specific study into the matter could be studying how the GDPR is known in different European Union Member States, how it has been implemented and if it has proven to be useful or not. This could be done by collecting data, minding the GDPR regulation of course, by interviewing both registered people and those who register them in different countries. This could give an insight on how for example cultural differences such as East-Europe compared to West-Europe has an effect on the GDPR and its implementation or whether or not they have an effect at all.

Since it has been proven that there are some differences in between how the Member States handle the GDPR in their legislation, the hypotheses is that a study of that sort would bring interesting new findings and could benefit in making the GDPR legislation more homogeneous and thus making the data protection and privacy around the European Union more equitable.

As this thesis is being written, Covid-19 epidemic is still ongoing and has been for two years already. In addition to the epidemic, there is also a war in Ukraine going on right now. It is interesting to see how these two crises affect the GDPR and is the legislation up to date in a way that when the whole world's attention is on something other than data protection, individuals' data is still protected and not used in a criminal way. It is a

sad truth that this is probably only the beginning with epidemics and nature crisis so this could also be an interesting subject to look into in the future and also wonder if there would be something that needs to be changed in the GDPR.

We are in a forever changing world and with a playground so quickly changing as data and technology as well as internet in general, the regulation also needs to be up to date. Privacy as a concept is something that has been a concept for the humankind a long time, but the new changing world has subjected even the strongest of rights to change. Privacy as a right in itself does not change but the circumstances affecting it do and how privacy can be balanced with other human rights.

Criminals are always coming up with new ways to profit from other individuals and therefore as the new ways come up, also new legislation needs to. Technology evolves as well as the ways in which personal data can be utilized.

6.3 Finally

In conclusion it can be said through the research done in order to write this thesis and with the information collected from the various sources that the economic value of data is the reason why such legislation needs to exist, and it is the most important reason as to why companies need to obey the General Data Protection Regulation in their everyday operations.

As stated in the previous chapter, there have already risen operators such as MyData, who aim to help individuals in enhancing their own personal data and being more in control of how their data is being used. This shows that personal data is something that is seen in a high value to individuals, and it has also been recognized as an asset for companies. Data processing is a big part of many companies' operation nowadays and therefore it is important that there is legislation on it. This supports not only the individuals by protecting their personal data from being used in an unlawful way but also the

companies by giving them the guidelines to follow when processing personal data. As has been stated in this thesis, the GDPR does cause additional work to the companies but once it has been implemented, it brings the company also benefits through for example their customers being able to trust the companies more and know that they are working in a way that is compliant with the Regulation.

As someone making research, it would be desirable to find something new and groundbreaking. This was obviously not the case with this study. However, this result is quite optimal when thinking about it from the individuals, the lawmakers or a company's point of view. The fact that concepts of personal data protection are well taken into account in EU data protection law means that the GDPR has achieved the goals that were primary set to it although it has at the same time faced some challenges. As stated, multiple times through the course of this thesis, privacy is an important right, and it should be treated as one. EU data protection law at its core is all about protecting personal data and that is something that is considered to be private to individuals. Because the EU data protection law is something that impinge on a lot of people and since the very basic core of personal data protection comes from the right to privacy, it is understandable that such legislation is done in a matter that is serving to the concepts of privacy.

It might seem that having no big revelations or finding no big differences would lead to not having any actual results from making the study. However, finding no concrete results should also be seen as a result. The hypotheses before starting to research this subject was that economic value of data would be the main distinction between privacy and data protection. This hypothesis came true since one of the few differences between the two was based on economic value of data and how without it, data protection would not even be needed in the width that it is now.

Even though it feels like technology has already developed a lot and in all honesty, it really has, it is still the truth that we are only now seeing the beginning of how personal data can be used and how it should be legislated. With every new invention and every

new company, the borders of both privacy and data protection regulation expand a little bit. As the world evolves more and more, there are still some basic rights that remain, and privacy is surely one of the strongest ones. Therefore, we can have faith that in the future also the data protection will be done as it is nowadays, with having personal data and the protection of it strongly as a starting point.

References

Articles

Cohen, J. E. (2013, May 20). What Privacy Is for. *Harvard Law Review*, 126(7), 1904–1933. https://harvardlawreview.org/2013/05/what-privacy-is-for/

Dörr, D. & Weaver, R. (2014). *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries.* Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110338195

Gruschka, N., Jensen, M., Mavroeidis, V. & Vishi, K. (2018) *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*. https://arxiv.org/pdf/1811.08531.pdf

Hoofnagle, C., Van der Sloot, B. & Borgesius, F. (2019) The European Union general data protection regulation: what it is and what it means, *Information & Communications Technology Law;* 28(1), 65-98, DOI: https://doi.org/10.1080/13600834.2019.1573501

Hughes, K. (2012, September 13) A Behavioural Understanding of Privacy and its Implications for Privacy Law. *The Modern Law Review*. 75(5) p. 806-836. [Resticted availability] https://doi-org.proxy.uwasa.fi/10.1111/j.1468-2230.2012.00925.x

Kocarev, L. & Sokolovska, A. (2018, June 5) Integrating Technical and Legal Concepts of Privacy. *IEEE Access*, vol.6. pp.26543-26557, 2018, DOI: 10.1109/ACCESS.2018.2836184

Kokott, J. & Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law,*

Volume 3, Issue 4, November 2013, Pages 222–228, https://doi.org/10.1093/idpl/ipt017

Raitio, J. (2012) *The Source of Law – Doctrine and Reasoning in Finland. US-China Education Review B 11.* Retrieved from: https://helda.helsinki.fi/bitstream/handle/10138/42078/Raitio_Source_of_Law_Doctrine_and_Reasoning_in_Finland.pdf?sequence=2

Reventlow, N. J. (2020) Can the GDPR and Freedom of Expression Coexist? *AJIL Unbound* 114:31-34 https://doi.org/10.1017/aju.2019.77

Sankari, V. & Wiberg, M. (2019) GDPR ei toimi: Tietosuojakäytännöt eivät noudata asetusta. *Yhteiskuntapolitiikka* 84 (2019): 3. https://www.julkari.fi/bitstream/handle/10024/138277/YP1903_Sankari%26Wiberg.pdf?sequence=2&isAllowed=y

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

Viljanen, J. (n.d.) *The European Convention on Human Rights and the Transformation of the Finnish Fundamental Rights System: The Model of Intepretative Harmonisation and Interaction*. Retrieved March 4, 2022, from https://www.scandinavianlaw.se/pdf/52-16.pdf

Books

Aveyard, H. (2010). *Doing a literature review in health and social care : A practical guide.* McGraw-Hill Education.

Larsson, A. & Lilja, P. (2019) GDPR What are the risks and who benefits? in Larsson, A. & Teigland, R. (Ed.) *The Digital Transformation of Labor*. Routledge.

Lynskey, O. (2016). *The foundations of eu data protection law.* Oxford University Press.

Oliver, P. (2012). *Succeeding with your literature review: A handbook for students.* McGraw-Hill Education.

Saarenpää, A. (2015). *Henkilö- ja persoonallisuusoikeus.* In: Oikeus tänään. Part II, pages 203-430. 3.revised, 2015. Ed. Marja-Leena Niemi. Rovaniemi: University of Lapland.

Taylor, M. (2012) *Genetic data and the law: A critical perspective on privacy protection.* Cambridge University Press.

Internet Sources

Accessnow (2021, May 25) GDPR: Three years in, and its future and success are still up in the air. Retrieved April 20, 2022 from https://www.accessnow.org/gdpr-three-years/

Asaolu, H. (2020, March 16) GDPR Compliance Implementation: all the requirements and things to do. Retrieved April 13, 2022 from: https://leadsbridge.com/blog/gdpr-compliance-implementation-for-dummies-all-the-requirements-and-things-to-do/

Cambridge Dictionary (n.d. A). *Comparing.* Retrieved April 29, 2022, from https://dictionary.cambridge.org/dictionary/english/comparing

Cambridge Dictionary (n.d. B). *Privacy.* Retrieved April 20, 2022, from https://dictionary.cambridge.org/dictionary/english/privacy

China Briefing (2021, August 24) *THE PRC Personal Information Protection Law (Final): A Full Translation.* Retrieved March 15, 2022 from https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

Cloudian (n.d.). *Data Protection and Privacy: 12 Ways to Protect User Data*. Retrieved April 10, 2022, from https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

Coos, A. (2021, April 23) *EU vs US: What Are the Differences Between Their Data Privacy Laws.* Retrieved March 19, 2022, from https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/

DigWatch (n.d.). *Privacy and data protection*. Retrieved April 12, 2022, from https://dig.watch/topics/privacy-and-data-protection

Edwards, J. (2021, January 14) *6 business benefits of data protection and GDPR compliance.* Retrieved April 15, 2022, from https://www.techtarget.com/searchdatabackup/tip/6-business-benefits-of-data-protection-and-GDPR-compliance

Equality and Human Rights Commission (n.d.A) . *International Covenant on Civil and Political Rights (ICCPR).* Retrieved March 15, 2022 from https://www.equalityhumanrights.com/en/our-human-rights-work/monitoring-and-promoting-un-treaties/international-covenant-civil-and

Equality and Human Rights Commission (n.d. B) What is the Charter of Fundamental Rights of the European Union? Retrieved May 22, 2022 from https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union

European Commission (n.d.A). *What is personal data?* Retrieved March 15, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Commission (n.d.B). *What is data controller or data processor?* Retrieved March 15, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

European Commission (n.d.C). *Eu funding supporting the implementation of the General Data Protection Regulation (GDPR).* Retrieved March 15, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

European Commission (n.d.D). *Data protection – Better rules for small business.* Retrieved March 17, 2022, from https://ec.europa.eu/justice/smedataprotect/index_en.htm

European Commission (n.d. E). *Data protection in the EU.* Retrieved March 17, 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Commission (2020, June 24) *Two years of the GDPR: Questions and answers.* Retrieved March 21, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166

European Court of Human Rights (n.d.). *European Convention on Human Rights.* Retrieved April 2, 2022, from https://www.echr.coe.int/documents/convention_eng.pdf

European Data Protection Supervisor (n.d.) *Data Protection.* Retrieved March 30, 2022, fromhttps://edps.europa.eu/data-protection/data-protection_en#Interaction

European Union (n.d.) *Facts and figures on life in the European Union* Retrieved March 30, 2022 from https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en

Gunathunga, S. (2017, September 11). *Individual's rights under GPR.* Retrieved February, 28, 2022 from https://sagarag.medium.com/individuals-rights-under-gdpr-3256fb3f356c

Hofmann, P., Kiyomoto, S., Nakamura, T., Serna, J. & Tesfay W.B. (2018) *PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation* Retrieved March 29, 2022, from https://www.researchgate.net/profile/Shinsaku-Kiyomoto/publication/323787516_PrivacyGuide_Towards_an_Implementation_of_the_EU_GDPR_on_Internet_Privacy_Policy_Evaluation/links/5b3ebbb3aca272078519c3fa/PrivacyGuide-Towards-an-Implementation-of-the-EU-GDPR-on-Internet-Privacy-Policy-Evaluation.pdf

Ikävalko, K. (2021, December 16) Tietosuojavaltuutettu määräsi Psykoterapiakeskus Vastaamolle 600 000 euron seuraamusmaksun erittäin vakavista tietoturvallisuuspuutteista. *Yle.* Retrieved March 30, 2022, from https://yle.fi/uutiset/3-12232962

Kuneva, M. (2009, March 31) *European Consumer Commisioner. Keynote Speech. Roundable on Online Data Collection, Targeting and Profiling*. Retrieved April 30, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156

Lord, N. (2018, September 12) *What is the Data Protection Directive? The Predecessor to the GDPR*. Retrieved March 2, 2022, from https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr

Ministry of Justice Finland (n.d.) *Constitution.* Retrieved March 11, 2022, from https://oikeusministerio.fi/en/constitution-of-finland

MyData (n.d.) *How we operate.* Retrieved May 26, 2022, from https://www.mydata.org/about/purposes-principles/

Nieminen, J. (2019, August 22). Emilia Laurila, 25, halusi selvittää, mitä tietoja hänestä on kerätty – paljastui hämmentävän tarkkaa raportointia ja yllättäen tuhottuja tietoja. *Yle.* Retrieved March 13, 2022, from: https://yle.fi/aihe/artikkeli/2019/08/22/emilia-laurila-25-halusi-selvittaa-mita-tietoja-hanesta-on-keratty-paljastui

Niinistö, M. (2020,October 27). Mistä tiedän onko tietoni vuodettu? Uskaltaako terapiassa enää puhua? Haimme vastaukset 31 kysymykseen Vastaamon tietomurrosta. *Yle.* Retrieved April 2, 2022, from: https://yle.fi/uutiset/3-11615408

Office of the Australian Information Commissioner (n.d.). *The Privacy Act. Australian Government.* Retrieved April 9, 2022 from https://www.oaic.gov.au/privacy/the-privacy-act

Office of the Data Protection Ombudsman (n.d. A). *What is personal data?* Retrieved March 15, 2022, from https://tietosuoja.fi/en/what-is-personal-data

Office of the Data Protection Ombudsman. (2020, May 22nd) *Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations.* Retrieved March 4, 2022, from https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista?languageId=en_US

Office of the Data Protection Ombudsman. (n.d. B) *Frequently asked questions on data protection and the coronavirus.* Retrieved April 2, 2022, from https://tietosuoja.fi/en/coronavirus-covid-19

Pietarinen, H. (2021, September 10th) Parkkipate ja Posti saivat kymmenienthuansien eurojen gdpr-sakot, joita suomalaisyrityksille on tulossa lisää. Helsingin Sanomat. Retrieved March 4, 2022, from https://www.hs.fi/talous/art-2000008247280.html

Petermeier, D. (2020, February 18th) *How the Wearable Market Deals With Sensitive Data. Wearables and Data Protection – What Providers Know About You.* Retrieved April 22, 2022 from https://www.ispo.com/en/trends/wearables-and-data-protection-what-providers-know-about-you

Smith, J. (2021, December 16) Q&A: Future pandemics are inevitable, but we can reduce the risk. European Commission. Horizon. *The EU Research & Innovation Magazine.* Retrieved March 17, 2022, from https://ec.europa.eu/research-and-

innovation/en/horizon-magazine/qa-future-pandemics-are-inevitable-we-can-reduce-risk

Tarnoff, B. (2016, July 15) How the internet was invented. *The Guardian.* Retrieved March 23, 2022, fromhttps://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf

United Nations (n.d.A) *Universal Declaration of Human Rights*. Retrieved April 2, 2022 from https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations (n.d.B) *Member States* Retrieved March 13, 2022 from https://www.un.org/en/about-us/member-states

United Nations Conference on Trade and Development (n.d.) *Data Protection and Privacy Legislation Worldwide.* Retrieved March 13, 2022, from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Wall Street Journal. (2018, May 21) *GDPR: What Is It and How Might It Affect You?* [Video]. Youtube. Retrieved February 21, 2022, from https://www.youtube.com/watch?v=j6wwBqfSk-o

White & Case (2019, November 13) *GDPR Guide to National Implementation: Finland.* Retrieved March 3, 2022, from https://www.whitecase.com/publications/article/gdpr-guide-national-implementation-finland

Wolford, B. (n.d.) *What are the GDPR Fines?* Retrieved April 14, 2022, from: https://gdpr.eu/fines/

Legal Sources

Finland

Act on the Protection of Privacy in Working Life 13.08.2004/759

Constitution of Finland 11.06.1999/731

Data Protection Act 05.12.2018/1050

Personal Data Act 22.04.1999/523

USA

Federal Information Security Modenization Act

Health Insurance Portability and Accountability Act

Australia

Privacy Act 1988

China

Personal Information Protection Law

EU and International Law and Regulation

The Charter of Fundamental Rights of the European Union (2012/C326/02)

The Data Protection Directive

The European Convention on Human Rights

General Data Protection Regulation (2016/679)

International Covenant on Civil and Political Rights

The Universal Declaration of Human Rights

Cases

Supreme Court

10.06.2015 File copy 1165 KKO 2015: 41 p.45

Supreme Administrative Court

17.8. 2018 File copy 3774 KHO:2018:112 p. 44-45