GDPR and European Healthcare Insurance – A PESTLE analysis

Master Thesis

Han Yong Cho
CPR: 130683-3169

MSc International Business and Politics
Number of Pages: 51
Number of STUs: 79.999
Hand-in: 15 January 2018

Supervisor: Mikkel Flyverbom, Department of Management, Society and Communication, CBS

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Preface

The research for this paper originally began as a partnership between Niklas Hedegaard and myself. We are both MSc. IBP students and had previously partnered together to write the bachelor thesis, with very satisfactory results.

A couple of weeks before we began the research process my mother, unfortunately, were diagnosed with cancer that would overcloud the process. Although my mother is currently making a recovery, the partnership, unfortunately fell apart, as I found it very difficult to deliver the work needed to meet our deadlines. As so, much of the empirical material, interviews, sources and ideas were jointly discovered and/or produced. The original intent of the paper was to investigate how the micro- and macroeconomics factors of EUs General Data Protection Regulation would affect the competitive structure of European life and health insurance in relations to the technological paradigm shift. As the partnership is no longer intact, the scope of the paper has been redefined. The paper will investigate how the European health insurance industry can leverage the EUs General Data Protection Regulation by performing a macroeconomic analysis of the industry.

1. Table of Content

1.2. List of Acronyms

ACTA The Anti-Counterfeiting Trade Agreement

Art. 29 WP Article 29 Working Party

DPA Data Protection Authorities

DPO Data Protection Officer

EDPB The European Data Protection Board

EIOPA The European Insurance and Occupational Pensions Authority

EU European Union

FRA The European Union Agency for Fundamental Freedoms

GDPR General Data Protection Regulation

IAIGs Internationally Active Insurers Group

OECD Organization for Economic Co-operation and Development

PESTLE Political, Economical, Social, Technological, Legal & Environmental/Ecological

PHI Private Health Insurance

SOPA Stop Online Privacy Act

TEU Treaty on European Union

TFEU Treaty on the Functioning of the European Union

1.3. List of Tables & Figures

2. Executive Summary

As our society becomes more and more digitized, we are spending more and more of our time with our noses glued to the smartphone, checking Facebook, shopping online, or just staying connected with our Fitbit. All of these activities send massive amount of data back to the companies were we, as consumers have no control over how it is used, stored or sold.

February 2015, Anthem, one the largest health insurance companies in the US reported that it had been hacked. The hackers got access to 79 million customer personal information. After being sued, Anthem agreed to pay a record breaking $115 million USD, the largest ever for a data breach to date (Pierson, 2017).

This paper examines the impact of EU's General Data Protection Regulation on the European health industry. Particular it looks at the regulatory barriers that are normally associated with the introduction of such legislation across so many countries, and takes the opposite view by examining the business opportunities within the legislation. Specifically it looks at the rights that have awarded to EU denizens, and how the rights may be used as a competitive advantage to increase market share and retain customers. It does this by performing a PESTLE analysis on the EU health insurance industry in the context of the GDPR.

Keywords: GDPR, Insurance, EU, E-business, Hacking, Privacy, Health, Data breach, Cyber security, Technology, On-demand economy

3. Introduction

In 1965, Gordon Moore made an observation that the number of transistors in a circuit doubled each year. A decade later he revised the forecast to it doubling every two years and defined what we later would be known as *"Moore's Law"* (Moore, 1975). Today the Nvidia Tesla V100 computer processer has 21.1 billion transistors, from around 2,300 transistors in the 70's. While Moore's law only describes the physical aspects of the technological advancements, the software components have seen a similar exponential growth. Today, as society and the economy increasingly becomes more digitized with smartphones, tablet computers and other smart devices such as the smart watch that tracks your every movement, monitors you sleeping habits to your smart-refrigerator that can tell you when you milk has gone bad. We have an unprecedented amount of software and algorithms running 24/7 to run all these devices. Likewise, the amount of data produced by these devices is unprecedented and more and more companies and organisations hold personal and sensitive data on their customers, clients and employees, were the data is increasingly being used to track our behaviour and preferences, creating value for businesses i.e. marketing and insurance. Wearable devices such as the smart-watch, Fitbit and other health and fitness trackers are not only able to monitor our physical health, but are able to monitor our mental health as well by linking our behaviour, conditions and geo-location data (Palmer, 2016). The rapid technological developments in convenience technology, wearables and the constant online present has changed consumer behaviour, and the consumers are putting more and more pressure on firms to deliver products and services faster at a cheaper cost. The constant online present, and convenience does not come lightly, nor cheaply. Often consumers give up their privacy and the data they produce, going about their day, are often processed and sold without their knowledge or consent.

In September 2016, an online news website, Motherboard, reported that Brazzers, a porn site was hacked and nearly 800,000 accounts were exposed (BBC NEWS, 2016; Cox, 2016). Although the website in question might put a smile on your face, the issues at stake were much more serious then just some embarrassed users. Hacking has given birth to a multibillion hacking industry estimated to cost the global economy around 445 billion USD in 2016 (H. Taylor, 2016). By comparison Denmark, which is considered one of the most developed, and advanced economies in the world had a GDP of around 301 billion USD in 2015 (World Bank, 2017). Although the news of the breach surfaced in 2016, according to Matt Stevens, a public relations manager at Brazzers, the breach happened in 2012/13 (BBC NEWS, 2016; Cox, 2016). Unfortunately breaches and slow reactions to them are not only reserved to the online adult entertainment business. In early September 2017, Equifax, one of the biggest consumer credit reporting agencies in America, reported that it had a cyber security breach involving more then 143 million US customers, one of the biggest data breaches in history (CBS/AP, 2017; Haselton, 2017; Roberts, 2017). Although the story broke in the beginning of September of 2017, on September 18th Bloomberg reported that Equifax had another cyber security breach happen in March of the same year, five month earlier then the initial breach that exposed the 143 million clients. Although the March breach did not result in any loss of customer data, a company spoke person stated that it was the same group of hackers in both cases (CBS/AP, 2017; Riley, Sharpe, & Robertson, 2017).

The rapid development in technology and increasing adaptation of the Internet by organizations, hackers, and state actors has led ordinary people vulnerable not only to the hackers but to the predatory behaviour from for-profit organizations, and foreign-state intelligence services alike. While the malicious intend could be expected from hackers, the predatory behaviour from for-profit organizations has led the EU to revise its privacy

and data protection legislation. After many years of consultations and negotiations the Article 29 Working Party, which is the EU Commission's data privacy advisory body, presented the General Data Protection Regulation (GDPR). The GDPR will come into effect on the 25th of May 2018, and is an attempt by the EU to harmonize privacy and data protection legislation across member states, to ensure the free movement of data in the single market, and to ensure the fundamental rights to privacy of its citizens by creating one legislation that covers the whole of the EU. The GDPR will require organisations to review its IT-Infrastructure, and create new IT-governance structures and policies. It will challenge how organisations view privacy, handle personal data, deal with security breaches, and notify on breaches when they occur in a timely fashion. The GDPR also introduces a wide range of requirements and obligations for organisations and gives individuals more rights to their own data. The penalty for non-compliance can be up to €20 million or 4% of global turnover, which ever is greater, at a group level. The threat of crippling fines has dominated many organisations resources as they scramble to try to get theirs house in order before the deadline.

3.1. Research Question

Considering how the GDPR will affect how organisations view IT, privacy and personal data. This paper will investigate how the European health insurance industry can leverage the new legislation to remain competitive in society today. The paper will do this by answering the following research question:

Considering the regulatory challenges of EUs General Data Protection Regulation, how will the creation of the individual rights affect the use of data within the insurance industry? And what business opportunities within the industry can we identify using the PESTLE framework?

3.2. Scope & Delimitation

The aim of this section is to give a description of the scope of the paper. Although there are many, many different categories of insurance available in the market today such as commercial, life, agricultural, auto insurance, and so on. To narrow the scope of the paper and due to practical considerations the paper will focus on the aspects of health insurance within the EU in relation to the GDPR.

As stated in the preface, this research started as a partnership where the scope of the paper dealt with both the life and health sector of the insurance industry in Europe. For practical reasons and to focus the research, the focus of the paper was narrowed to only cover the health sector of the insurance industry in the EU. The paper focuses on the GDPR as our society is transforming into a digitized one. Considering the penalties and scope of the GDPR, it is expected that the GDPR will have a huge impact not only for how businesses treat privacy and personal data, but possibly how individuals and society as a whole can reclaim ownership and use their own data.

The insurance industry was chosen as initial investigations showed that the industry is heavily reliant on data about their clients such as where they lived, age, marital status, health status and so on. Meaning that the GDPR would affect the core business of the industry. The European health insurance industry was chosen, as it offers more complexity, then life insurance. These complexities arise from the nature of the different healthcare systems we find across the EU. Although a EU citizens from one member state has access to the healthcare system of another member state. The system is far from well implemented and easy to use, as almost all of the member states have different and unique healthcare systems, with some offering a taxpayer funded universal healthcare, while

others have more complicated systems were they utilize a mix of taxpayer, self and employer funded healthcare systems (Gold, 2011; Sagan & Thomson, 2016).

3.3. Structure and Outline of the Paper

The aim of this section is to give an overview of the structure and outline. The paper is structured as follows: This chapter introduces the topics, provides the context in which it is presented and provides the research question of the paper. It then gives the scope and delimitations of the paper, before moving on to the definitions of terms used in this paper that is designed to assist the reader by explaining the terminology used.

In chapter four, the methodology of the paper will be introduced, as well as the approach and philosophical stance of the paper. It will also touch upon the research design and literature review, before moving onto the theoretical and analytical framework used in the paper will be developed.
In chapter five, the paper will give a brief introduction to the insurance industry and the technological developments that might influence the industry. It will then give a short background and history of privacy and data protection, before introducing the GDPR, the principles and the rights.

In chapter six, the paper will link the theoretical and analytical framework presented in chapter four with the GDPR and empirical evidence collected throughout the paper.

Chapter seven will discuss some of the elements analysis in chapter six, before ending the paper with concluding remarks in chapter eight.

3.4 Definition of key terms

The aim of this section is to clarify the terminology used in this paper, and will act as a guide throughout the paper.

Controller (Data)	A natural or legal person, public authority, agency that determines the purposes and means of processing personal data
Data Subject	A living individual to whom personal data relates
InsurTech	Is a mix of insurance and technology. The term is used for technological innovations that are designed to optimize the current insurance business model
Legal Person	A private or public organisation with legal right
Natural Person	An individual, human being
On-demand Economy	An economic activity created by the digital marketplace that immediately fulfils consumer provisioning of goods and services
Personal Data	Any information relating to an identified or identifiable natural person (Data Subject)
Premium	A premium (Insurance) is the amount of money an individual must pay for an insurance policy
Processing	Any operation performed on personal data, whether automated or not including collection, recording, structuring storage and so on

Processor (Data) A natural or legal person, public authority, agency that processes personal data

Sensitive Data Any data concerning racial or ethnic origin, political opinion, religious beliefs, trade union activities, physical and mental health, sexual orientation or criminal offences

4. Methodology

The aim of this section is to give an overview of the methodology used in this paper by discussing the philosophical stance in which the data was gathered and the research approach employed in the paper. In addition the section will also present the limitations of methods used, specifically the use of qualitative data in relations to the interviews and secondary data collection, which is a mix of articles and journals.

Since the purpose of this paper is to investigate how the health insurance industry in the EU can leverage its business opportunities within the new legislation, the paper will utilize a mix of descriptive and explorative approaches (Abott, 2004; Saunders, Lewis, & Thornhill, 2012).

4.1. Approach and Philosophy

In order to analyse the thematical issues the paper will adopt a critical realist research philosophy. The aim of the paper is to investigate how the health insurance industry within the EU will be impacted by the GDPR. As the GDPR is not in effect yet, the paper will have to look at trends in society i.e. online data, and qualitatively assess the result to predict future trends. The research will therefore be guided by the need to interpret both the quantitative and qualitative data. Critical realism

encourages us to reflect on the concepts in which interpret the world. Critical realism is also useful to identify multiple perspectives in line with the PESTLE framework that will be applied in this paper (Gorski, 2013). The paper will take an inductive approach, as the approach allows us to explore and develop a theory whilst researching the paper(Saunders et al., 2012). The research will therefore start by observing the GDPR and actors within EU health insurance industry before developing a theory that fits (Ibid).

4.2. Research Design

The aim of this section is to describe the research process, and which frameworks, and considerations has been led to the methodology. As mentioned in the previous section this paper will use a mix of explorative and descriptive methods. The paper will begin the research by taking an explorative method when interviewing insurance professionals and experts. The explorative nature of the studies allows use to ask broad open-ended questions to the experts, before narrowing the research. The descriptive nature of the study allows it to be utilized after the interviews have been concluded, to gain a more accurate and focused research (ibid).

4.2.1. Data Collection

As a mix-method will be taken, the data for this research was collected in several ways.

Firstly, qualitative data was collected through interviews and researching academic papers, professional reports and through online sources, such as newspapers and journals. The data collection technique used for the interviews was a semi-structured one. This collection method allows the interviewer to have broad open-ended questions, allowing the interview to

naturally take shape (Ibid). Two interviews where held. One with a senior management consultant at the consultancy firm EY, and one with two insurance practitioners from the TopDanmark Insurance. One of the interviews was recorded, but as the interviews acted as a guide to narrow the research the interviews have not been transcribed.

Secondly, on the basis of the qualitative data collected through the interviews and desk research. A quantitative research was initiated to validate and confirm the assumptions made during the qualitative research period (Ibid).

4.3. Literature Review

The aim of this section is to review and give an account of the academic literature used in this paper. The GDPR will come into effect from May 2018, and many organizations are just realizing the inevitable deadline is creeping up. As so there is a lot of hype regarding the penalties associated with non-compliance, especially from the legal and IT departments from organizations, and consultancy firms as they are trying to sell their services at a premium. There is therefore not much academic literature that can be found on the subject, at the moment. Much of the literature and research on the subject, either academic or from professional legal firms or consultancies, are focused around the legal obligations, the technical constraints or the fines associated with non-compliance. Although important and necessary, none of these fall in the scope of this paper.

Likewise the EU health insurance industry is not a consolidated entity, as so literature and research is hard to come by, and although much research and reporting exists around some countries and regions there is no consolidated literature about the health insurance industry in the EU. The literature that exist are from the EU bodies and agencies that

consolidate financial and general insurance data, and from organizations like Eurostat[1] or Insurance Europe[2], that is a federation of 35 national insurance associations. While they do publish reports on trends, the categories within them are often divided to life and non-life insurance policies, and not directly applicable to the paper (Insurance Europe, 2016a).

The paper is therefore heavily reliant on sources from the online news articles to explore the current state of the GDPR, and trends in society, the EU organizations like FRA (FRA, 2014), and the Official Journal of the European Union, EUR-Lex[3] to describe legal obligations, and reports from consultancies like EY (EY, 2017), McKinsey (Manyika et al., 2011), and Deloitte (K. Taylor, 2015) to try understand how the industry is reacting the regulation.

To try to fill the gaps and shortcomings of these areas, extensive research into each thematic area was conducted, and interviews with insurance professionals were executed to guide the research. After some research Francis J. Aguilar's PEST framework (Aguilar, 1967) was chosen as the theoretical framework to bridge the two thematic fields. The PEST analysis framework, which stands for Political, Social, Economical and Technological, is framework to analysis the business environment in which the business is located, and is one of the most common approaches for considering the external business environment (Gupta, 2013). According to Gupta, the PEST analysis is an important tool for to make strategic management decisions, as a study of the organizational environment can pinpoint factors that could significantly influence an organizations

[1] http://ec.europa.eu/eurostat
[2] https://www.insuranceeurope.eu
[3] http://eur-lex.europa.eu/

operational and long-term survival (Ibid). The paper will go more in-depth with the PEST framework in the following sections.

4.4. Theoretical Framework

The aim of this section is to provide the background, and an overview of the theoretical framework and justification for their use in this paper. We will start by providing an overview of the GDPR in the historical context of privacy and data protection in Europe.

Then we will apply the PESTLE framework to the European health insurance industry, this will result in an analysis of how and what the industry is influenced by, and to what extent. The section will end with a summary where we comment on the findings, the scope, the timing and the enforceability of the GDPR.

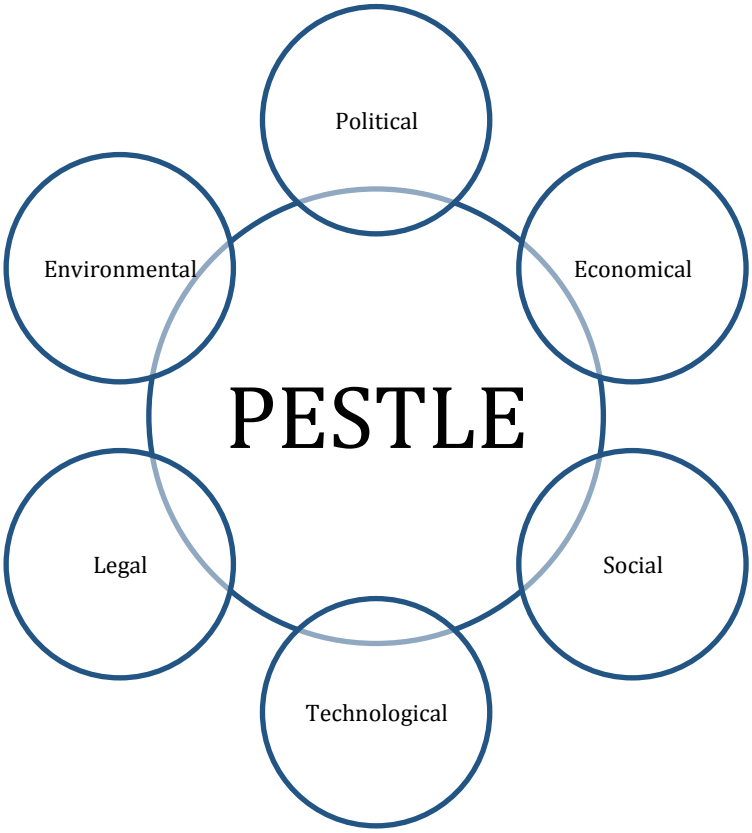
We will apply the PESTLE framework to the European health insurance industry and analyse how the GDPR will impact the competitive structure, and its ability to collect, process and use customer data. The PESTLE framework, first introduced by Francis J. Aguilar in his work *"Scanning the Business Environment"* (1967), is a useful tool that gives us the macroeconomic point of view in which an organization operates in.

4.4.1 PESTLE Framework

PESTLE it is an acronym of factors, that when expended stands for Political, Economic, Social, Technological, Legal and Environmental. Originally called PEST, its origin can be contributed to Francis J. Aguilar in his work *"Scanning the Business Environment"* from 1967. The PEST framework has since then become a popular tool to describe and analyse the macroeconomic environment of organizations, markets and industries. Since its conceptualization the framework has been subject to countless relabeling, adding and subtracting factors to fit the situational and

environmental needs. It can do so as the framework is not a theory that is formulated to predict, explain and understand phenomena, rather it is a taxonomy that we can use to structure, systemize and classify factors. As so we have a myriad of choices to choose from when applying the framework such as PESTLE, STEEPLE, DESTEP, STEER, and so on each adding or subtracting factors such like legal, ethical, demographical, and inter-cultural factors. The PESTLE framework is macro orientated by focusing on the competition structure i.e. by examining the external factors such as the political, economical, social and technological issues, and due to the nature of the tool it is useful for a wide range of applications such as business strategy, marketing and organizational planning as well as product development. The framework is also used by the industry and is incorporated in the syllabus when training to become an actuary (Barbara, Cortis, Perotti, Sammut, & Vella, 2017).

Figure 1 - PESTLE Framework



A PESTLE analysis is normally used in conjunction with a SWOT analysis, which stands for Strength, Weaknesses, Opportunities and Threats, and looks at the internal factors (strength and weaknesses) as this section focuses on the external environment, it would be inappropriate to apply the full SWOT framework here. The paper will though, evaluate the opportunities and threats of the European health insurance industry, as it is a part of the external factors. Although we are focusing on the macroeconomic environment of the EU as a single market and thereby as a single actor, we recognise that there are many member states, and they don't always agree on everything, and there are cases where some member states are exempt from following the general rule, but as for the case of our paper the GDPR is a regulation and therefore does not require any further adaptation nor needs to be transposed into national law by member states, as stated in article 288 of the Treaty on the Functioning of the European Union and article 99 of the GDPR. In this paper we will focus on the acronym PESTLE, as it allows us to look into the Legal and Environmental situation of the insurance industry as it stands at the abyss of the GDPR.

Table 1 – PESTLE Factors

PESTLE Factors		
Political factors	**Economic Factors**	**Social Factors**
P - looks at the influence and risk an organization faces from the political sphere and its affects on the organization, market or industry e.g. government intervention, trade and tax policies, environmental regulations, labour unions, political stability etc.	E - looks at the macroeconomics factors of an economy such as interests rates, economic growth, inflation rate and exchange rates.	S - looks at the cultural aspects in the society i.e. social trends, demographic change and make up, attitude towards health and so on.
In the case of this paper we will look at the EU as the main political actor, and focus on the pressures, policies and trends in the EU	Here, rather then focusing on each member state, we will look at the EU as a whole, and there the economic factors of the EU single market	Here we will look at the EU as one single market, and thereby focus one e.g. cross border pan-European social trends
Technological Factors	**Legal Factors**	**Ecological Factors**
T - looks at the technological factors that can influence the industry and society e.g. rate of technology change, automation, R&D and so on	L - looks at the legal factors e.g. consumer law, antitrust laws, privacy laws and etc.	E – normally stands for the Environmental factors, and looks at the weather, climate change, attitudes toward and support for renewable energy etc.
Here we focus on the technologies available in the digitized society	Here again, we focus on EU legislation and how it will influence the industry	Here we will be substituting the environmental factors with Ecological factors and look at the concept of data as natural resource that arisen

5. Background & GDPR

The aim of this section is to give an introduction to the insurance industry, the privacy legislation in Europe in the context for the GDPR. The first section will give a short introduction to the insurance industry before moving towards the background of privacy and data protection. The last section will give an introduction to the principles, obligations, and the rights that are the backbone of the GDPR.

5.1. Insurance Industry

Insurance is the art of managing risk. Whether it is the risk from bandits and Somali pirates when shipping goods across the ocean or from a random fire that might leave you homeless or from illness and death. Insurance is the means to protect you from the possible financial risk that you take when going about your professional and daily life. The idea of sharing and redistributing risk can be traced back to 3000 B.C. when Chinese merchants would distribute goods on several boats when shipping them down stream on risky waters (NTT Innovation Institute, 2015; Vaughan & Vaughan, 2007). The concept was very simple, instead having all the goods on one ship and risk that one ship capsizing and losing all the goods. They could spread the goods on several boats so that the risk associated with one ship capsizing would be smaller. Later in 1754 BC in the Code of Hammurabi, a Babylonian code of law, describes how a trader could transfer the risk of loss due to bandits to the moneylenders by paying a premium for the loan, the loan would then be discarded in the case the goods were pillaged. The origin of modern insurance can be traced to the Italians and British marine merchants from the 13th and 15th century where they dominated commerce and finance. British merchants who were seeking to insure the ship and cargo would circulate a sheet of paper with the information and description about the ship, the cargo, and destination. Those interested in sharing the risk would then sign under the description, where the term underwriting insurance arose (Vaughan & Vaughan, 2007). Underwriters are insurers who evaluate classify the exposure to risk a certain project or insurance policy have. The underwriters have to determine the risk, and evaluate how much coverage they are willing to take on and to determine the premium that needs to be charged to insure the risk.

One of the first modern life insurance companies, the Society for the Assurance of Widows and Orphans, was founded in London in 1699. Although it, and several other insurance companies were unsuccessful due to a flawed business model, the Equitable Society for the Assurance of Life and Survivorship, likewise founded in London in 1762, became very successful. One of the reasons for its success was contributed to the differentiated premiums they charged according to age, an innovation that the previous insurers did not have access to (Ibid).

Today we have a myriad of insurance types and services. There is almost nothing you can't insure yourself against, whether it is auto insurance, earthquake, fire and flood insurance, you can even get a space and satellite insurance, while it might not be for everyone. The increasing adaptation of the Internet and growing technological developments we see in smart and wearable's devices the conservative insurance industry is feeling the pressure to be more innovative with the products they offer and deliver it in a increasingly faster tempo and flexibility.

5.1.2. From Analog Insurance and Forward

Ever since Blaise Pascal presented the theory of probability in the 1650s and John Graunt discovered the predictable patterns of longevity in the 17th century the science of creating actuarial tables to predict life expectancy and thereby what premium to charge, has basically not changed since (NTT Innovation Institute, 2015; Vaughan & Vaughan, 2007).

There has been a dramatic technological transformation of the insurance industry the past 60 years. The advancements in technology, mainframes and adoption of computers has moved the actuaries science from a analog and manual calculation to a semi-automated and tech enhanced version of the analog model of insurance, as the insurance industry moves into the

21st century (NTT Innovation Institute, 2015; Vaughan & Vaughan, 2007). This upgrade of technology and the emergence of the Internet have led insurance firms to drive efficiency and optimize their operations by implementing paperless billing, creating online quote systems and semi-automated underwriting, and has left insurance firms in technological parity with each other. Insurance firms must therefore find other ways to stay competitive, such as though marketing or accepting and taking a bigger risk on their customers (Ibid).

As we move into the 22nd century the insurance industry stands again over a major transformation both technological terms, due wearables and Big Data and in the regulation as society and regulators have become less tolerant to cyber security breaches and predatory behavior of firms.

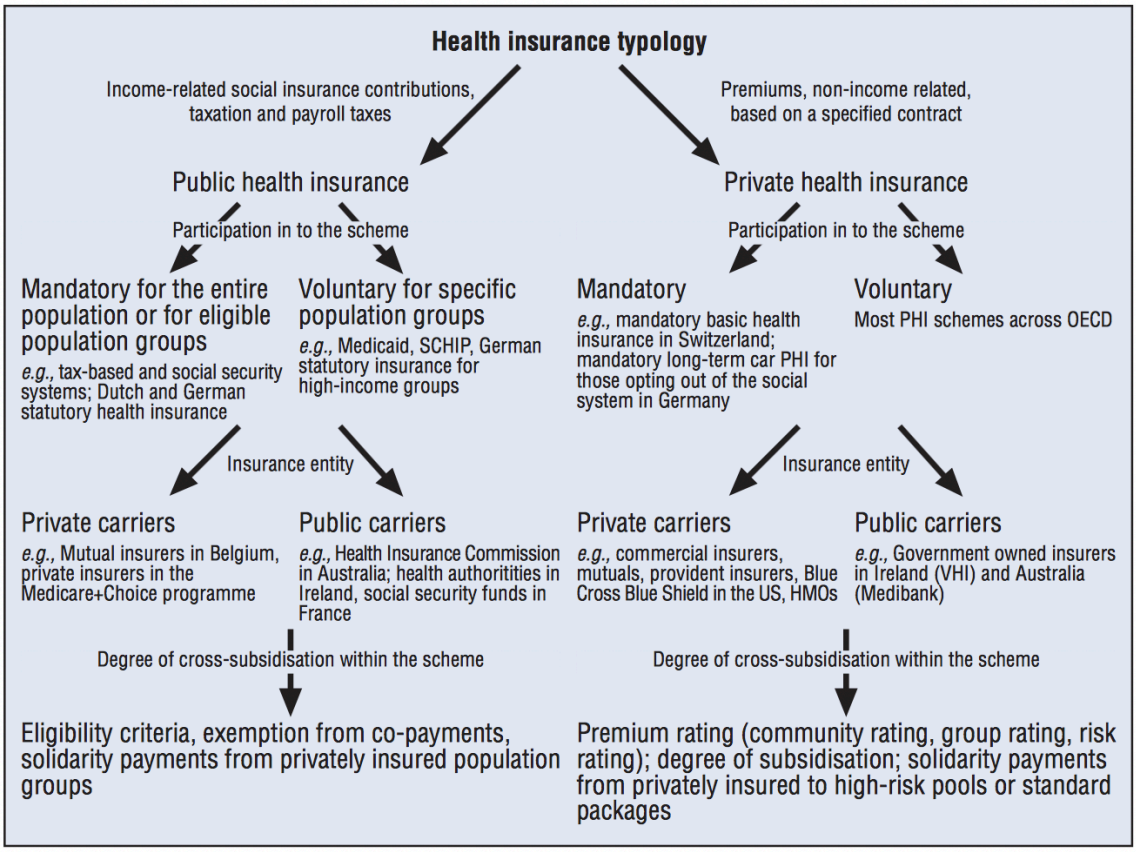
5.1.3. European health insurance & Technological Developments

With over 510million denizens in 28 member states. The EU is a complex web of legal, social, and cultural norms with each member states having unique financial and healthcare systems. While article 168 of the Treaty on the Functioning of the European Union (TFEU) concerning public health gives the EU the mandate to pursue activities and policies to protect human health in the EU. It also very clearly states that the EU shall respect the right of member states to define their own health policies and organize the health service and medical care (EU, 2016, Art. 168). It is therefore very common for EU member states to both have a public health insurance and private health insurance system in place in the countries, but due to the difference each member states have in their health service and medical care, we do not observe many internationally active insurance groups (IAIGs) that operate across all European countries. The EU has tried to rectify this by introducing the European Health Insurance

Card that gives EU citizens access to healthcare for unplanned and necessary state-funded medical healthcare during a temporary stay in another partner country (Commission, 2018).

This adds to the complexity to the overall health insurance landscape of the EU. Although this paper will not go in-depth with the different types of healthcare systems in each member state, as it is less important to the research question of investigating how the insurance industry can leverage the GDPR. It is still important that we are able to distinguish between public and private health insurance schemes as it contributes to the our knowledge of the complexity of the case. Figure 2 illustrates typologies of the health insurance arrangements.

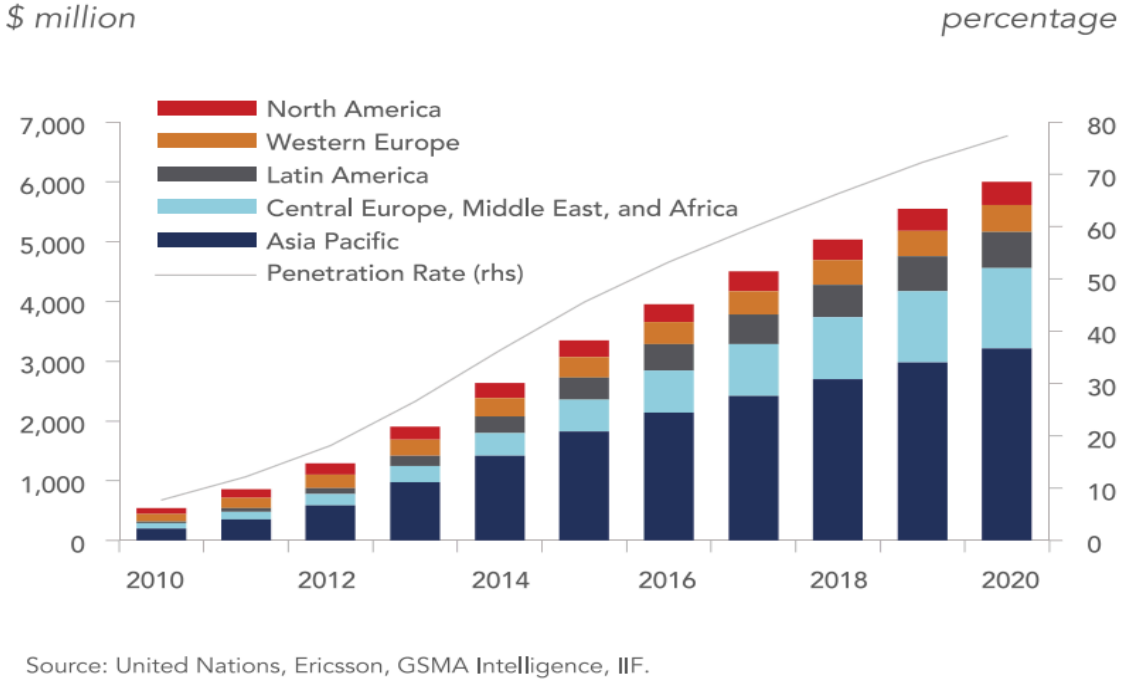
Figure 2 - Typology of health insurance arrangements



(OECD, 2004)

Much like the rest of society and businesses today, the insurance industry is experiencing a massive technological push, and consumer pull. Innovative technology firms like Fitbit, Apple, and Samsung launch a new, smarter, smaller and more connected device every year. While firms like Google and Facebook know everything about you. This digital transformation of society has led to an on-demand economy where consumers expect immediate, personalized and flexibility of goods an services (IIF, 2016; Jaconi, 2014). The consumer expectation of immediate deliverance of goods and services has "trickled down" to complex financial and insurance services as well. Today you can fill out a loan application online and get an answer within minutes or buy travel and auto insurance from the convenience of your sofa. In May 2017, Forbes reported that 40% of Americans hadn't used a physical bank within the previous six months due to online and mobile banking, consequently the number of physical banks have reduced to almost half between 1995 and 2015 (Newman, 2017).

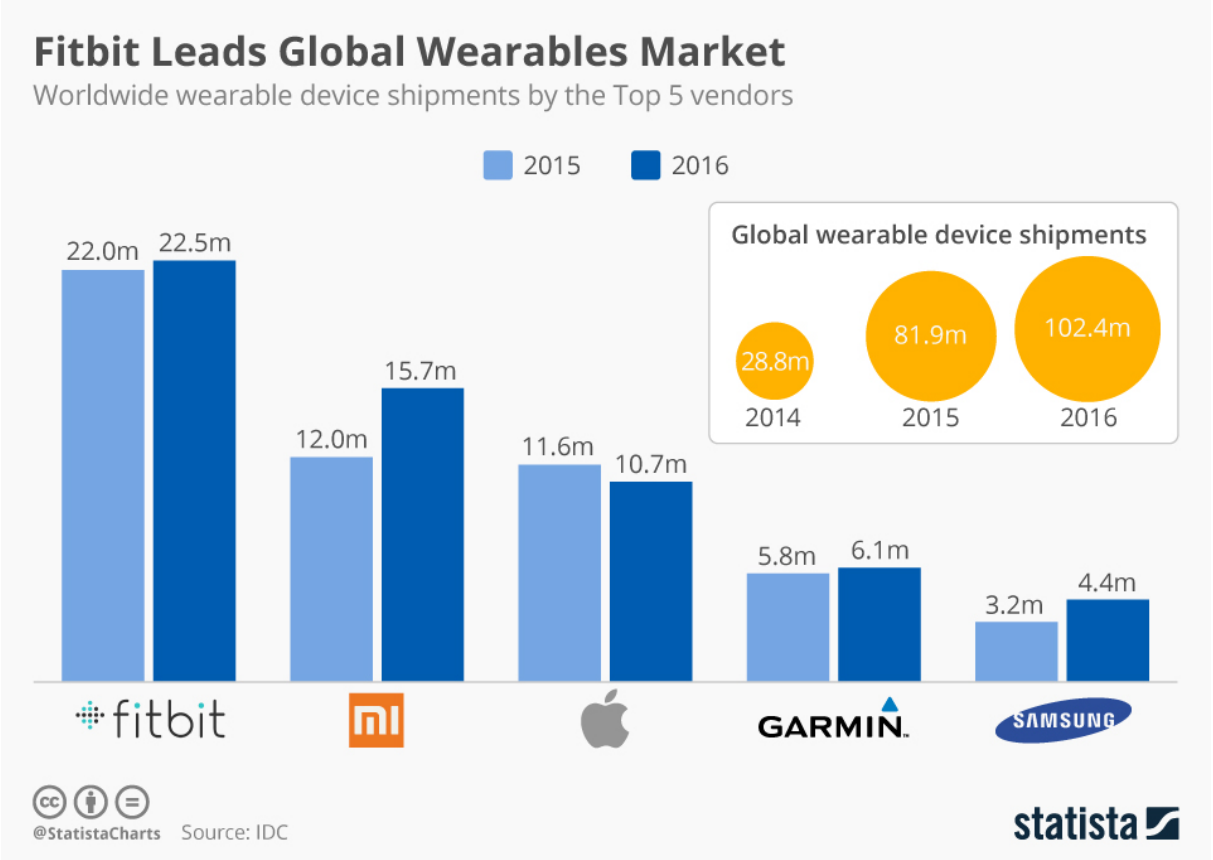
Figure 3 - Global Smartphone Subscriptions and Penetrations Rate



(IIF, 2016)

According to the European Insurance and Occupational Pensions Authority (EIOPA) Sixth Consumer Trends Report, the rise and hype of the Big Data and the possibilities of wearables are leading consumers to expect increasingly more innovative, and more flexible insurance products that are tailored to the individual (EIOPA, 2016; IIF, 2016). Wearbles like the Fitbit can provide insurance firms with unprecedented amount of data on health of their clients. The device linked with other sensors could provide data about peoples exercise and food habits, blood pressure and heart rate and other vitals signs. Using the technological developments in artificial intelligence and Big Data Analytics this in turn could create a predictive, preventative and personalized insurance policy (EIOPA, 2016; EY, 2017, 2017).

Figure 4 - Global Wearables Market



(Richter, 2017)

5.2. Protection of Privacy

Since the end of the Second World War, Europe has had strong tradition of privacy protection. The first traces of privacy and personal data protection can be linked to the *European Convention on Human Rights* "*Convention for the Protection of Human Rights and Fundamental Freedoms"* of 1950, where the right for private and family life is described under article 8:

"Everyone has the right to respect for his private and family life, his home and his correspondence" (Echr-cedh, 1998, Art. 8(1))

Later the right to privacy and correspondence found its way to the *Charter for Fundamental Rights of the European Union* (The Charter), which has two articles under Title II covering the issue, and a dedicated agency was created named the European Union Agency for Fundamental Freedoms (FRA). The FRA is tasked with supporting the EU institutions and member states on safeguarding the rights and to ensure the fundamental rights of its citizens (FRA, 2014).

"Article 7: Everyone has the right to respect for his or her private and family, home and communication.
Article 8(1): Everyone has the right to the protection of personal data concerning him or her" (European Parliament, 2000)

The European Parliament, the Council and the Commission proclaimed the Charter in the year 2000 and came it into effect with the signing of the Lisbon Treaty in 2009, giving the Charter the same jurisprudence as the EU treaties. As the FRA was created to support and monitor member states, the European Court of Justice was mandated to enforce the European treaties and the Charter, thereby creating a legal system where

states and citizens can challenge member states in disputes regarding violations of their fundamental rights, laid out by the Charter and treaties. While the Convention and the Charter was being adopted in continental Europe, the Organization for Economic Co-operation and Development (OECD) in lieu of increasing pressure of the technological developments in computers, cross-border data transfer and processing, the OECD published the *"OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data"* in September 1980. The guidelines were an attempt by the OECD to protect privacy and individual liberties, while addressing the disparities of privacy legislation between member countries, which acted as obstacles for the free flow of information and data, thereby a barrier for economic growth (OECD, 1980). The guidelines introduced eight principles of privacy, which have played a significant role in shaping privacy legislation we see in force today. Table 2 shows the OECD privacy principles as they were laid out in 1980.

Table 2 – OECD Privacy Principles

OECD Privacy Principles	
Collection Limitation Principle - §7	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
Data Quality Principle - §8	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date
Purpose Specification Principle - §9	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose
Use Limitation Principle - §10	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law
Security Safeguards Principle - §11	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data
Openness Principle - §12	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller
Individual Participation Principle - §13	An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended
Accountability Principle - § 14	A data controller should be accountable for complying with measures, which give effect to the principles stated above

(OECD, 1980)

Like its OECD counterpart the GDPR and its predecessor the EU's Data Protection Directive was created in lieu of increasing pressure by technological developments and the exponential growth of cross-border transfers and processing of data, this growth was primarily driven by the success and wide adaptation of the Internet, smartphones and IoT devices. The GDPR's predecessor, EU's Data Protection Directive 95/46/EC, was adopted in October 1995 and heavily inspired by both the OECD privacy principles and the *European Convention on Human Rights*. The directive has since governed the EU and protected it citizens concerning *personal data.* The goal of the directive was to protect individuals with regards to the processing of personal data and to ensure the free movement of such data (EU-Lex, 1995). The directive was introduced in an effort to harmonise European privacy laws, and to guarantee the secure and free movement of personal data across European borders, much like the OECD principles did over a decade ago. As it is a directive it sets up a regulatory framework for member states to implement their own national legislation and a supervisory body around the core principles of privacy and data protection. Whilst a directive is a legislative tool used by the EU to give the member states more autonomy on how to implement EU rules and goals, the way the member states choose to reach the goals are up to them. This has led to a wide range of disparities in the legislation and sanctions opportunities among member states, making the marketplace more complex rather then consolidating the market as the original intent of the directive (EUR-Lex, 1966, 1995, 2010, 2016a). Unlike its predecessor, the GDPR, is an EU regulation meaning that it is a binding legislative act the must be applied in it entirety across the EU (EU, 2017). While the regulation allows for national derogations in special cases these are strictly restricted to purpose of national security, prevention and detection of crime and in certain other situations and requires supplementary national legislation. In the case of the insurance industries, EU member states have less individual discretion

in designing the regulations applicable to Private Health Insurance (PHI) than their OECD counterparts, as their requirements must conform to applicable EU law. These restrictions will also influence the activities of EU accession countries as well since they will be subject to these same requirements in the near future. Under EU law, PHI products are subject to the same insurance directive as other non-life insurance products. These requirements focus on competition, companies' freedom to offer services across EU countries, as well as financing standards (D. J. Cummins & Weiss, 2004; J. D. Cummins, Rubio-Misas, & Vencappa, 2017).

5.3. The General Data Protection Regulation (Regulation (EU) 2016/679)

After more then four years of consultations and negotiations, the EU Parliament approved the GDPR on the 14th of April 2016, and after a grace period of two years the GDPR will come into effect on the 25th of May 2018. The GDPR will apply to all data controllers and processors that handle personal and sensitive data for all EU denizens whether or not the organisation is located in the EU. This is due to the extra territorial scope of the regulation (EUR-Lex, 2016, Art. 2, 3). Unlike any previous privacy and data protection legislation before it, the GDPR carries the threat of crippling fines for non-compliance and creates a series of new rights for individuals while imposing responsibilities and obligations on data controllers and processors. The administrative fines are multi-layered, but for the scope of the paper we will suffice to say that the fines for non-compliance can be up to 20 million Euros or 4% of total worldwide turnover of the preceding year, which ever is higher as stated in article 83 §5.

The GDPR also have provisions to promote accountability and good governance in relations to personal data that compliment the

transparency requirement in article 5. In the spirit of transparency the GDPR also states that the controllers have notify in case of breaches of personal data. The notification shall happen without any undue delay, and no later then 72 hours (Ibid, Art. 33).

As previously mentioned the GDPR creates a set of rights for the data subjects and imposes responsibilities on organisations. In the following section the paper will go through the responsibilities and individual rights to give an overview of the responsibilities and rights laid out in the GDPR.

5.3.1 Principles for Processing Data and Responsibilities for Controllers

The responsibilities for data controllers are stated in article 5 of the GDPR as it introduces seven key principles. While elements of these principles can be found in some national and members states legislation, the concepts are more fully developed in the GDPR and is accompanied by the possibility of crippling fines for non-compliance, and therefore the GDPR should be taken very seriously by organisations and actions taken to mitigate the business risk that the regulation possesses as soon as possible. The seven core principles of the GDPR as stated in article 5 are listed in table 3.

The principle concerning the lawfulness, fairness and transparency states that processing of personal data should be lawful and fair. It must be transparent to the data subjects to whom the personal data are collected, stored and used. It requires that information relating to the processing should be clear, plain and easily be accessible and to understand. The principle regarding the limiting the purpose states that the data collected should be for a specific and legitimate purpose and that data subjects should be made clear of the risks, rules, safeguards and rights in relation to the processing of personal data. Information on how to exercise their

rights in regards to the processing of their personal data should also be clear to the data subjects. The personal data collected should be adequate, relevant and limited to what is necessary for the purposes they where collected.
A controller can therefore not escape the responsibilities by outsourcing to a second nor third-party data processors (EUR-Lex, 2016, Art. 28, 29).

The accuracy principle states that personal data should be accurate and kept up to date where necessary. This entails that data subjects must be allowed to review the personal data collected to ensure its accuracy. Inaccurate data should be rectified or deleted within a reasonable time limit. The integrity and confidentiality principle concerns the protection of the data. Data controllers and processers should ensure appropriate security measures surrounding the personal data

"…including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure…" (2016, Art. 5 (1e))

This provision includes the obligation to inform of a data breach to the data protection authorities and the data subjects concerned without any undue delay (GDPR, 2016, Art. 5 Recital 39). A failure to do so could lead to a fine at the group level. The last and final principal concerns accountability, although short in text, it has major implications for data controllers as the article 5 states

"The controller shall be responsible for, and be able to demonstrate compliance…" (2016, Art. 5(2))

Table 3 - Processing of Personal Data Principles

Principles relating to processing of personal data	
Lawfulness, fairness and transparency - §5.1(a)	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose Limitation - §5.1(b)	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes
Data Minimization - §5.1(c)	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy - §5.1(d)	Personal data shall be accurate and, where necessary, kept Personal data shall be up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
Storage limitation - §5.1(e)	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
Integrity and confidentiality - §5.1(f)	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability - §5.2	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1

This means controllers will have to be able to show compliance with all of the above principles. Meaning that controllers have to assess their current data practices and develop data/it governance structures that can deal with breaches and in cases of large data usage or sensitive data processing, data protection officers have to be appointed; create reporting mechanisms; obtain new consents where appropriate; and ensure organisational and technical measures are in compliance with the data protection principles. In some case Data Protection Officers (DPO) have to be appointed to act as a point of contact of the authorities. This is the case when it is a public authority, an organisation carries out large scale monitoring of individuals or when carrying out large scale processing of special categories of data or data relating to criminal offences as stated in article 37-39.

5.3.1 Requirements for processing

In order for an organisation, for-profit, public or non-profit, to process personal data the first principle in article 5 requires that it to be lawful, fair and transparent. For the processing to be lawful the GDPR sets out six lawful bases in article 6, where at least one of the basis must applicable for the processing to be considered lawful. The six bases are consent, contractual, legal obligations, vital interests, public interest and legitimate interest as listed in table 4.

Table 4 - Articles for Lawful Processing of Personal Data

Lawful processing	
Consent - Art. 6.1	The data subject has given consent to the processing of his or her personal data for one or more specific purposes
Contractual - Art. 6.2	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
Legal Obligations - Art. 6.3	Processing is necessary for compliance with a legal obligation to which the controller is subject
Vital Interests - Art. 6.4	Processing is necessary in order to protect the vital interests of the data subject or of another natural person
Public Interest - Art. 6.5	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
Legitimate Interest - Art. 6.6	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

All but the first lawful basis is a result of the processing being necessary because it is vital, of public or legitimate interests or to fill a contractual or a legal obligation. In these cases the data subjects may have no say to whether or not its data is being processed. In the case of the processing being based on consent, where data subject have given theirs consent the controllers have to be able to demonstrate that the consent has been given. The consent has to be freely given and the data subject have to be aware of to the extent to which consent is given (GDPR, 2016, Art. 4(11), 7). The GDPR requires data controllers to be further considerate when the data processing relates to children, criminal conditions and special

categories of personal sensitive data. For these categories data controllers will need specific consent or be under the control of an official authority (GDPR, 2016, Art. 8, 9, & 10). Furthermore the GDPR require controllers to implement privacy by default when implementing processes, services and products, to technical and organisational measures so that personal data is not stored or processed for any matter that is not in the spirit it was collected or stored longer then necessary (GDPR, 2016, Art, 25, 47(2(d), recitale 78).

"…applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons" (GDPR, 2016, Art. 25(2))

5.3.2. Rights of data subjects

Not only have the controllers been given more responsibilities and obligations that they have to live up to. The data subjects have be given rights that are designed to give them more control over their own data and how it is used. These rights are as listed in table 5 and is stated in chapter III of the GDPR.

The right to be informed is also embodied in the first privacy principle and concerns the rights of data subject's right to be informed on the processing of their personal data *"…in a concise, transparent and easily accessible and written in clear and plain language…"* (GDPR, 2016, Art. 12(1)). Furthermore the data subjects have the right to access their personal data as stated in article 12 and 15. The right includes the right of conformation that their data is being processed from the data controller, why the data is being processed, to what extent and how long the data

will be stored, and also if the data will be transferred to a third organisation or country (GDPR, 2016, Art. 12, 15, Recital 63).

Table 5 - Rights of Data Subjects

Individual Rights	
Art. 12, 13 & 14	Right to be Informed
Art. 12 & 15	Right of Access
Art. 12, 16 & 19	Right of Rectification
Art. 17 & 19	Right of Erasure
Art. 18 & 19	Right to Restrict Processing
Art. 12 & 20	Right of Data Portability
Art. 12 & 20	Right to Object
Art. 4, 9 & 22	Rights in relation to Automated Decision-making and Profiling

The right of ratification is closely linked to the two previous rights, and states that the data subject has the right to rectify incorrect or incomplete data as stated in article 16.

The right of erasure better known as "the right to be forgotten", is the right of data subjects to request the removal or deletion of personal data when there is no longer lawful and compelling reason for its continued processing, consent is withdrawn, or where the data is no longer necessary for the purpose it was originally collected (2016, Art. 17, 19).
The right to restrict processing is the right to halt the processing of the personal data. This can be due to disputes regarding the accuracy of data and or when there is no longer need for the data, but organisations have to store the data due to legal requirements (2016, Art. 18).

The right of data portability is the right that allows data subjects to obtain and reuse their personal data for their own purpose i.e. transferring personal data from one service provider to an other (2016, Art. 12, 20). Although short in text, the right to move ones data can have major implications for service providers whose core business surrounds the use of such collected data i.e. marketing and health insurance.

The right to object concerns the right to object when processing of data in such cases of profiling for direct marketing or where the processing is carried out in the public interests (2016, Art. 21).

The rights related to automated decision-making and profiling can be seen as safeguards for EU citizens against potential damaging decision-making without any human intervention. This could potentially have large implications when concerning loans and insurance applications (2016, Art. 4(4), 9, 22).

6. PESTLE Analysis

The aim of this chapter is to use the findings from the previous chapters on the GDPR, the technological developments and the health insurance industry to identify and analyse the macroeconomic factors and link them with the theoretical framework laid out in this paper. The analysis will support the empirical evidence and research that has been carried out in this paper. Therefore this section seeks to answer the guiding research question:

Considering the regulatory challenges of EUs General Data Protection Regulation, how will the creation of the individual rights affect the use of data within the insurance industry? And what business opportunities within the industry can we identify using the PESTLE framework?

We will be doing so by applying the PESTLE framework to the industry one factor at the time.

6.1. Political

Following the financial crisis of 2008, the industry has been under constant scrutiny, and as the nature of the industry, it has multiple political, social and regulatory stakeholders that it has to pay attention to. Latest the increasing high level data breaches and revelations by Edward Snowden and the indiscriminate surveillance by the Americans has led to political outcry for better data and privacy protection that has led to the adoption of the GDPR. The increasing number of breaches and scandals has put the governments, legislators and politicians under pressure to do more to protect its citizens. This pressure combined with European tradition of privacy, and the single market has led the EU to be on the forefront of data protection and privacy. The GDPR sets up strong regulatory requirements for both public and private organisations that

handle personal data, with harsh fines for those who are non-compliant. Looking at the current political environment and the posturing of the likes of the EU Commissioner for Competition Margrehte Vestager, and the harsh fines given to major IT companies like Google and Apple for breach of competition and tax rules (Graham, 2017), public and private organisations are scrambling to get there house in order before the 2018 May deadline.

The GDPR does not only ensure that the fundamental rights of its citizens are protected, but it fits well with the political goals of the EU to integrate Europeans and the promotion of the single market. Especially in the context of events like Brexit, the migration crisis, and the uncertainty of the US-EU relations, where the GDPR can be interpreted as a unified EU approach to a cross border problem, and where the EU can claim that it has a legitimate stake, and relevance in society today. As so, the industry is heavily regulated, and for insurance firms that operate in the EU the GDPR is only the recent in a range of regulatory requirements spurred by political motivations like the promotion of the digital and financial single market i.e. the Solvency II Directive (2009/138/EC), International Financial Reporting Standards 17 (IFRS), Insurance Distribution Directive (IDD) (2016/97/EC) and Packaged Retail Investment and Insurance Products (PRIIPs) (Regulation (EU) 1286/2014). These regulations are in place to promote the single market by making it easier to do business across EU borders and to mitigate the risk of insolvency by financial and insurance firms in the EU. With these regulations and the GDPR in place, the commission goals is to increase competition, foster innovation in the industry and at the same time ensure the security of its citizen's data. These political interventions will greatly impact both the macroeconomic situation within the insurance industry i.e. the IDD and PRIIPs goal is to ease the regulatory, financial and bureaucratic requirements for expanding business across the different EU member states (European

Parliament, 2014, 2016). While the Solvency II the goal is to codify and harmonise EU insurance regulation to increase the capital requirements insurance companies have to hold to reduce the risk of insolvency (European Parliament, 2009). Although Europe has one of the stringiest data protection legislation in the world, the deregulatory and corporate friendly attitude that the Trump administration in the US has taken, may lead financial and IAIGs to advocate the EU parliament, EU Commission and MEPs for a more lax attitude to create a level playing across the Atlantic Ocean (EY, 2017a; Zeppos & Wallach, 2017).

6.2. Economical

According to the EU Commissions Spring 2017 economic forecast the European economy will reach its fifth consecutive year of growth, with growth reaching all member states in 2017 (Commission, 2016). While inflation rates, within the euro area have seen a temporary spike from 0.2% in 2016 to an expected 1.6% in 2017, this is expected to fall to 1.3% in 2018, while the core inflation rate remains stable and below its long-term average (Ibid). The unemployment rate still remains high, but has a downward trend and is expected to fall to 9.4% in 2017 and to 8.9% in 2018. While the macroeconomic numbers seem to be optimistic, there are still major political uncertainties around the world that can upset the forecast such as: Oil prices; an escalation of the North-Korea situation; the Poland-EU crisis; Brexit; Trump in the White House, just to mention a few. The European insurance market is one of the worlds largest markets for insurance, with 32% of the market share (Insurance Europe, 2016b), and as one of the largest institutional investors, the insurance industry plays a vital role in ensuring the long-term economic investment, security and stability within the EU.

The rapid technological developments in Big Data Analytics, connectivity, and the political pursuit for the single digital market in the EU, has opened

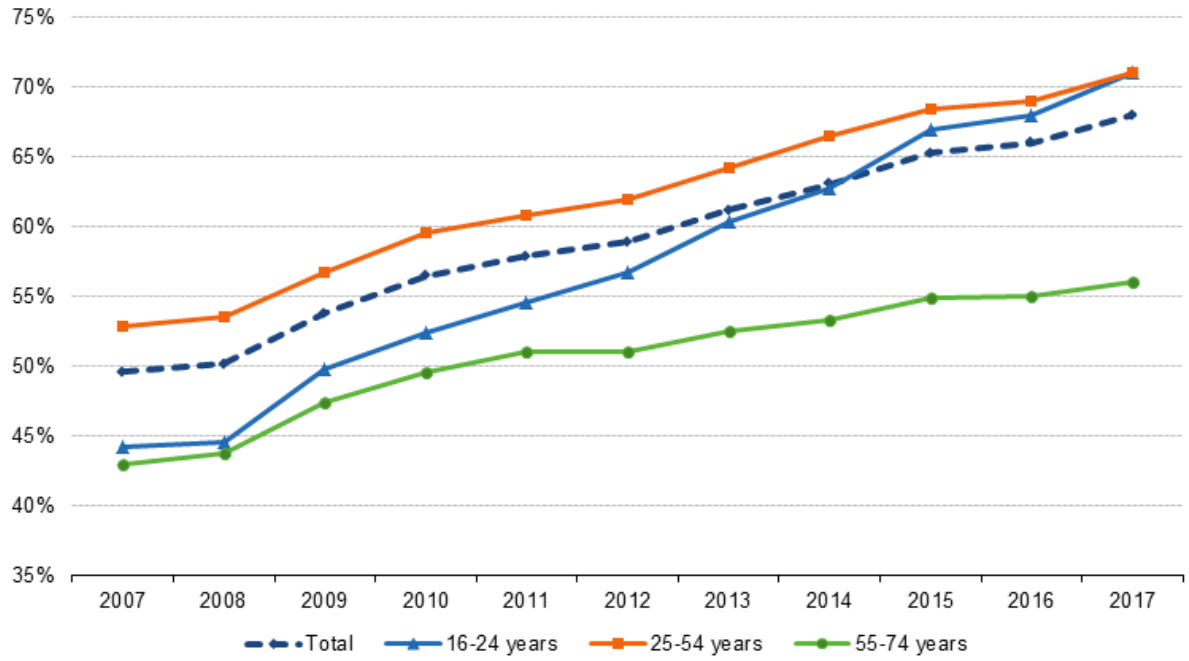
up new opportunities by lowering technological and technical barriers, as it is the case of the introduction of the IDD and PRIIPs. According to IHS the market for IOT is expected to grow to 75.4 billion devices by 2025 from 15.4 billion devices in 2015 (Columbus, 2016), and is estimated to have a compounded annual growth rate of 15.6% between 2015-2020, reaching $ 1.29 trillion in 2020 (IDC, 2017). Social media users grew from 970 million users in 2010 to 2.28 billion in 2016, and it is predicted to grow to 3.62 billon by 2021 (Statista, 2017a) while the global revenue from social media markets are expected to reach € 22.9 billion by 2019 (Statista, 2017b). These exponential growths in data has created new industries such as the data broker, e-commerce and cloud service providers, and created new job titles such as a youtuber, search engine optimiser, social media manager and so on. These new economic and commercial opportunities will in the mid- to long-term future greatly impact all aspects of the insurance industry. Firms will see an increase in rivalry between those who can utilise the new technologies, and those who still want to use the fax-machine. We will increasingly see more and more players enter the market with innovative and modern insurance products, that does not have a big and heavy legacy system they have to carry around (EY, 2017; Protiviti, 2016).

6.3. Social

In 2007, Sony's than executive director for information security, Jason Spaltro, argued in an interview that *"it's a valid business decision to accept the risk"* to *"not invest $10 million to avoid a possible $1 million loss"* for a data breach (Holmes, 2007). With the implementation of the GDPR this is no longer an option. The number of breaches has only risen since 2007 and in 2016 around 1,378,509,261 billion records were breached from 1,792 incidents reported (Gemalto, 2017).

With the wide adaptation of smartphones, Internet and social media services like Facebook, Instagram, twitter etc. Society has never been more connected than we are today, and risk associated with it has never been greater. Corporate attitudes like the one of Jason Spaltro, Equifax, and the revelations made by Edward Snowden about mass surveillance programs like PRISM, has made citizens and civil society organisation wary of corporations and national intelligence services alike. While there has been a social movement and protest of such agreement as the "Stop Online Privacy Act" (SOPA) in the US (Ngak, 2012) and the Anti-Counterfeiting Trade Agreement (ACTA) in the EU (Lee, 2012), consumers and organisations across the world have largely embraced IoT, wearable devices and social media services that track your location, share your thoughts, and preferences. The digital transformation of our society has led to an emergence of the on-demand economy, and has fundamentally shifted consumer behaviour, and firms have to adapt to the new changes or risk being left behind. According to Eurostat, 71% of all 16-54 year olds have in the previous 12 months bought something online (see figure 5).

Figure 5 - Internet user who bought or ordered goods or services for private use in the previous 12 months by age - EU-28



(Eurostat, 2017)

Although it seems that consumers are embracing online shopping and the on-demand economy, a 2015 report published by the Danish Business Authority on the consumer online behaviour "Befolkningens adfærd på nettet" found that 57% of the participants asked in the survey would not wear a fitness tracker to get a 25% discount on insurance (Erhvervsstyrelsen, 2015). The same report found that 45% of participants would share health information with their insurance company, and only 26% of participants asked would share information about their medical drug use with their insurance company (Ibid).

6.4. Technological

The rapid development of technology has spurred a fundamental and technological transformation of the insurance industry, as we know it. The technological developments can be seen as a blessing and a curse for

many insurance firms at the same time (Barbara et al., 2017). Although the firms have enjoyed the many cost savings properties that the technological development has brought with it since the 1960s. They now find themselves unable to keep up with the changes and demand from consumers, for faster, cheaper, and more personalised insurance products. One of the reasons is that traditional incumbents have to deal with large, bureaucratic, and slow moving corporate organisations, where the decisions are slow and expensive to be approved. Many incumbent firms also have legacy IT systems, that are expensive to replace and possibly pose a security threat. Although a KPMG report from 2014, stated that legacy systems might cost more to keep operational, rather then replacing them, due old and out-dated software (KPMG, 2014).

there is a risk of more tech-savvy firms entering the market and capture a large portion of the market (EY, 2017, 2017; NTT Innovation Institute, 2015). Firms with heavy legacy systems need to update and

6.5. Legal

As mentioned previously, the GDPR has not been the only regulation to affect the insurance industry e.g. Solvency II Directive (2009/138/EC), Insurance Distributive Directive (2016/97/EC) and Packaged Retail Investment and Insurance Products (Regulation EU 1286/2014) have all been introduced within the last couple of years. Although Solvency II has been around since the 2009, the directive was only adopted in January 2016, and is already up for review at the end of 2018. Unlike some of the previous regulations the GDPR brings a different, and some might say unfamiliar set rules to the table. Although privacy regulation is not new, the scope of the regulation and implementation of individuals right to their own data might be a surprise for organisations. The GDPR also introduces principles concerning transparency; accountability and the obligation to

report breaches within 72 hours, some thing that was taken rather light in previously. The penalty for non-compliance, as previously mentioned, is up to 4% of global turnover or 20million €, which ever is higher.

6.6. Environmental/Ecological

Since the Data Protection Directive was adopted in 1995, there has been an exponential growth in technological developments across the board. This has led to the rise of new technologies like the smartphone, iPods and cloud services. While others like the compact cassette and the VCR have faded out, some like the LP is making a comeback. Moving from a digital to the data paradigm, the availability of data and processing power has led to an exponential growth in the data industry. The growth in data is driven by the wide use and adaptation of smart devices, and the Internet. This development has led to what some call data, or Big Data, as the new natural resource (Picciano, 2014).

6.7. Summary: A partial conclusion

The aim of this section is to give an overview of the main drivers of each factor and give a brief comment on them in the context of the GDPR, healthcare and the insurance industry.

Political & Legislative factors	
Main drivers	**Example**
Insurance	GDPR, Solvency II, IDD
Healthcare	European Health Insurance Card, Single Market, Solvency II
GDPR	High regulatory control
Uncertainty	Trump, Brexit, Cataloniaen independence movement, EU-PL Crisis

There is a high level of regulatory interventions in the financial and insurance sector in the EU. With the implantation the regulations such as the GDPR, Solvency II, IDD, PRIIPs and so on, businesses need time to adjust to the new regulatory reality. The high regulatory interventions can there act as a barrier for growth.

In the healthcare sector we see that, although the healthcare is not within the EU mandate, the introduction of the European Health Insurance has led to a stronger integration of its citizens, and makes it easier to move around the EU. This is in line with EUs political goal of harmonisation between member states. As so we can observe that there is still a drive for harmonizing the different marketplaces within the EU, despite some uncertainties.

The introduction of the GDPR has been a political wish for a long time. As so the political goals of the GDPR are well in line with the EU Commission, especially the European Commissioner for Competition Margrethe Vestager. Margrethe Vestager has become famous for taking on the likes of Google, Apple and has become a crusader for the right for privacy.

Liberalisation and deregulation used to be high on the agenda of almost every country in the world. After the financial crisis of 2007-2008 we have seen an increase in regulation especially in the financial, banking and insurance industry. As these industries are especially important for a stable economic development but! With Donald Trump as the new US president, we have seen his administration move towards deregulation and a more corporate friendly attitude. With the current "protectionist" view of the EU we might arise regulatory disparity between the EU and other economic regions.

Economical Factors	
Main Drivers	**Example**
Insurance	Changes in inflation, Harmonization
Healthcare	Demographics Crisis in Horizon
GDPR	Innovation
Uncertainties	Trump, North Korea, Brexit,

The insurance industry was not that severely affected by the financial crisis of 2007-2008. As so the industry has experienced a stable growth in 2017 and is also expected to do so in 2018 (Barbara et al., 2017).

The healthcare sector in the EU is facing a potential demographic crisis. The population in the EU is getting older, and there a fewer babies being born. This might led to an excess pressure on the healthcare system across Europe.

The rapid technological development has led to new and innovative products, services and job opportunities. The GDPR will work as a regulatory framework that firms can move within, this will create a level playing field for all the players within the single market. Here the right of portability can also possibly act as a bargaining chip for consumers to shop around for better deals, and allow greater competition between firms.

The success of such rights and tools like the right of data portability is linked with the success of the GDPR, and how authorities choose to enforce the regulations. The uncertainties in the economical factors are similar to the uncertainties in the political factors.

Social Factors	
Main Driver	**Example**
Insurance	Consumer pull for greater personalization, faster
Healthcare	Mass adaptation of wearables and smart-devices
GDPR	Social movements away from mass-surveillance
Uncertainties	Regulatory catch-up

The rapid developments in technology and the emergence of the on-demand economy have led to customers to be on the forefront of technology. This is resulting in insurance companies being left behind, giving room for smaller, nibbler and hi-tech savvy firms, also called insurtech.

Healthcare is experiencing a "social movement" in wearables and smart-devices. Although the Danish Business Authority report showed that 57% would not wear a fitness-tracker for a 25% discount of healthcare insurance, it still leaves 43% that are open to the idea (Erhvervsstyrelsen, 2015)

The GDPR is being introduced just in time, or maybe a couple of years to late. Stolen pictures, no right over on own data, data breaches and predatory behaviour of some firms have led to a social movement demanding better privacy protection and ownership one own data.

The uncertainty in the social factors arises with the implementation and enforceability of the GDPR. If the GDPR is able to curb the rise of data breaches and the predatory behaviour of firms while giving ownership back to individuals, it will be considered a success. If not it would be another example of an EU failure.

Technological & Environmental Factors	
Main Driver	**Example**
Insurance	Digital Transformation
Healthcare	Wearables, Smart-devices,
GDPR	Regulative Pull
Uncertainties	Enforcement

The insurance industry is currently experiencing a digital transformation like it has never experienced before. Futuristic concepts are becoming actionable, and consumer demand for predictive, preventative and personalized insurance products are only going one way (EIOPA, 2016; EY, 2017, 2017). The environment and time to develop these technologies and business models have never benne better.

Likewise the possibility of smart devices and wearables are revolutionizing the healthcare sector. The concept of going to the doctors remotely via video chat has existed for many years, but with the mass adaptation of smart devices and wearables, health care professional can get accurate and real time measurements and data, and even monitor you remotely.

Society and consumers are currently widely adopting everything that is smart and connected. Whether it is a smart tv, smart fridge or a smart vacuum cleaner, as long as it is smart and connected. Smart-phones and wearables like the Fitbit have the ability to measure your heartbeat, track you and your behaviour and when the data is linked with your shoes and your fridge it is possible to track how you exercise, what you like to eat and when.

The success relies on two factors. First, success criteria lies with the tech companies itself, are they able to make these technologies safe, stable and accurate enough for the use in healthcare. The second success criteria is can tech companies convince the consumer to trust and use these

products? According the sales number of smartphones and Fitbits in figure 3 and 4 the answer is yes.

8. Concluding Remarks

There are no discussion that implementing the GDPR will be time and resource demanding for any organization. It will require the effort of the whole organization as the GDPR is not only and technological change, but as it will change to how the organization view privacy and handle personal data. This will especially be the case for insurance companies, as they hold vast amount of data, and for insurance firms that offer health policies, the GDPR requires you be especially considerate as much of the data would be considered sensitive data. Consumer exercising their right to access their data, their right of erasure or right of portability will be especially challenging for incumbent firms with heavy legacy systems. As these will often require manual deletion and conformation as they are often not compatible with newer systems (EY, 2017). Firms that are able to identify and utilize opportunities within the GDPR, such as start-ups, also known as insurtech, will be able to navigate the market much better and be able to adapt to trends and changes much faster then incumbent firms.

8.1. Further Studies

During the research and investigative period of the paper, I have come across many themes that I'm unable to touch upon due practical reasons and limitations. So for further studies one could link Michael Porter's five forces to get an in-depth analysis of the industry and identify the internal forces driving the insurance industry. Another filed of study could be to go into the moral and ethical aspects metadata or Big Data is used. For this I would recommend Shoshana Zuboff's "Big Other: Surveillance and the prospects of an information civilization.

9. Bibliography

Abott, A. (2004). *Methods of Discovery - Heuritics for the Social Sciences* (1st ed.). W. W. Norton & Company Inc.

Aguilar, F. J. (1967). *Scanning the Business Environment*. London: Cambridge University Press.

Barbara, C., Cortis, D., Perotti, R., Sammut, C., & Vella, A. (2017). The European Insurance Industry: A PEST Analysis. *International Journal of Financial Studies*, *5*(2), 14. https://doi.org/10.3390/ijfs5020014

BBC NEWS. (2016, September 6). Brazzers porn account holders exposed by hackers. *BBC NEWS*. Retrieved from http://www.bbc.com/news/technology-37285715

CBS/AP. (2017, September 19). Equifax had data breach months before big one hit: report. *CBS/AP*. Retrieved from https://www.cbsnews.com/news/equifax-data-breach-happened-months-before-big-one-hit-report/

Columbus, L. (2016, November 27). Roundup Of Internet Of Things Forecasts And Market Estimates, 2016. *Forbes*. Retrieved from https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#189fbdda292d

Commission. (2016). Spring 2017 Economic Forecast | European Commission. Retrieved August 18, 2017, from https://ec.europa.eu/info/business-economy-euro/economic-performance-and-forecasts/economic-forecasts/spring-2017-economic-forecast_en#spring-2017-economic-forecast-steady-growth-ahead

Commission, E. (2018). European Health Insurance Card. Retrieved January 14, 2018, from http://ec.europa.eu/social/main.jsp?catId=559

Cox, J. (2016, September). Nearly 800,000 Brazzers Porn Site Accounts Exposed in Forum Hack. *Motherboard Vice*. Retrieved from https://motherboard.vice.com/en_us/article/vv7pgd/nearly-800000-brazzers-porn-site-accounts-exposed-in-forum-hack

Cummins, D. J., & Weiss, M. A. (2004). Consolidation in the European Insurance Industry: Do Mergers and Acquisitions Create Value for Shareholders? *Brookings-Wharton Papers on Financial Services*, 217–258.

Cummins, J. D., Rubio-Misas, M., & Vencappa, D. (2017). Competition, efficiency and soundness in European life insurance markets. *Journal of Financial Stability*, *28*, 66–78. https://doi.org/10.1016/j.jfs.2016.11.007

Echr-cedh. European Convention on Human Rights (1998). Retrieved from www.echr.coe.int

EIOPA. (2016). *SIXTH CONSUMER TRENDS REPORT*. *EIOPA*. Retrieved from https://eiopa.europa.eu/Publications/Reports/Sixth Consumer

Trends report.pdf
Erhvervsstyrelsen. (2015). Befolkningens adfaerd på nettet. Retrieved from https://erhvervsstyrelsen.dk/sites/default/files/befolkningens_adfaerd_paa_nettet_tilgaengelig.pdf
EU. (2017). EUROPA - Regulations, Directives and other acts. Retrieved June 29, 2017, from https://europa.eu/european-union/eu-law/legal-acts_en
EU-Lex. EUR-Lex - l14012 - EN - EUR-Lex (1995). EU. https://doi.org/Directive 95/46/EC
EUR-Lex. Precedence of European law, Pub. L. No. EUR-Lex-l14548-EN-EUR-Lex (1966). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14548. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14548
EUR-Lex. Data Protection Directive 95/46/EC (1995). EU. https://doi.org/Directive 95/46/EC
EUR-Lex. (2010). *Treaty of Maastricht on European Union*. *EUR-Lex*. https://doi.org/EUR-Lex - xy0026 - EN - EUR-Lex
EUR-Lex. General Data Protection Regulation, EUR-Lex § (2016). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1
EUR-Lex. REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Journal of the European Union § (2016). EU. Retrieved from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
European Parliament. (2000). Charter of Fundamental Rights of the European Union. Retrieved May 27, 2017, from http://www.europarl.europa.eu/charter/pdf/text_en.pdf
European Parliament. (2009, November). DIRECTIVE 2009/138/EC. *Official Journal of the European Union*, p. 155. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0138&from=EN
European Parliament. (2014, November). REGULATION (EU) 1286/2014. *Official Journal of the European Union*.
European Parliament. (2016, January). DIRECTIVE (EU) 2016/97. *Official Journal of the European Union*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0097&from=en
Eurostat. (2017). E-commerce statistics for individuals. Retrieved January 14, 2018, from http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals
EY. (2017). 2017 European insurance outlook. *EY*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-2017-european-insurance-outlook/$FILE/EY-2017-european-insurance-outlook.pdf

EY. (2017). Digital transformation in insurance. *EY*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-digital-transformation-in-insurance/$FILE/ey-digital-transformation-in-insurance.pdf

EY. (2017). EU General Data Protection Regulation: are you ready? Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017/$FILE/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017.pdf

FRA. (2014). About FRA | European Union Agency for Fundamental Rights. Retrieved May 27, 2017, from http://fra.europa.eu/en/about-fra

Gemalto. (2017). *Mining for Database Gold PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN*. Retrieved from http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf

Gold, S. (2011, May 11). How European nations run national health services. *The Guardian*. Retrieved from https://www.theguardian.com/healthcare-network/2011/may/11/european-healthcare-services-belgium-france-germany-sweden

Gorski, P. S. (2013). What is Critical Realism? And Why Should You Care? *Contemporary Sociology*, *42*(5), 658–870. Retrieved from http://www.jstor.org.esc-web.lib.cbs.dk/stable/pdf/23524414.pdf

Graham, L. (2017). Here are some of the largest fines dished out by the EU. *CNBC*. Retrieved from http://www.cnbc.com/2017/06/27/the-largest-fines-dished-out-by-the-eu-commission-facebook-google.html

Gupta, A. (2013). Environmental and pest analysis: An approach to external business environment. *Merit Research Journal of Art, Social Science and Humanities*, *1*(2). Retrieved from https://pdfs.semanticscholar.org/7fde/e2395679e8d930d3ebf601faa84313098af6.pdf

Haselton, T. (2017, September 7). Credit reporting firm Equifax says data breach could potentially affect 143 million US consumers. *CNBC*. Retrieved from https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html

Holmes, A. (2007). Your Guide To Good-Enough Compliance. *CIO*.

IDC. (2017). Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by Manufacturing, Transportation, and Utilities Investments, According to New IDC Spending Guide - prUS42209117. Retrieved July 14, 2017, from http://www.idc.com/getdoc.jsp?containerId=prUS42209117

IIF. (2016). INNOVATION IN INSURANCE: HOW TECHNOLOGY IS CHANGING THE INDUSTRY. *Insitute of International Finance*. Retrieved from

https://www.iif.com/system/files/32370132_insurance_innovation_report_2016.pdf
Insurance Europe. (2016a). Annual Report 2016-2017. *Insurance Europe*. Retrieved from www.insuranceeurope.eu
Insurance Europe. (2016b). Insurance Data. Retrieved June 30, 2017, from https://www.insuranceeurope.eu/insurancedata
Jaconi, M. (2014, July). The "On-Demand Economy" Is Revolutionizing Consumer Behavior — Here's How. *Business Insider*. Retrieved from http://www.businessinsider.com/the-on-demand-economy-2014-7?r=US&IR=T&IR=T
KPMG. (2014). *How well is the life insurance industry keeping pace with rapidly changing technology?* Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2014/06/life-insurance-keeping-pace.pdf
Lee, D. (2012). Acta protests: Thousands take to streets across Europe - BBC News. *BBC*. Retrieved from http://www.bbc.com/news/technology-16999497
Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity*. *McKinsey Global Institute*. https://doi.org/10.1080/01443610903114527
Moore, G. E. (1975). Progress In Digital Integrated Electronics. *IEEE, IEDM Technical Digest*, 11–13. https://doi.org/10.1109/N-SSC.2006.4804410
Newman, D. (2017, May). Top 5 Digital Transformation Trends In Financial Services. *Forbes*. Retrieved from https://www.forbes.com/sites/danielnewman/2017/05/09/top-5-digital-transformation-trends-in-financial-services/#1caa6d33204c
Ngak, C. (2012). SOPA and PIPA Internet blackout aftermath, staggering numbers. *CBS News*. Retrieved from http://www.cbsnews.com/news/sopa-and-pipa-internet-blackout-aftermath-staggering-numbers/
NTT Innovation Institute. (2015). *The Insurance Industry as a Digital Business*.
OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved May 29, 2017, from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
OECD. (2004). *Private Health Insurance in OECD Countries The OECD Health Project Private Health Insurance in OECD Countries*. OECD. https://doi.org/10.1787/9789264007451-en
Palmer, V. J. (2016, December). Downside of fitness trackers and health apps is loss of privacy. *The Conversation*. Retrieved from http://theconversation.com/downside-of-fitness-trackers-and-health-apps-is-loss-of-privacy-69870
Picciano, B. (2014, June 30). Why Big Data Is The New Natural Resource.

Forbes. Retrieved from https://www.forbes.com/sites/ibm/2014/06/30/why-big-data-is-the-new-natural-resource/#7e7fca556628

Pierson, B. (2017, June 24). Anthem to pay record $115 million to settle U.S. lawsuits over data breach. *Reuters*. Retrieved from https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML

Protiviti. (2016). Modernizing Legacy Systems in Insurance, p. Protiviti. Retrieved from https://www.protiviti.com/sites/default/files/united_states/insights/modernizing-legacy-systems-in-insurance-protiviti.pdf

Richter, F. (2017, March 7). Fitbit Leads Global Wearables Market. *Statista*. Retrieved from https://www.statista.com/chart/8420/wearable-device-shipments/

Riley, M., Sharpe, A., & Robertson, J. (2017, September 18). Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed

Roberts, J. J. (2017, September). Why Equifax Executives Will Get Away With the Worst Data Breach in History. *Fortune*. Retrieved from http://fortune.com/2017/09/16/equifax-legal/

Sagan, A., & Thomson, S. (2016). *Voluntary health insurance in Europe: Role and regulation*. United Kingdom: World Health Organization.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6th ed.). Pearson Education Limited.

Statista. (2017a). • Number of social media users worldwide 2010-2021 | Statista. Retrieved August 2, 2017, from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Statista. (2017b). Global social media market size 2013-2019 | Statistic. Retrieved August 2, 2017, from https://www.statista.com/statistics/562397/worldwide-revenue-from-social-media/

Taylor, H. (2016, February 5). An inside look at what's driving the hacking economyitle. *CNBC*. Retrieved from http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html

Taylor, K. (2015). *Connected health: How digital technology is transforming health and social care*. *Deloitte*. London.

Vaughan, E. J., & Vaughan, T. M. (2007). *Fundamentals of risk and insurance*. *The Journal of Risk and Insurance* (Vol. 57). https://doi.org/10.2307/252935

World Bank. (2017). GDP (current US$) | Data. In *World Bank*. World Bank. Retrieved from

http://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DK

Zeppos, N. W., & Wallach, P. A. (2017, December). Tracking deregulation in the Trump era. *The Brookings Institution*. Retrieved from https://www.brookings.edu/blog/fixgov/2017/12/05/tracking-deregulation-in-the-trump-era/