UNIVERSITY OF LJUBLJANA

SCHOOL OF ECONOMICS AND BUSINESS

MASTER'S THESIS

THE IMPACT OF GENERAL DATA PROTECTION REGULATION ON COMPANIES

Ljubljana, June 2019 HANA GABER

AUTHORSHIP STATEMENT

The undersigned Hana Gaber, a student at the University of Ljubljana, School of Economics and Business, (hereinafter: SEB LU), the author of this written final work of studies with the title The Impact of General Data Protection Regulation on Companies, prepared under supervision of red. prof. dr. Aljoša Valentinčič

DECLARE

1. this written final work of studies to be based on the results of my own research;

2. the printed form of this written final work of studies to be identical to its electronic form;

3. the text of this written final work of studies to be language-edited and technically in adherence with the SEB LU's Technical Guidelines for Written Works, which means that I cited and/or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU's Technical Guidelines for Written Works;

4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offense and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;

5. to be aware of the consequences a proven plagiarism charge based on the this written final work could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;

6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;

7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained the permission of the Ethics Committee;

8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;

9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;

10. my consent to the publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

Ljubljana, 20.06.2019 Author's signature: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF APPENDICES

INTRODUCTION

Nowadays we are observing a major shift in the world's perception of privacy, both caused and reflected in the rise of potential threats and attempts for its protection. This trend is related to modern technological capabilities to collect and analyse enormous amounts of data, which enable connectivity of this data between different data sets, including those with identifiable information, ultimately linking this data to individuals.

Such technological innovation therefore allows companies and governments to process personal data in once unimaginable ways, introducing completely new challenges for privacy protection. Entities processing such data gain valuable insights into every aspect of human behaviour and these insights can be used for better or for worse. They can strengthen domestic and global security on one hand, or enable Orwellian-like surveillance on the other. They can be used to improve products and user experience or manipulate a person's political opinion and directly effect the election results. Too often, it is the worse of the two.

Despite obvious threats, we are not seeing an equally strong reaction from the public. While ignorance regarding how the information technology (hereinafter: IT) works and how our data is being used could explain why people are not more actively involved in protecting our privacy, convenience could also be the answer. Modern society is willing to trade off privacy for free apps and personalised user experience. In an interview for Harvard Law Today, a cybersecurity expert Bruce Schneier sums it up by saying: "*In the internet era, consumers seem increasingly resigned to giving up fundamental aspects of their privacy for convenience in using their phones and computers, and have grudgingly accepted that being monitored by corporations and even governments is just a fact of modern life"* (Schneier, 2017).

The European Union (hereinafter: EU) has a plan of its own to tackle the privacy issue and there is no better manifestation of it than **The General Data Protection Regulation (hereinafter: GDPR or Regulation**). GDPR is a result of governmental understanding that new technological advances also mean old rules regarding privacy are no longer sufficient and that regulative changes concerning privacy need to be on the frontier of national, global and business strategies. In the words of the European Data Protection Supervisor: "*Over the last 25 years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed."* (European Data Protection Supervisor, 2016). In May 2018, GDPR officially repealed the EU Directive 95/46/EC and became the new standard for personal data protection. But there was a twist that gave whole new gravity to an EU regulation - not only were these strict new standards binding for European companies, but for *any* company processing personal data of European citizens, regardless of the company location. This means that GDPR's territorial and material scope is incredibly wide, potentially affecting more companies than any other regulation and resulting in major financial consequences for

companies due to strict and wide set of requirements for companies that are processing personal data. And as it turns out, there is hardly any company that does not processing personal data.

In this thesis, we will limit our research on micro-economic aspects of GDPR, therefore focusing on companies as one of its stakeholders. Our aim is to analyse currently available data and trends in order to understand GDPR's impact on companies across the globe. We will try to investigate the magnitude and source of this impact and understand which factors influence it the most.

In our research, we will also touch on a very important element of regulation that is much less talked about or even exposed as an issue, but extremely relevant for companies - the rising cost of compliance. If and when addressed, it is usually talked about in terms of more regulated industries (e.g. finance), but it seems like this trend of rising regulation and complementary costs of compliance are becoming industry neutral and GDPR has greatly contributed to that as well. At WebSummit, the largest tech conference in the world, Andy O'Donoghue emphasized that with a statement: "*It's the first time where a regulation is blanketed across everyone. Usually it's in financial services or insurance or healthcare, but now we are starting to see regulation hit every industry and GDPR was one of the first to really have a pretty wide berth in terms of who gets impacted"* (O'Donoghue, 2018).

Considering this aspect, we will also investigate if and where there is breakeven point in GDPR's case, where company's pursuance of its compliance actually forces the company to act economically irrational and what this potentially means for the future of regulatory compliance. After beginning our analysis by extracting elements of all legal characteristics that are vital for our financial impact analysis, we will approach our research questions in the following way:

- identification and analysis of all potential negative impacts resulting in company costs related to GDPR compliance;
- identification and analysis of all potential positive impacts resulting in company benefits related to GDPR compliance;
- investigating which factors influence these potential costs and benefits and understand if such factors are related to individual companies, regulatory requirements or a combination of both.

We will use general cost and/or benefit analysis approach and apply to it GDPR's case, mostly focusing on models for calculating the cost of compliance. In order to understand not only the wider impact of GDPR, but specific implication as well, we will also perform a detailed analysis of GDPR's effects on a particular company. We will use the case-study approach by gaining access to company's data, enabling us to investigate actual costs and benefits occurred and recognized in the process of striving for GDPR compliance.

Lastly, by comparing costs and benefits for this selected company, we will gain an understanding of company's return on investment related to GDPR and how this data can tell us about not only financial, but also ethical threats and opportunities. What happens if company's analysis shows that the costs of compliance are bigger than its benefits as maximisation of profit is still considered the basic reasoning of the decision-making process in most companies? This is one example of a questions which trigger our minds to start thinking how public and private sector can and should work together in regulatory strategy to achieve a sustainable solution with clear benefits for all stakeholders. Additionally, these are cases where ethics and social responsibility cannot be excluded from the conversation despite the money-driven business world.

The thesis will be divided into four main chapters. The first part will provide a general overview of the regulation through GDPR's background and legal context, as well as main characteristics that have contributed to its wide and global impact. We will also analyse the regulation requirements itself, focusing on parts that affect companies acting as data controllers and/or data processors. In the second part will dive into researching where do costs related to GDPR come from, how do they map with its requirements, as well as research how are they influenced by factors such as company location and company size. We will do a similar research for benefits, where we will not only focus on benefits that come with avoiding penalties, but also secondary benefits such as new service opportunities, competitive advantage and business optimization. In the third part we will analyse real-life cost and benefits related to GDPR for one Company and compare them to understand what has been the company's financial outcome as a result of investing into compliance up to this point.

While legal and financial analysis through companies' perspective will help us understand the impact level of GDPR, we will devote the final chapter to evaluate the (potential) influences of such financial metrics towards companies' decision-making process and provide a general opinion on the matter of the future of both privacy protection and compliance.

1 GDPR GENERAL OVERVIEW

1.1 GDPR background

In today's digital world, any information we seek is accessible to us within seconds due to smart, interoperable digital devices. New technologies and their diverse applications have had an enormous impact on our daily lives – from changing the way we work and do business, to how we socialize and live our private lives. Due to its impact and importance, this technology

driven era happening right now has been identified as The Fourth Industrial Revolution (hereinafter: 4IR[1]).

Its predecessor, the Third Industrial Revolution happened in the second half of the 20th century and brought us electronics, IT and automated production and showed us a new world of information sharing and processing (Davis, 2016). Half a century later, its advances are spreading across the world and being upgraded in once unimaginable ways. In 2013, United Nations (hereinafter: UN) reported that while 6 billion people have a mobile phone, only 4.5 billion have basic sanitation with access to toilets (United Nations, 2013). We are now also approaching the historical "50/50 moment" where half of the planet's population will have internet access for the first time. It is predicted to be reached in May 2019 (Sandle, 2018).

The 4IR is responsible for inventions of technological connectivity and all the different ways technology and cyberspace is currently operating and relating to each other. The devices we have built are becoming smart – they are communicating with us and with each other. Algorithms are starting to make decisions instead of people. It is the era of so-called *Internet of Things (hereinafter: IoT),* described by Forbes as *a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things* (Morgan, 2014).When compared to other three industrial revolutions occurring from 18th century onward, this one is being singled out due to some of its unique characteristics - its speed, magnitude, scope and wide range of application and effect (Marr, 2018).

Despite the obvious benefits these technological advances bring to our lives in terms of productivity, health, convenience and overall well-being, there are many potential perils that we need to collectively, as a society, protect ourselves from. We have recognised that new technology and IoT also means new problems and new solutions we need to come up with. Tim Berners Lee, the person who "invented" the World Wide Web in 1989 (which arguably makes him the person that has influenced modern life more than anyone else), started a campaign in 2018 called "A Contract for the Web". With it, he is hoping to aspire positive action in this direction. He believes a once hopeful and optimistic idea of the internet that he envisioned and created, has shown its dark side. With the campaign's aim to reach a global consensus and negotiate new rules of the modern internet, the #ForTheWeb campaign is encouraging governments, companies and people to work together and negotiate the terms of safe and valuable internet usage, as well as decide on the moral standards of our century (Sandle, 2018). Besides hate speech, cybercrime and political manipulation, abuse of our privacy through personal data processing has been pointed out by Berners-Lee as one of the most vital and problematic issues connected to 4IR.

With this rapid change in quantity and quality of data processing around the globe, data and privacy breaches become inevitable and more problematic than ever due to the magnitude of

[1] Also referred to as Industry 4.0.

data compromised and people affected. In 2013, Yahoo was attacked by a group of hackers. While initially trying to hide the attack, they later estimated that, in fact, all 3 billion of their accounts were compromised (Armerding, 2018). The fact that a single cyber-attack can affect almost half of the global population (and almost everyone that has internet access) is a good indicator of how centralised data processing actually is.
Although smaller in number of people affected, no personal data breach has been as exposed, talked about or controversial as Facebook's 2018 Cambridge Analytica (hereinafter: CA) scandal. Donald Trump's election campaign hired CA, a political data analysis company, which gained personal data from more than 50 million users from Facebook and used this data to influence their political opinion (Granville, 2018). The story was brought to life through CA's former employee and now world-famous whistle-blower Christopher Wiley exposing the company's practices. The story published on his Twitter account was picked up by media giants like The New York Times and The Observer and sent "*shockwaves around the globe, caused millions to #DeleteFacebook, and led the UK Information Commissioner's Office to fine the site the maximum penalty for failing to protect users' information. Six weeks after the story broke, Cambridge Analytica closed"* (Magee, 2018).

These types of cases indicate that the value of data is being recognized and taken advantage of*: The world's most valuable resource is no longer oil, but data"* (The Economist, 2017). As companies are coming up with new ways of monetising data, people need to be protected from companies exploiting their personal information in exchange for what seems to be free services, while in reality we are just witnessing a change in the business model - people's data is shifting into a revenue generating product. As the European Commission (hereinafter: EC) wrote: "*Data is the currency of today's digital economy. Collected, analysed and moved across the globe, personal data has acquired enormous economic significance"* (European Commission, 2018a).

But the above-mentioned Facebook scandal was not the only topic in 2018 dramatically raising awareness of the importance on online privacy issues and emphasising how there are both technical and ethical questions regarding our privacy and data handling that need more of our immediate attention - so was **GDPR.** As a regulation, it is quite an "underdog" in popularity terms, but it somehow managed to gain the public's attention and interest. Although its very public narrative mostly came from people terrified about how they will successfully implement its requirements within the prescribed timeline, it still managed one very important thing - being talked about. Get *reach* or die trying could be the motto of any important issue fighting for people's attention today and GDPR was more than successful on that note. In January 2019, European Commission revealed that "*GDPR"* had more google searches in May 2018 than "*Beyoncé*" or "*Kim Kardashian*" (European Data Protection Board, 2019).

Personal data was being protected through regulation way before GDPR came into the picture, however it was obvious that current rules are no longer serving its purpose, mainly due to two reasons:

- never before have companies had access to so much personal data on every step, a trend greatly influenced by technological expansion that came with 4IR;
- the existing regulation was not taking into account how companies doing business in a global matter can stay competitive while regulatory standards greatly varied across countries.

The Data Protection Directive 95/46/EC from 1995 had to be replaced with something that could cope with challenges of today's dynamic and globally oriented technological environment. The European Commission announced the new regulation in 2012, where they referred to it as a data privacy reform (European Commission, 2012). For the past year, GDPR has been one of the most talked about and controversial legal documents of this century. It's wide range effect on both micro (companies) and macro (countries) level across several industries has had everyone bound by its strict rules worried and sceptical about its implementation and execution in practice. A survey conducted by Netapp and published in April 2018, stated that 35% of businesses think GDPR threatens their existence due to its high financial penalties for non-compliance (Netapp, 2018).

The general discourse was negative and worrisome, because the people who were writing and talking about it were looking at GDPR from the company's side - or better yet, from the side of companies' employees and shareholders. Everyone seemed to forget that they too, are the data subjects whose data is being abused daily and that this regulation is positive in its nature, protecting individuals from companies exploiting their personal data. Although this aspect is often overlooked, miss-interpreted or both, GDPR's aim is not to restrict data processing and its transmission, but make it is secure and transparent. Apart from harmonisation, enabling free flow of data was one of its main purposes (European Parliament and the Council, 2016). But this meant, standards for when and how companies were able to do so needed to have been drastically changed.

Regardless of its tight connection to 4IR, GDPR is still technology neutral in its material scope - it is not a regulation on *digital* personal data processing, but simply data processing: "*The law protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organized in accordance with pre-defined criteria".* (European Commission, 2018b).

GDPR does not discriminate on whether data is being processed online or offline. One of the recent penalties given to companies based on GDPR violation until now reminds us of that, as the penalty was related to good old surveillance cameras: "*With the introduction of the GDPR, much focus has been put on cutting-edge technologies. However, the CCTV case out of Austria demonstrates that old-fashioned violations still matter. After all, old-fashioned technologies*

are well understood by the DPAs, making them a low-hanging fruit from the enforcement perspective" (Feiler, 2018).

However, both the incentive and practical problems have been connected to digital data processing. Additionally, the intended digitally neutral language seems to bring problems when put into practice and interpreted by companies and authorities for digital environments, where some things just do not seem to make sense. One such example is data subject's right to erasure of their personal data, while IT experts have emphasised complete deletion from backups is almost impossible in practice, so workarounds are needed (Irwin, 2018). While our research aims to present an overview of the current privacy landscape as shaped by both the regulators and companies' reactions to their requirements.

In the end, only time will tell whether GDPR was a "one hit wonder" of the Regulation world or will it succeed and be remembered as a turning point in history - a new trend that shaped the power dynamic between companies and individuals and forever changing how personal data can be treated.

1.2 Impact of GDPR's legal characteristics

We will first present the wider context and content of GDPR needed for evaluating its impact in relation to the requirements it sets out for the companies, as this is a prerequisite for analysis of the companies' reactions towards such requirements and our ability to critically evaluate them.

The General Data Protection Regulation, mostly known and referred to by its abbreviation **GDPR,** is a "*Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC"* (European Parliament and the Council, 2016). Although this legal definition might at a first glance seem too technical to be of any help, analysing its individual elements can give us great insight about GDPR's most important characteristics which create impact on companies, without even looking at the content of its articles.

1.2.1 Regulation

GDPR's full name reveals it is a *Regulation* and in EU law, the term *regulation* has a very definite meaning and therefore predictable legal effects on the different entities it applies to - that is mostly EU member states (hereinafter: Member States), EU citizens (hereinafter: Citizens) and EU companies. Every document's name therefore determines its place in the legal hierarchy and consequently its nature, power and effects.

To understand how an EU Regulation fits into European legal hierarchy, we will briefly examine how the EU legal system is structured. The European Union is both a political and economic union and currently consists of 28 Member states. Due to its unique status, it is often referred to as *sui generis*[2] occurrence in international law, because there is no other State or Union similar to it (Shaw, 1996). This ambiguity is evident on the most basic levels of its functioning. Barnard and Peers (2014) sum up its distinctive identity by saying: "*The EU in not a State, thought it exercises powers which are normally exercised by the States"* (Barnard & Peers, 2014).

The European Union Law is also unique - it has been referred to as "*a new legal order of international law"* by European Court of Justice in one of its first and landmark cases, where the EU law was put above member state law and with that becoming (in some areas and under certain conditions) directly applicable for its citizens (NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, 1963). The highest legal power of EU can be traced down to its legal sources, defined as "*something (as a constitution, treaty, custom, or statute) that provides the authority for judicial decisions and for legislation"* (Merriam - Webster, n.d.). In most sovereign countries the main source is a constitution, but EU does not have a codified constitution like most other states, as it is founded on two Treaties:

- The Treaty on European Union (hereinafter: TEU) and
- The Treaty on the Functioning of the European Union (hereinafter: TFEU).

These two treaties along with some other, less important treaties, its annexes and similar documents are referred to as **primary sources of law**. *"Every action taken by the EU is founded on the treaties. These binding agreements between EU member countries set out EU objectives, rules for EU institutions, how decisions are made and the relationship between the EU and its members"* (European Commission, 2018d). Based on these sources, Member states have given up some of their sovereignty (usually in the procedure of changing their constitution) and accepted EU as its legal authority.

A far wider category of legislative documents are the **secondary sources of law.** This is "*the body of law that comes from the principles and objectives of the treaties"* (European Commission, 2018d). This is the category where also all EU Regulations, including GDPR, fit into. Other legal instruments and documents that are classified as secondary sources of EU law are directives, decisions and agreements (European Commission, 2018f).

Identifying a legal document as part of primary or secondary law is very important, since "*the hierarchical relationship between primary and secondary law is relatively simple. A normative*

[2] Meaning *one of a kind.*

act based directly on the Treaty must comply with the Treaty itself, the Charter and the general principles of the Union Law" (Barnard & Peers, 2014).

Since GDPR is repealing Directive 95/46/EC, we can deduct that not only has the content been updated, but the legislative form has been changed from a Directive to a Regulation, giving it more power. The most relevant difference of the two legislative form lies in the direct legal effect. Regulations are enforceable in all Member states immediately, the very moment they take effect, meaning there is no procedure needed on the Member state level for the regulation to be entirely and immediately binding. The consequence is that regulations' effect on companies and citizens is the same as Member state law. If the two are contradictory, regulations are binding and overrule national legislation, which clearly indicates their supreme power.

The Directives, however, are different in that aspect - they need to be implemented into each member state's national legislation with a transition procedure by each member state respectively. Directives are still binding for member states from the moment they become effective on the EU level, however they are not effective for companies and citizens per se until the member state transitions the goal through legislative documents into their national law (Barnard & Peers, 2014).

If a Member state fails to comply with EU law, there are consequences and ways of enforcement prescribed: "*If national authorities fail to properly implement EU laws, the Commission may launch a formal infringement procedure against the country in question. If the issue is still not settled, the Commission may eventually refer the case to the European Court of Justice"* (European Commission, 2018e). This important distinction consequently also affects the content and narrative of these two legislative acts (European Union, 2019).

Directives are far less specific, while regulations need to be written in a straightforward manner due to their direct effect. Directives set a certain goal that all EU countries need to achieve, but there is a lot of discretion on the member state level on *how* exactly this goal shall be achieved. The Regulation is generally applicable and therefore becomes immediately binding to all entities it refers to. Due to these differences, the EU must put a lot of thought into examining what the best legislative form for achieving a certain goal is. While in a small number of areas the form of legal act is prescribed by the TEU (e.g. commercial policy), it is far more common that institutions can choose the form of legal act they use to attain a specific objective. The guideline or principles that is used for making such decision in the principle of proportionality - choosing the least intrusive form possible that still allows them to achieve the desired goal (Barnard & Peers, 2014).

In GDPR's case, EU was free to choose its legislative form. Due to the goal of harmonising data protection laws across Europe, regulation was chosen as the more appropriate legislative

form: "*The EU decided that one major way to enhance harmonisation through the new law was to enact it in the form of a regulation, rather than another directive"* (Bender, 2018). Since GDPR is a regulation, it became entirely and immediately binding for Member state authorities, companies and EU citizens from the very day it became effective, which was on May 25th 2018. From that day forward, Citizens could enforce the rights granted to them under GDPR and companies could hypothetically start receiving high penalties in case of non compliance. Compared to all other forms, the impact of an EU legal act is therefore the highest for its recipients whenever this act is a Regulation, as was the case here. While this shows us the gravity of GDPR due to its legal power, it does not explain why GDPR was so unique in the amount of attention it received from companies and authorities compared to other regulations.

We will investigate whether the very things that made GDPR special in this sense, are also the ones that also contributed to the amount of impact GDPR has had on companies ever since it came into existence.

1.2.2 Member state legislation

In many places in the text, the Regulation prescribes it is up to the Member states to further define and develop the application of a certain article in practice. There are more than 50 clauses in the Regulation, which are written in this way and therefore encourage Member states to fill in the blanks with their own (national) data protection laws and hence supplement GDPR in such elements (Baker McKenzie, 2018). Since GDPR is entirely binding, this is the first problem for its implementation – Companies had to start implementing the above-mentioned loose requirements. Additionally, these clauses which could at any point in time be changed or updated with specifics of national legislation.

This problem became even more relevant when some Member states failed to pass their national laws within appropriate timeline. Baker McKenzie, a multinational law firm, did a study (2018) with Member states regarding the state of national law passed until May 2018. The results were not so good:

- 7 states have passed acts which came into force on 25 May 2018;
- 19 states have published a bill, including a bill that is sitting with parliament (Slovenia included);
- 1 state has not published a bill nor has limited publicly available information on how it will implement the GDPR.

This data shows, Member states had their own issues understanding and defining how to interpret GDPR, but that this did not make it any less obligatory for companies to achieve GDPR compliance by May 25th (Baker McKenzie, 2018).

This created a lot of legal gaps and even some contradictory requirements, leaving companies in a state of general confusion and despair. Companies were mostly left without practical requirements to implement or even guidelines to follow. This level of uncertainty highly affected companies. Fast forward to 2019, Slovenian parliament still hasn't managed to pass the Personal Data Protection Act "ZVOP-2", which will replace the current statue ZVOP-1 and fully implement their GDPR requirements (Information Commissioner, 2019b).

In June 2019, it is still not certain when we can expect for the parliament to pass the law. Since the lack of national legislation cannot affect the rights and obligations granted to natural and/or legal persons under GDPR, there is currently two legislative documents defining personal data protection that Slovenian companies have to follow: GDPR and ZVOP-1. To make things even harder for companies, the two are contradictory in some points. As mentioned before, this is resolved by legal hierarchy, where Regulation overrules national legislation, whenever in conflict (Information Commissioner, 2019a).

This confusion, however, seems minor compared to one major consequence of not passing national legislation in line with GDPR. One very clear obligation for Member states set out by GDPR is to officially name a *Supervisory Authority*, which will be responsible for controlling compliance across a Member state and issuing penalties for non-compliance, among other things. At this moment, Slovenia officially does not have a body with this authority, despite the fact it is clear that data protection control will continue to be in the hands of Information Commissioner. From companies' perspective, there could be major upsides to this - the fear of receiving any kind of GDPR related penalty is most likely postponed to the day ZVOP-2 comes into effect.

One final issue related to Member state legislation is connected to the unification of data protection law across Europe. Because each Member state has the right and the obligation to fill in the blanks of the GDPR's open clauses on its own terms, it somewhat defeats the purpose of unifying personal data legislation across Europe. Harmonisation was one of the main goals of GDPR, which was supposed to enable easier free flow of data in a safe and secure way. This aspect always been highly emphasised by the EU as well: "*In other words, instead of each country having their own data protection laws, now the entire EU is governed by a single regulation. Thus, a company operating in different countries no longer needs to comply with multiple — often differing — regulations Instead, they only need to conform to the GDPR in order to offer their services anywhere in the EU"* (European Commission, 2018c).

While it may seem as if EU is "outsourcing" practical solutions to Member states, there are possible explanations this was intentional and considered the most optimal: "*Perhaps this diversity results from a desire on the part of the enacting EU institutions to allow some minimal latitude to the states (even though that would create dissonance, rather than harmony). More*

likely, those EU institutions found it necessary to provide this flexibility in order to get the GDPR enacted in the first place" (Bender, 2018).

To sum up, the legal nature of GDPR as a Regulation had very clear requirements for companies, while in practice there were two main problems connected with legislation that prevented companies to achieve compliance in due time:

- open clauses that needed further instructions implemented by their national legislation, which was not prepared in time;
- "directive-like" theoretical requirements that were unclear in practical terms or not applicable in all use-cases, especially related to modern technology;

Both contributed to making GDPR implementation more difficult for companies, which negatively affects the companies due to high levels of uncertainty.

1.2.3 Effective Date of GDPR

There is a certain time period in EU law between the moment a certain legislation is officially and publicly announced and its effective date, which is the date when it actually enters into force. In legal terms, this period between adoption and enforcement is referred to as *vacatio legis.* The logic behind it is quite simple: entities affected by a certain new legislative act need some time of adjustment before it takes effect: *"The purpose of this period of time is to create a possibility of acquaintance with the new law before it begins to obtain. Moreover, this period should let us adapt and prepare to new conditions"* (Kasprzyk, 2016). In Slovenia, *vacatio legis* is also mentioned is in the Constitution in Article 154, where it is defined that all legislative acts need to be publicly announced before they can become effective and that if not defined otherwise, this period lasts for 15 days (Constitution of the Republic of Slovenia, 1991).

If we take into account *vacatio legis'* main purpose, the length of this period offers some valid insight into how much time authorities believe is necessary for preparation and/or compliance. GDPR was announced on April 27th 2016, but only came into effect of May 25th 2018 (European Parliament and the Council, 2016). The long, two-year transition period in the case of GDPR indicates the gravity of this Regulation has been recognised by regulators and as they predicted the impact level to be significant. It has been evaluated by the European Commission that Member states and companies would need 2 years time to successfully implement and prepare for GDPR taking effect.

1.2.4 Increased territorial scope

The final legal aspect which we will introduce due to its relevancy for company impact evaluation is GDPR's territorial scope – "*a geographical area where something applies"* (Translegal, 2019).

EU has been known for its highly regulated environment in many areas. While in general, this is positive for the quality of life for EU Citizens, it has not been easy for EU companies to adhere to the strict regulatory requirements, while staying competitive on the global market. GDPR came with a twist called increased territorial scope: GDPR predicts that the Regulation applies not only to companies in the EU, but also to companies *outside* EU if and when they are processing personal data of subjects in the EU. The territorial scope of GDPR was so unconventional and surprising that it was one of the reasons GDPR received so much world-wide attention: "*The GDPR encompasses a number of game changing concepts but increased territorial scope is arguably the most significant change to the data privacy regulatory landscape*" (Hewett, 2017).

The legal grounds for this can be found in Article 3/2 of GDPR, defining that this Regulation also applies to companies not established in the European Union, as long as the data subject of whom the data is being processed is from the EU: "*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of data subject is required, to such data subjects in the Union;…"* (European Parliament and the Council, 2016). All of a sudden, the scope of the Regulation is framed around the location of a person whose data the company is processing, instead of the location of the company, which is usually the case with any regulation in general. This has sparked so many questions from companies which tried to evaluate whether it also applies to them and to what extent, that the European Data Protection Board (hereinafter: EDPB) released an official 23-page document just regarding this issue called "*Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation*" in November 2018 (European Data Protection Board, 2018).

A bit unconventional, yet interesting proof of territorial scope relevance regarding GDPR has happened to me while doing my research: when I googled the query *territorial scope* in search for a legal definition (and we need to keep in mind this is a general legal concept applicable to any legal system and any legislation), all of my first 10 organic (not paid) search results were related to GDPR. It seems like increased territorial scope was EU's hook to get the whole world to listen - and it was a successful one indeed.

All these legal elements have not only helped us understand GDPR's main characteristic, but already enabled us to do a basic assessment of GDPR's impact on companies:

- due to its legislative form as a Regulation, the impact was more severe, since it was direct and immediate;
- problems with member state legislation, as in May 2019 not all Member states have even managed to adapt their own legal system to GDPR increased impact through extreme unpredictability and lack of practical guidelines;
- the two-year transition period could be considered as something that alleviates immediate impact and post-pones it, since it is a very long adjustment period. However, at the same time, a Regulation that needs such a long transition period probably has a very high impact, hence the long period in the first place;
- the increased territorial scope indicated higher impact due to the much higher number of companies impacted in the first place. GDPR's global effect and "world-wide" panic is not only due to very high fines, but the fact that the European Regulation all of a sudden becomes applicable outside the EU, as long as the data that is being processed "belongs" to European citizens.

European Union is facing legal challenges of its own - it will have to find solutions of enforcing GDPR's external territorial scope, which brings us into the sphere of international law policies and practices. While international law solutions are not relevant for our analysis, this issue deserves being mentioned since it may impact the non-compliance risk in a great way. This will be analysed later on in relation to company location impact comparison. The second step of our impact analysis is focusing on the actual requirements in order to evaluate their impact later. In the end, all costs and benefits originate from the Regulation's content, so its important to at least provide a high-level overview.

1.3 GDPR Requirements

Research of GDPR's requirements will be based on the original text of the Regulation[3]. Whenever I felt an additional perspective of GDPR interpretation is needed or could offer an interesting perspective, it has been included in the analysis.

1.3.1 Material scope

The material scope of the Regulation identifies the situations or activities under which someone falls within the regulation's scope. Together with territorial scope, it gives us the answer who is GDPR relevant for and therefore which stakeholders will be impacted by getting new rights, obligations or both. While we could usually limit our analysis of GDPR related company obligation to the comparison previous and new requirements of EU's data protection legislation, this increased territorial scope makes such benchmarking irrelevant.

[3] Unless stated otherwise, the only source for this chapter has been The General Data Protection Regulation.

GDPR's official legal definition already gives us the basic overview of the material scope by saying it is a Regulation "*on the protection of natural persons with regard to processing of personal data and on the free movement of such data".* GDPR therefore introduces new rules for processing personal data and is mainly relevant two entities, each on one side of the data processing spectrum:

- individuals or *natural persons* whose personal data is being processed, referred to in GDPR as the "**data subjects";**
- companies that define the purpose of processing **(hereinafter: data controllers or DC)** and/or process the data **(hereinafter: data processors or DP).**

If we use *argumentum a contrario*[4], we can therefore come to two very relevant conclusions:

- If a company is processing "personal" data of another legal person (e.g. company's phone number), this processing can never fall under the scope of personal data - it needs to be personal data from a *natural person* for it to be protected or legally relevant in terms of data processing protection: "*This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."*

- If a natural person is processing personal data of another individual, this is also excluded from GDPR's scope. If someone were to ask us for our friend's telephone number and we give it to them without asking the friend for permission first, we could all agree it was given without this person's consent (GDPR requirement for lawful processing). However, this action would *not* represent a breach of GDPR, while a company doing the exact same thing (giving their customer's telephone number to someone else without that person's consent) would definitely be. GDPR states that clearly by stating "*This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity*" in Recital 18.

One important use-case to emphasize here is that of a sole proprietor. In Slovenian legislation, a sole proprietor is defined as a natural person, not a legal one. However, since sole proprietors act on the market in relation to their professional or commercial activity, they are bound by GDPR, despite being categorised as a natural person. This is the first important conclusion: there are two entities standing on two adversary sides in the light of GDPR - one has rights, the other has obligations:

[4] Meaning *argument from the contrary.*

- Individuals (whenever they are *not* acting in relation to professional or commercial activities such as sole proprietors, hereinafter referred to as "Individuals) are protected with GDPR by having **rights** related to their personal data;
- Companies, defined as legal person or natural persons processing personal data of an individual in relation to their professional or economic activity, are affected by having **obligations** related to processing of personal data of individuals.

While this also includes public bodies, we will for the purpose of this thesis only investigate the impact on companies in the private sector. Not only do public companies operate completely differently, they also have many exemption clauses and/or additional obligations in the Regulation. This definition of Companies only as private ones will hereinafter be used for the purpose of our analysis.

Apart from Individuals, Companies and Member states, there is one other party affected and included in GDPR by having certain rights and obligations that we haven't mentioned yet and that is the Supervisory authority. GDPR defines **supervisory authority** (hereinafter: SA) as "*an independent public authority which is established by a Member State pursuant to Article 51"*. Each Member state needs to appoint one, as this is an obligation set by GDPR for each Member state respectively. Officially appointing a Supervisory Authority has to be done with a legislative document that has adequate power in the legal hierarchy – in Slovenia, this can only be done with a legislative statue, which as mentioned, will be ZVOP-2 once it is passed and put into effect. Until then, there is no single public entity in Slovenia with the official authority to evaluate companies' action and issue non-compliance penalties. In practice, everyone knows that this role will be given to the Information Commissioner, a body that is even now releasing many materials, opinion and education on GDPR. It is also a body responsible for data protection control according to ZVOP-1, so technically they would only be "prohibited" to issue penalties related to GDPR rights and obligations.

The way such supervisory authorities are organised and operating in practice will also play an important role on the costs and benefits for companies. The SA's influence on financial effect on companies is very direct. SA in each Member state is the only ones with the authority to act upon non-compliance and decide on the penalty amount. GDPR only provides two things, which can serve as non-compliance reaction guidelines: maximum penalties and principles on which penalties should be determined. Actual amounts will then be defined on a case by case basis by the SA of each Member state. Every new penalty that is issues brings a bit more predictability for all other companies, which lowers the costs and/or raises benefits. The difference is even bigger for companies from the same Member state, as predictability is increased even more.

1.3.2 Main definitions

All criteria for GDPR relevance (material scope) mentioned above can only determine who is *hypothetically* affected by GDPR, not who necessarily is. There are material conditions that must be fulfilled as the final step and this is how the content of the Regulation narrows down the group of Individuals (protected by the Regulation) and the group of Companies (that have obligations) affected by it. For example, a company incorporated in Slovenia satisfies the territorial scope criteria. They process some data, however its all hashed[5], so there's no way of identifying people without connecting the codes by accessing a database. It seems like such company has all the pre-dispositions to fall under the data controller and processor definition, yet it all depends whether what it is in the database counts as personal data or not. Sometimes, it is one article of a 90-page long Regulation that will determine a hundred of other obligations in that text. In this case, properly evaluating whether this company falls under the material scope can only be done by properly understanding definition of **personal data processing.** Material scope relevance in this case therefore depends on properly interpreting the separation between pseudonymisation and anonymisation.

Personal data is defined in Article 4 (a) as "*any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".* There are two important parts of this definition that we need to examine, since they reveal something that on the first glance seems a bit counter-intuitive. The first really important element of this definition is the identified and/or identifiable - individual, because only such individual can be considered **the data subject**. We might think encrypting or using codes/pseudonyms would mean we are no longer dealing with personal data, but GDPR is very clear and unambiguous when it comes to this. It is clearly stated that such information is only identifiable therefore counting as personal data: "*Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the law*. (European Commission, 2018b). This means that no matter how hard we try to hide the information that creates the link to a specific individual, it is enough that can be identified at any point and by any person.*"For data to be truly anonymised, the anonymisation must be irreversible"* states the European Commission (hereinafter: EC) clearly. We therefore see that we must permanently destroy all link between data and tracing it back to a person in order to avoid falling under GDPR's scope.

Processing is defined as wide as one could possibly imagine: "*'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring,*

[5] Hashed data maps the original string of characters to data of a fixed length. An algorithm generates the hashed data, which protects the security of the original text (Google, 2019).

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;" In short – any action related to personal data in any way. Impact of GDPR on an individual company is changed enormously if they evaluate that a certain action they are performing does not count as processing or a certain piece of data does not fall under the definition of personal data.

For companies, this means the first and most important check for the main impact assessment (does GDPR apply to a particular company or not) basically comes down to understanding two definitions - *processing and personal data.* Failing to interpret one definition correctly can have enormous financial consequences – either by not pursuing required compliance or pursuing not-needed compliance. Correctly understanding and interpreting such terms in the scope of company's business is one of the biggest challenges. Companies often help themselves with case law, trying to understand how the judicial branch has interpreted the same legislation in similar use cases. When it comes to GDPR, we do not have any judicial opinions yet and only a few explanations of SA when penalties were issued. For certain aspects (like increased territorial scope as mentioned before) we do have guidelines from official EU bodies or their SA, but for most parts companies have to trust their own judgement and hope for the best. Even when directly contacting and asking the Information Commissioner for advice, their answer is not binding and does not give the companies any guarantee of correct interpretation.

In the end, for companies it all comes to being able to evaluating risks and internal compliance. The less certain you are of what you have to do to be compliant as a company, the more risk there is for potential penalties, regardless how hard you try to comply with the relevant law. This was another element contributing to high levels of uncertainty for companies and increasing the overall impact.

1.3.3 Company obligations

Company requirements are the basis of evaluating GDPR's impact for companies, as these requirements define actions which translate to either costs or benefits related to it. The Regulatory Compliance Cost Measurement Framework, which we will use for GDPR cost analysis, predicts such requirements scanning as the first step for cost calculation, saying we begin the analysis in the following way: "*Define the regulatory activities that impose a compliance cost*", which can only be performed by working through the requirements. (Asia-Pacific Economic Cooperation; Ministry of Justice, n.d.).

GDPR Obligations for Companies can be divided into two groups. The first group are the active obligations, which are explicitly states as obligations of data controllers and/or processors. The second ones are passive obligations as they are a direct reflection of data subject's rights. Below

is a very summarized list of obligations for companies that either collect and define purpose(s) of personal data processing, actually process such data or both:

- Every personal data processing shall be lawful, which can be achieved through one of 6 criteria (legitimate interest, performance of a contract and consent being the most commonly used ones). This is true for all personal data, including the one collected prior to GDPR taking effect. The lawfulness is a condition for every purpose of *processing*, not only for every data subject[6];

- Whenever personal data is collected or obtained, there is an exhaustive list of information that need to be provided to the data subject (defined in Article 13 and 14);

- Companies need to ensure their data subject the following rights (Articles 15–22):
- right of **access**
- right of **rectification and erasure**
- right to **restriction of processing**
- right to **data portability**
- right to **object and automated individual decision making**

- Implementing appropriate **technical and organisational measures** for ensuring and demonstrating of compliance;

- Ensuring **security** of processing, at least through implementation of pseudonymisation, encryption, confidentiality, availability, resilience etc.;

- Implementing **notification of personal data breach** procedures, which have a notification response time of less than 72 hours;

- Implementing **data protection impact assessments**;

- For Companies not in the Union, **designating a representative** in the Union;

- Designating a **Data Protection Officer** (hereinafter: DPO) if certain criteria are satisfied, mostly related to the amount of personal data processing;

- Clear **instructions** for each processing purpose from DC to DP through agreements;

[6] If a data subject has given consent to process their e-mail for the purpose of informing them regarding a prize game they joined, you need a different legal basis if you want to use that e-mail for another purpose.

These bullet points are very high-level obligations that bring come form of costs to companies and as we will see, implementing some of these requirements sometimes also brings benefits. How exactly these requirements translate into costs (and/or benefits), in what phases and what influences its magnitude is what we will explore in the second part of our GDPR impact analysis.

2 COSTS AND BENEFITS OF GDPR

2.1 Research outline and method

2.1.1 Potential costs and benefits

We will analyse the microeconomic impact of GDPR through its financial impact, which are recognized as either costs or as benefits companies encounter and are related to GDPR compliance. As we are taking into account all companies in order to gain a general understanding of the impact, we will be examining the impact in the following way:

- Identifying all potential costs that occur in the process of GDPR compliance;
- Identifying all potential benefits that companies might get with GDPR compliance;
- Understanding to where in the process of achieving compliance do these costs and benefits occur;
- Identifying which of their characteristics or action might increase or decrease such identified costs and benefits.

We will not completely neglect the social, ethical and moral challenges and opportunities GDPR imposes, regardless of their macro-economic nature or indirect impact of the financial aspect of the company. These types of impacts are mostly referred to as social benefits and costs and appraise the efficiency of private projects from a public interest viewpoint (Campbell & Brown, 2016). However, they will be discussed separately in the final part of this thesis.

2.1.2 Method

The impact is divided into two groups: positive and negative impact. In our case, the negative impact accounts for all things which result (either directly or indirectly) in company costs. One might argue that things like *"reputational damage"* are then excluded, but we must keep in mind that such (relevant) consequences always eventually convert to a financial cost. By looking at all potential costs, we will therefore account for such aspects as well. Benefits, as the word itself implies, account for all the positive impacts, which again have a financial result, either through increased revenue, decreased cost and/or avoided cost.

The first part of this financial analysis will be done through a detailed investigation of (a) costs of company's GDPR compliance activities and (b) benefits of company's GDPR compliance activities. In part (a), we will investigate methods used for calculating cost of compliance in general, and apply them to the case of GDPR with the data that is available. We will also examine the trends, statistics and opinions that might affect our topic of analysis and determine which company parameters might affect the recognised costs in either positive or negative way. For additional structure, we will try to identify potential compliance costs in accordance of the company process of implementation. This will allow us to recognize the steps or phases companies undertake on their path towards compliance and evaluate occurring costs at the same time.

For part (b) we will use a similar approach, although it is expected that more assumptions will be needed, since it is too early to see and understand all potential benefits GDPR compliance might bring for the companies. This slight unbalance of uncertainty is understandable, since for compliance implementation projects, costs always come before the benefits.

In the first part we will not focus on any specific type of company, quite the contrary – we will look at companies in general and try to understand which internal and external factors influenced their related costs and benefits. This part will present a general framework from which a case-study will be approached, where we will investigate costs that occurred for one specific company based on data provided from them. We will also analyse benefits from their perspective, taking into account company characteristics that affect it. Benefits will need more assumptions than costs, as they will be analysed *ex ante*, while the costs will be analysed *ex post*.

2.1.3 Compliance vs. non – compliance

If we have GDPR compliance on one side, its direct opposite is non-compliance with every single requirement. Because they are the exact opposite, they are by default also mutually exclusive and therefore cannot and should not be grouped together. This is important in applying to our costs vs benefits analysis, as we can easily count actions from both of these situations as "costs" and wrongly put them on the same side of the equation.

This does not mean we will assume compliance as the only option. But we need to take either compliance or non-compliance as default in order to make the analysis. Our **costs section** will therefore include only the costs that are related to compliance. All non-compliance costs (e.g. paying the fines) therefore go to the other side of the equation and shall be analysed as benefits of compliance since avoided. In that aspect also benefits will be "assuming" compliance in terms of calculation. They could have been tackled also with a vice versa approach, since consistency is key: if you choose not comply with this regulation, your costs would equal only to non-compliance costs (e.g. paying the fines) and your benefits would then change to not

having the costs for compliance (e.g. saving much on implementation costs). If in that case the costs outweigh the benefits, it would make financial sense to actually pursue compliance. In our approach, the exact opposite conclusion could be made.

2.2 GDPR related costs for companies

2.2.1 General costs overview

2.2.1.1 Accounting vs. economic costs

Costs are a widely known term we use in everyday life whenever talking about the things we spend our resources for. However, in economic theory, a cost can have a very definite meaning, depending in what context we use it. The first important delimitation is the difference between two types of costs: economic costs and accounting costs. In accounting, the costs are strictly separated from expenses: *"The difference between cost and expense is that cost identifies an expenditure, while expense refers to the consumption of the item acquired"* (Bragg, 2018). In Slovenia, accounting costs are regulated by law and defined in Slovenian Accounting Standards, which were adopted by the Slovenian Institute of Auditors on the basis of national legislation, defined in Companies Act, Article 54/7 (Companies Act, 2006). The legislation also explicitly states that such standards need to be in line with the EU Directive 2013/34/EU (which came into effect in 2015) and international accounting standards (ZGD-1, article 9), implying that definitions regarding accounting costs are harmonized not only across the EU, but internationally. But how we look at costs in accounting again differs from other economic fields.

The main difference between accounting and economic costs is based on the idea of how broadly we want look at costs. Which concept is more appropriate in a certain situation mainly depends on why we are interested in measuring them in the first place. Accounting costs are very direct in their nature, while economic costs incorporate a broad set of criteria, offering a wider interpretation. Economic costs are an overarching term – they always include all accounting costs, but also take into account some other costs, which are referred to as implicit. Accounting costs are explicit costs, which have a direct monetary value which needs to be spent by a company in order to receive a certain benefit (Hawks, 2019).

The economic costs are wider, because they also include opportunity costs. These relate to the value of the goods and services which would have been produced by the land, labour, capital and material inputs (explicit accounting costs) if they would not be spent to achieve this goal (benefit of spent accounting costs), but another one (Campbell & Brown, 2016). We can also say that accounting costs are explicit opportunity costs, because this is the money the company could have spent on something else. The main addition are therefore the implicit opportunity costs, which are profits from other, non-executed projects (Khan, 2014)

The vital (and also the most difficult) part of economic costs is correctly evaluating how this money would have been spent otherwise and what value would it bring, if that particular goal would not have been pursued by the company: "*You can calculate the economic cost by finding the difference between the chosen economic activity and the alternative economic activity"* (Grimsey, 2019).

The opportunity cost in GDPR's case would be the follows: company evaluates they need to hire a Data protection officer, because this is one of GDPR's requirements for company processing of large amounts personal data. The salary for Data protection officer is around 60,000 USD per year. (CW Jobs, 2019). If it weren't for this requirement, the company could have put this money into something else, for example hire an additional sales person for the same salary. The salary represents an accounting costs, while the economic costs would besides the salary also account for all revenue this sales person would have generated for the company. Evaluating economic costs is very subjective, since the alternative "project" one would undertake is a hypothetical scenario that we are investigating and involves understanding the company roadmap or strategy.

While in the case of a single company we would mainly be interested in the economic costs, we will focus on accounting costs for the first part of the impact analysis. The reason is that while (potential) accounting costs occurring from activities related to GDPR compliance can be analyzed for companies in general, opportunity costs are too company specific. Opportunity costs will be included in the second part of this analysis, where one company's compliance project will be evaluated.

2.2.1.2 Cost of compliance – general overview

Due to the fact that GDPR is a new Regulation, there are no publicly available studies or existing company analyses describing and revealing the cost analysis of their GDPR compliance projects. An additional reason is also that this usually very confidential information and companies do not want to reveal such data.

Nevertheless, the cost of compliance is a well-known financial term that companies use to evaluate their cumulative costs for complying with all regulatory requirements relevant for them. In this case it's easier, because companies are not revealing any particular "compliance" status which could potentially provide data showing non-compliance or reveal some valid insight for company's competitors.

Investopedia defines compliance costs as "*the ongoing price for following the rules as they are"* and *"all the expenses that a firm incurs in order to adhere to industry regulations"* (Kenton, 2018). They are all the company costs that occur as a consequence of following governmental requirements that apply for a company - local, national and international,

depending on how globally the company is operating. It includes everything from the salaries of people, to implementing and maintaining new systems and processes. (Kenton, 2018).
It has nothing to do with a particular regulation (like GDPR), but is meant as general compliance applicable to your company at any given point in time.

The Organisation for Economic Co-operation and Development (hereinafter: OECD) uses the term "regulatory costs" and defines it as "*all of the costs attributable to the adoption of a regulatory requirement, whether direct or indirect in nature and whether borne by business, consumers, government and its respective authorities (i.e. taxpayers) or other groups."* (Regulatory Policy Committee, 2015). In 2014, OECD published a document, which serves as a guideline for Member state officials responsible for regulatory compliance. Some categories of costs mentioned in the guidelines are specific to Member states and public authorities, but are not relevant for companies adhering to regulation, such as:

- administration & enforcement costs,
- macro-economic effects (OECD, 2014).

While those costs are of course also present also in GDPR's case, our focus remain are the business - related costs. OECD differentiates regulatory from compliance costs identifies compliance costs as "*the costs that are incurred by businesses or other parties at whom regulation may be targeted in undertaking actions necessary to comply with the regulatory requirements"* (OECD, 2014). For our research therefore only compliance costs will be researched and even here we won't be investigating costs of Supervisory authorities, although they would fall under compliance costs category.

Regulations that highly affect companies, are usually very industry specific. Forbes stated in 2014 that the top industries affected by regulatory compliance were health and finance. Already then, leaders of the industry were concerned about this new trend they were witnessing, where regulations are impacting businesses more than economy. Tim Zuber, the regulatory center leader at KPMG, one the "BIG 4" global auditing houses, was quoted in that same Forbes article saying that "*the global pace of regulatory change is accelerating*". Main concern of industry leaders? Cost. "*Regulatory compliance can add costs, slow down processes and restrict expansion"* says Moreno. In highly regulated industries, costs of compliance are so big, they can become one of the vital elements of the company's cost structure and planning. Even more so, compliance issues can make companies change their business model and organizational structure (Moreno, 2014).

In the Food and Beverage industry, they have detected a 22% surge between 2015 and 2016 of recalls related to food safety, which results in billions of dollars in associated costs for the industry (Locke & Barnes, 2018). Not only industries, also specific territories are much more inclined towards regulation than other. European Union is known to be one of the most

regulated markets, *which "seems to have a regulation for every imaginable business practice."* (Kenton, 2018). Brief check of EU statistics heavily supports this point. In 2017 alone, the EU adopted 91 basic and 158 amending Regulations, as well as 6 basic and 20 amending directives (Publications Office, 2019). One can only imagine how exhausting and costly only keeping up with these regulatory changes is for European companies, yet alone implement all necessary actions for each new act that demands compliance from companies. In 2013, KPMG conducted a study about the costs of compliance in the hedge fund sector, which was done in collaboration with Alternative Investment Management Association (hereinafter: AIMA) and Management Funds Association (hereinafter: MFA). According to their research, the cost of regulatory compliance for the entire industry was more than USD 3 billion and was expected to grow in the next years. They also state in the report: "*The industry is investing heavily in compliance on average spending more than 7 percent of their total operating costs on compliance technology, headcount or strategy"* (KPMG, AIMA & MFA, 2013).

The issue of the rising cost of compliance was also heavily emphasized by Eurochambers in a study that showed the scale of the challenge regulation presents for EU businesses, briefly even connotating its role in EU's (nonsufficient) growth, stating that *"regulation has been growing much faster than the economies"* (Ambler, Chittenden & Bashir, 2019). Even more shocking that their opinion on the gravity of regulatory burden are the estimated costs: "*The study's findings demonstrate vividly the scale of the challenge, with an estimated overall EU regulatory cost to business of approximately €1 trillion. This figure confirms that complying with EU regulations and the associated reporting obligations account for a significant percentage of EU GDP"* (Ambler, Chittenden & Bashir, 2019).

Along came GDPR - international and industry neutral, affecting almost everyone. This applicability across different industries has also been one of the reasons why GDPR's impact has been so huge. "*GDPR holds companies of all sizes to account*," Facebook Chief Operating Officer Sheryl Sandberg said at a January 2018 conference in Brussels, shortly before the Cambridge Analytica leak was revealed. "*The law will affect almost everyone"*, she said, because businesses "*all use data to improve their services*" (Kahn, Bodoni & Nicola, 2018). Bloomberg reported a worrying estimation from Ernst & Young in March this year that "*The world's 500 biggest corporations are on track to spend a total of $7.8 billion to comply with GDPR"* (Kahn, Bodoni & Nicola, 2018). How can GDPR related costs add up to such high amounts, is what we'll be researching in the next part.

2.2.2 Cost of GDPR compliance

We will use International Standard Cost Model Manual prepared by Standard Cost Model Network and published by OECD, which is the most widely applied methodology for measuring such costs. It is a "*method that can be used to measure a single law, selected areas of legislation or to perform a baseline measurement of all legislation in a country. Furthermore,*

the SCM is also suitable for measuring simplification proposals as well as the administrative consequences of a new legislative proposal" (Coletti, 2013).

Another document, The Regulatory Compliance Cost Measurement Framework follows the same methodology (Asia-Pacific Economic Cooperation; Ministry of Justice, n.d.), where it divided these costs into 3 main categories are:

- **Direct financial costs**, which are the costs that are related to "*a concrete and direct obligation to transfer a sum of money to the Government or the competent authority"* (OECD, 2014). The main criteria of whether a cost is categorized as direct financial costs is related to whether or not such costs are remitted to the government (e.g. permits, licences, certifications etc.)

- **Administrative costs,** which are the costs related to demonstrating compliance, such as filing and submitting forms, providing records etc. In other words: *"Administrative costs are incurred by regulated entities to demonstrate compliance with the regulation"* (Asia-Pacific Economic Cooperation; Ministry of Justice, n.d.). This categorisation also differentiates between administrative costs and administrative burdens for governmental compliance with the following criteria: the burdens are the activities that businesses conduct only for the purpose of complying with the regulation, while the costs refer to activities that businesses may continue to do even if the regulation would cease to exist. We can also say that administrative burdens have no benefits for the company, while administrative costs might (OECD, 2014).

- **Substantive compliance costs**, which are costs that are related to complying with the requirements of the regulation, including delivering the outcomes being sought.

Substantive costs are very fragmented and are divided into several categories: *implementation costs, direct labour costs* (wage costs and non-wage labour costs), *overhead costs, equipment costs, material costs and external service costs*. This group is by far the most relevant for GDPR compliance, as most costs will fit into one of these categories, and will therefore fall under substantive costs, due to heavy changes GDPR predicts on all levels of business daily operations and activities.

2.2.2.1 GDPR cost categorisation

At the moment, companies can expect to not have any direct financial costs, as all certification possibilities are mentioned as options in the regulation in Article 42, where it specifically says that bodies will encourage certification mechanism, which would serve as mechanism for demonstrating compliance (European Parliament and the Council, 2016).

However, as this is not yet available, there are no transactions to governmental institutions that companies should or could make in the process of achieving GDPR compliance.
We can expect this to change, once certification becomes possible.
Administrative costs are very relevant for GDPR, as the Regulation itself emphasizes the importance of demonstrating compliance, saying that companies must "*be able to demonstrate that processing is performed in accordance with this Regulation"* (European Parliament and the Council, 2016). Specific examples of such costs are keeping of records, notification of incidents, annual reports etc.

The third category, substantive compliance costs, can be expected to be the largest, as they are related to actual implementation of requirements. Due to GDPR's heavy influences of all aspects of a company, we can assume a lot of costs to be related to human resources performing tasks to implement such changes.

For a more structural approach to potential costs analysis we will, besides categorizing costs as mentioned above, identify GDPR compliance costs as they appear in chronological order during implementation. They will be divided in 3 stages, as follows:

- **Research & Strategy costs**, which includes all costs related to company's understanding the applicability of GDPR for their business, evaluating the requirements and preparing a strategic plan on how to execute the implementation process of the steps you identified;
- **Implementation,** which are costs related to execution of all activities the company set out in their strategy to achieve compliance;
- **Maintenance** which are costs related to maintaining compliance after it has been implemented in the first place, therefore all costs related to ongoing activities and operations.

This basic outline or project phases could have been named differently, but the important part is that our implementation procedure is structured in a way that covers all potential costs that can occur. For example, Info Security Europe also list three phases, namely prepare, operate, maintain (Info Security Europe, 2019). Each phase they are describing has 5-10 sub-phases or activities, but all of them can be grouped under the 3 phases that we have identified.

All potential costs come from activities companies need to perform to achieve compliance, and each of these costs can be classified in either direct financial cost, substantive or administrative cost and happens in one of the project phases.

As we will not yet be analysing any actual costs in this part, we will also emphasize how company characteristics can influence the identified potential costs in either positive (costs are reduced or non-existing) or negative (costs are present or increased) way. The goal is to analyse

how the impact of GDPR varies from company to company and how certain main company characteristics affect these variations.

The company parameters that we will be investigating are as follows:

- **Company size,** where we will compare the impact of GDPR for small and medium-sized companies vs large corporations;
- **Company portfolio,** where we will compare SaaS vs non-SaaS business model companies;
- **Company location,** where we will compare the costs for EU vs US companies;

2.2.3 Potential costs identification by phases

2.2.3.1 Phase 1: Research & strategy

This first phase involves all costs related to the following company activities:

- understanding the applicability of the Regulation for a company (territorial and material scope);
- understanding GDPR requirements related to the business;
- making a decision whether the company will proceed with the implementation project and to what extent;
- an implementation strategy, provided the company decides to move forward with the implementation.

The above-mentioned cost incurring activities could be identified as sub-phases of the GDPR company project.

Every single company (or its relevant employee) had a moment when they first heard about GDPR and the relevant questions appeared: *"Does it apply for my company"?* We will name this sub-phase **applicability research**. In terms of costs, the applicability research phase is not that significant. This is mostly because the main purpose is solely to identify whether GDPR applies to your company or not. It is not such a time-consuming task and as mentioned before, usually the material and territorial scope is defined in two articles of the regulation. The answer was to be affirmative in any case where you were able to identify your company as a data controller or a data processor.

However, it was perhaps a phase where the biggest impact happened due to GDPR's unexpected territorial scope. All of a sudden, US companies heard that there is an EU regulation concerning data privacy which will also applies to companies outside EU. This was an important mental shift, which had an instant impact on the companies, since this potentially meant a shift in the entire company strategy. Company size is relevant only due to the company's HR structure. In-

house lawyers are almost never included in the first phase of company's organizational structure: *"Hiring in-house counsel only makes financial and logistical sense if you have a certain volume and type of legal work"* (Schmitz, 2019). But this doesn't mean data processing amount of some smaller size start-ups cannot be that of a big company – this is especially true if they are offering services online.

Small companies therefore might have a harder time figuring out if GDPR is relevant for them, because they had no legal department to turn to regarding such questions. Company location can also be relevant – while it was straightforward for EU companies that there is applicability for them (therefore they basically had no cost in this phase), the US companies were not used to dealing with EU regulation and the applicability was dependent on the location of their data subjects. Additionally, EU companies are aware of EU legislation and are much more likely to come accross its existence. This identification split the companies in two groups: the ones affected by GDPR and the ones not affected. The majority of the ones not affected were from non-EU territory, because for EU companies it is applicable by default if the company processes any kind of data. However, once such important regulations come into place, all companies must make sure to implement mechanism to be compliant in the future when either understanding of GDPR or the nature of company's business changes.

For the companies that estimated that GDPR does apply to them, came a long process of researching the requirements of GDPR. This meant not only understanding exactly which GDPR obligations you must follow as a company, but also a deep understanding how your current data processing looks like. Only then could you understand what needs to be done in order to ensure your company becomes compliant with GDPR. In the "GDPR world", this group of activities soon became widely referred to as the **GDPR gap analysis,** which represents another sub-phase. A gap analysis in its general meaning can be defined as "*A technique that businesses use to determine what steps need to be taken in order to move from its current state to its desired, future state"* (Business dicionary, 2019b). In the context of GDPR it therefore involves (a) understanding obligations based on whether the company identified itself as the data controller, the data processor or both, (b) scanning its processes, activities and operations through the GDPR perspective and (c) preparing a list of activities that should be done to achieve compliance. The gap analysis was just some of the services GDPR consultants started to offer, so companies had many chances to outsource this task instead of doing them internally. This process did not incur any administrative or maintenance – this whole sub-phase involved a lot of hours spent reading through GDPR text and comments, researching how others understand it, applying it to practical use-cases, figuring out your current data processing practices and much more. This is the part that companies needed to go perform in order to prepare a cost - benefit analysis of GDPR compliance implementation for their company. The decision could also have been that they will not implement anything at all, but such decisions were based mostly based on such assessments. Microsoft and many other big corporations shared their take on GDPR implementation with the general public, so other companies could

follow their example on the road to becoming a GDPR compliant company. Of course, Microsoft had other reasons to do so that did not have anything to do with their own good will. One very evident intention behind it, is to use GDPR content as part of their marketing and sales strategy. In this particular action plan for GDPR compliance, they are suggesting companies to use "*Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data"* (Carter, Flores & Johnson, 2018). Nevertheless, content marketing has its clear benefits for subjects it is intended for. Their GDPR related content, although provided with the business goal to "convert", still offers free and useful tips regarding the phases of implementation – the same phases we are using to identify costs in our own analysis as well. Microsoft has also identified that the first out of three phases includes the GDPR gap analysis which helps companies understand its requirements (Carter, Flores & Johnson, 2018).

Compared to the first sub-phase, these costs are already much more substantial, as companies need to engage people with a variety of skills and professions to perform the gap analysis as the basis for your company's strategy.

Company parameters again influence the amount of costs. In general, the bigger the company, the more data they normally process and the more complex the data flow and data related processes are. SaaS and technology related companies also have larger amounts of data. For SaaS providers, any customer that uses their software becomes one by creating their account with personally identifiable information. In any case, for an IT company, the digital data processing amounts are increased. After performing a gap analysis, the company now has an understanding of what GDPR requires of it.

The next step is the third and final sub-phase – **GDPR strategy.** Not using the term GDPR implementation or compliance strategy has been done on purpose. Just because GDPR is applicable to a certain company, does not automatically mean that they will pursue compliance. Non-compliance can be also a strategic decision made by a company, which can happen due to various reasons, most obvious one being on the basis of a cost-benefit analysis.

In the GDPR strategy phase, companies had to decide on three key aspects: project activities (what needs to be done), project members (who needs to do it) and project timeline (when). The last part therefore includes the decision about the financial commitment the company is willing to make for GDPR compliance. One of its most important elements, however, is also a value-based decision regarding the final goal(s) of a GDPR implementation project. As we will see later on, avoidance of penalties in not the only necessary benefit of GDPR compliance, meaning the business goals of such project can be defined very broad.

One key element potentially influencing the goal(s) definition this is the amount of data a company processes – the companies where they rely heavily on data, where this is their business

core, the impact is expected to be higher in both the cost and benefits aspect: "*A business-oriented approach is usually preferred by organisations whose core business includes personal data processing. In these organisations, the number of activities involving personal data processing and the volume of such data will be higher. Accordingly, the GDPR will have a greater impact on this type of enterprise, which will therefore identify a range of business benefits during the implementation of measures to ensure GDPR compliance"* (Ramboll, 2018).

A unique aspect of choosing an appropriate business strategy was choosing the most optimal project members. The task force needed for the GDPR project success was not so easy to identify as it might appear at a first glance: "*One particular area of confusion is around who, within companies, bears responsibility for issues related to the regulation"* (GDPR Beyond, 2017). This was due to its very unique nature of obligations, which required a combination of technical, IT, security, legal and business-operational knowledge, skills and experience. Additionally, the question of the project "task force" was not just about department that should be involved, but the level of seniority. It was often mentioned that GDPR compliance is something that the highest management needs to get involved with: *"Historically, IT has been responsible for data security and network protection, but GDPR's requirements make this a C-suite affair. This is a whole new ballgame that many didn't see coming*" (Forbes Technology Council, 2018). The versatility of GDPR related tasks is mentioned also in a PwC survey: "*The expanding budgets reflect many companies' commitment to a cross-functional approach, as at least one-third of executives surveyed said their companies have completed preparations in each of PwC's 10 standard GDPR implementation areas – with the information security, strategy and governance, and individual-rights processing workstreams leading the way"* (PwC, 2018).

In economic theory, **sunk cost** in also an important cost-related concept that (should) influence a company's decision-making process, such as GDPR implementation. Sunk cost theory suggests that costs that have already occurred should not influence the decision going forward. One of many available definitions is that this is "*money already spent and permanently lost. Sunk costs are past opportunity costs that are partially (as salvage, if any) or totally irretrievable and, therefore, should be considered irrelevant to future decision making"* (Business dictionary, 2019a). If companies were behaving economically rational, they should have categorized all costs occurring prior to their GDPR cost benefit analysis as *sunk costs*, meaning all the time and resources spent for identifying the costs and benefits with some basic estimates. The aim of this categorizations is that such costs (which have already occured) should not influence the decision regarding how much resources will the company be allocating for GDPR related purposes in the future. The gap analysis (comparing current company state with requirements of GDPR) defines the scope of project tasks and therefore is the basis for estimating costs. This is why we can assume that costs related to gap analysis should by default occur before a cost benefit analysis is made and decision is reached. This does not mean they should be disregarded in general – these are still costs that occur and should be taken into

account when evaluating the impact of GDPR on companies. Additionally, actions of a company happening before cost-benefit analysis can also bring benefits, not only costs. Doing a GDPR gap analysis means scanning the company's entire data flow from technical and organizational point of view.

Regardless of the company strategy, having made this analysis is beneficial from the operational and security perspective. Because the gap-analysis is so broad in terms of resources needed to be put into it, the decision can also be made much sooner, therefore making the gap analysis part of the actions identified in the cost-benefit analysis and in the final strategy. Due to the pressure and importance GDPR has gained among companies, we have to assume the possibility some companies decided to strive for compliance by default, without performing an internal cost-benefit comparison, as regulation often leaves companies the feeling this is not something to be decided upon, but is obligatory. In those case, the previous sub-phases could already be part of the project that we are identifying here.

2.2.3.2 Phase 2: Implementation

Actions taken and their associated costs are much harder to predict or generalise for this phase. We cannot even assume all companies will have the same sub-phases, especially in chronological terms, as we could with Phase 1, even though the scale of the sub-phases could still vary greatly across companies. Actions for implementation are unique for each company, mostly due to the following main factors:

a) the company's data processing practices:

Two similar companies can have very different data processing practices, despite their general similarities in terms of size, industry, location etc. We will support this with an example: Company A is a restaurant who does not have a website, but gets all of their customers through word of mouth and location by-passing. They collect very data, mostly related only to their employees. Company B has a very similar offering, but their marketing and sales strategy is exactly the opposite. They rely heavily on content marketing and social media channels, where they get most of their website traffic from. Their website has many hooks - places, where you leave personal information in exchange for useful content.
We can see that while company A' s implementation phase will include very few activities, (as they don't have to worry about their data flow, data processing agreements, IT structure, cyber security, hiring a data protection officer etc.), while all these actions will be the main components of Company B's GDPR implementation phase.

(b) Company's individual understanding of GDPR requirements

Companies are still waiting for practical guidelines on GDPR implementation, which would help them know exactly what are compliance milestones and which actions are needed to achieve these milestones. This is predicted within the GDPR Section 5, most specifically Article 40 (hereinafter: Codes of conduct) and Article 42 (hereinafter: Certification). When could we expect this is still unclear and until then companies are left to figure it out on their own. The current available "help" comes from three sources:

- a few official guidelines of EU bodies, which are usually related to a very narrow GDPR element (one example already mentioned was the guidelines on territorial scope);
- shared (good) practices of other companies, however due to sensibility of information, company's advice is usually either very general or "undercover" promotional content;
- content and services provided by companies that offer GDPR related activities as their service.

All this information together with the company's own understanding influenced how their process was being executed.

(c) Company's strategy they decided for in the previous phase

This is especially true for company decisions related to how much will be done in-house vs out-sourced tasks, which can completely change the implementation process. Regardless of all differences, all costs related to implementation can be divided into two groups:

- **Costs of actual implementation –** costs related to salaries of employees working on this project, costs related to payment for outsourced services (if there were any) and costs of any technology needed for implementation;
- **Costs of implemented changes –** costs related to changes in the business practices that reflect in the lost benefits of non-regulated data processing.

This second category should not be mistaken with opportunity costs. What is meant by *costs of implemented changes* is the absence of actions which used to bring benefits to the company, but are now considered "illegal". For example, under GDPR companies are not allowed to group many different (non-necessary) "data processing purposes" and pack them as *take it or leave it* policy of using company's service. The cost of implemented change also accounts for the loss of business intelligence or other business benefits (e.g. better conversions due to marketing purposes) brought by these additional data processing practices, which can now no longer be practised. Most of these costs in the phase 2 are substantive as a category, however there are some minor costs that we can classify as administrative, like obligations towards supervisory authority or direct financial costs, e.g. for new technologies used as solutions.

2.2.3.3 Phase 3: Maintenance

This last phase means all the overhead costs that occur in order to (strive to) achieve continuous compliance, as it becomes incorporated into organizational processes, operations and culture. Part od this has a direct reference in the Regulation, mentioned as data processing *by design and by default* (European Parliament and the Council, 2016).

Too often think about compliance as an end goal of an implementation project that needs to achieved. This is especially true whenever we have compliance certificates available for companies to acquire. However, compliance can only be evaluated from a particular point in time, therefore you can be fully compliant one day and be in major breach a week later. The same logic applies to all companies who did not fall under GDPR's scope up until this point, but certainly might in the future.

This is why with compliance, there is always a third group of costs associated to the ever-lasting phase of maintaining a state of compliance.
This includes:

- sustaining all implemented processes, which are mechanism to achieve compliance in every way;
- implementing compliance in the company culture and ensuring an on-going employee training and awareness;
- implementing new processes once business changes or new activities are undertaken;
- keeping track of GDPR related activities that were perhaps unclear, like judicial and supervisory authority decisions which that re-interpret compliance.

2.2.4 Opportunity costs

We briefly mentioned opportunity costs in the light of accounting vs. economic costs. With regards to compliance projects, opportunity costs are perhaps even more evident, as often it feels like pursuing compliance is a necessary burden and not a project that is an investment project which we chose instead of another project, because it made more financial sense. What would have been an alternative for each company is always hypothetical, therefore return on investment (hereinafter: ROI) of such non-realized projects are always a very rough estimate.
It is important to keep in mind that regardless of whether we can calculate them with accuracy or not, such costs always exist. The data on cost estimates that we can find and are mentioned in this thesis give some estimates, although we do not find any mention of opportunity costs, but we cannot say with accuracy whether companies have accounted for them or not in providing their data. It is not clearly stated whether opportunity costs have been taken into account or not. As we will see below, data on costs that is available show the numbers are very high, meaning companies put a lot of resources were put into GDPR.

2.2.5 General cost assessments

There are some assessments of GDPR related costs available, although we mostly estimations and predictions as opposed to actual company calculations of resources spent. One additional reason that makes it hard to make financial conclusions is the recency factor - there are not many companies that have reached compliance (excluding the maintenance elements), while all the rest are in one of the various phases and sub-phases that we have identified. With most companies being somewhere on this path, they can provide us a mix of occurred vs predicted costs. Most surveys also have their participants, segmented not only by factors like size and location, but by reached state of compliance (e.g. the PWC survey mentioned below).

Most of such information regarding costs are available through published survey results performed by other private companies – some were done before the Effective date, some after. What's clear is that numbers are high. PwC, another "Big 4" auditing giant, reports from the pre-Effective date survey that: "*Of the companies who said they have finished preparations, 88% reported spending more than $1 million on GDPR preparations and 40% reported spending more than $10 million*" (PwC, 2018). They performed their survey twice (both prior to Effective date) and saw some visible changes. Netsparker survey shows a bit lower numbers - their participant were a group of 300 C-level employees of US Companies and the results showed that "*The majority, 59.6%, will spend somewhere between $50,000 and $1 million, while 10.3% will spend more than $1 million to become GDPR compliant"* (Abela, 2018). The same survey also emphasizes the correlation between company size and cost. Statista analyzed data for UK companies, which reports that from FTSE 100 companies, the ones with more than 100.000 employees estimated costs of 49 million pounds, while companies from 1000–5000 employees' costs start at 1 million (Statista, 2018). Another estimation from The International Association of Privacy Professional estimates that Fortune's Global 500 companies will cumulatively spend about 7,8 billion USD to comply with GDPR, and the FTSE 350 1,1 billion USD (Smith, 2018).

While many factors that have the potential to increase company costs are due to some level of uncertainty, it is also important to understand that some costs could therefore be decreased by moving the time of implementation date closer (or over) the Effective date. Every new information related to GDPR (either from SA decisions, to official EU guidelines or companies sharing their good practices) can be helpful and has the potential to lower the cost.

We have now reviewed GDPR related costs from various perspectives. We have seen that companies could turn to known methodologies for predicting future costs (ex ante cost-benefit analysis), however the predictions were much harder for this project than many others, especially due to high levels of uncertainty on both costs and benefits side. Data collected until now cannot give us some insight into what activities the costs are associated

with or help us understand how costs should be (better) estimated for the future. Most importantly, such cost breakdown can give us a general feeling regarding the overall impact of GDPR on companies. Additionally, this overview has shown the range of impact on companies is very wide – any company characteristic can influence almost any identified cost. It was our goal to point out the most obvious ones and put that range in perspective.

We will continue our research by looking at all potential benefits, with the aim to get a similar holistic perspective on the positive impact effects of GDPR. As mentioned in the beginning, benefits are not only harder to estimate (even if we are making an ex post analysis). With less than a year from the Effective date of GDPR, we are mostly left with many benefit predictions that companies, authorities and other "experts" are pointing out. The limitations and variety of impact that we've identified in the costs section, will therefore be even more limiting here. Nevertheless, we will break down potential benefits of GDPR for companies – from the most obvious ones, to the ones that for now will have to stay on the theoretical level, as there is not any real data to support it yet.

2.3 GDPR related benefits for companies

When we think about regulatory benefits, we mostly associate them with macroeconomic, social benefits and identify those as the main purpose or goal or governmental intervention on the market. Society believes there are areas where companies need to change the way they work to adhere to regulatory requirements and adapt for the greater good. It is also a common belief that regulation is vital for the markets to function properly: "*No one doubts that markets require regulation in order to operate fairly yet competitively for the good of society as a whole"* (Ambler, Chittenden & Bashir, 2019). But in this thesis, we are not interested in macroeconomic benefits, but solely the benefits that GDPR compliance brings to companies, as this is the second piece of its impact.

Our first intuitive reaction when thinking what regulation bring to companies is *costs.* But at a second glance, there may be many upsides to GDPR from the company perspective as well. Sirota, the CEO of BigID company writes: "*It's a mistake for companies to view compliance with GDPR as just a financial burden. There are real benefits to be had in understanding and protecting customer data"* (Sirota, 2018). He mentions benefits such as understanding the customer, cyber insurance and civil action savings and protecting brand reputation among other (Sirota, 2018).

If we think about the cost-benefit analysis and its role in the decision-making process, it would only make sense for companies to predict larger benefits than costs in order to even undertake the compliance project in the first place. But is it really so, or is there something about "regulation", that make companies oblige even if there is no economic sense behind it? To get to some answers, we first have to breakdown all possible benefits a company can detect,

both short and long term. Some of them will be easier to be evaluated from a financial perspective than others, but this is a limitation we are aware of and has been pointed out already. We will divide the benefits into two large groups. The first group, **the primary benefits**, will be a direct result of compliance, therefore avoiding of the possible penalties of GDPR prescribed for companies who fail to follow the requirements of the regulation. We have mentioned this aspect in our thesis already: if we consider the cost of compliance on one side of the cost-benefit analysis, the other part of the equation must also presume compliance and therefore translates to benefits of not suffering non-compliance consequences, which are its penalties. The first benefit of GDPR is therefore avoiding (some level of) penalties due to reaching (some level of) compliance for each company.

The second group, **the secondary benefits**, are the ones that come out of the changes we implement to the nature of our business and business operations. They are also the benefits connected with quality of business – raising the level of business operations, processes and understanding of the data and all added value that comes through that.

2.3.1 Primary benefits – avoiding penalties

From the very beginning of GDPR's wider media presence, the penalties that await companies that will not comply with GDPR have been identified as the key change of GDPR compared to (at that time) existing legislation and one of the main reasons GDPR has gotten so much attention from companies.

The non-compliance penalties are defined in Article 83 of the General Data Protection Regulation. The penalties (or *administrative fines* as they are referred to in the text) are clearly determined in paragraphs 4 and 5, which actually splits the prescribed fines into two groups. The criteria for the division are based on the non-compliant provisions or GDPR requirements that a company fails to implement or execute properly. The fines are only determined in terms of their maximum value, which are:

- *"administrative fines up to **10.000.000 EUR,** or in the case of an undertaking, up to **2% of the total worldwide annual turnover** of the preceding financial year, whichever is higher;*

- *administrative fines up to **20.000.000 EUR,** or in the case of an undertaking, up to **4% of the total worldwide annual turnover** of the preceding financial year, whichever is higher"* (European Parliament and the Council, 2016).

These amounts do in fact represent a huge change in the impact level a single regulation brings to a microeconomic environment. Comparing the penalties to its predecessor, GDPR's fines are "*more than 20 times larger than EU member states' maximum state retributions based on Directive 95/46/EC"* (Klekovic, 2017). Regardless of how frightening these number seem at a

first glance, we must read these clauses with great precaution, just like any other legal text. The first paragraph of the same article serves a guideline for supervisory authorities who will be imposing such fines, stating that fines shall "*in each individual case be effective, proportional and dissuasive"* (European Parliament and the Council, 2016). Additionally, the whole second paragraphs gives more information on which premises should the amount of the fine be calculated. When it comes to deciding on an appropriate fine, each case will be carefully assessed and a range of factors will be taken into account, e.g.:

- the gravity/duration of the violation;
- the number of data subjects affected and level of damage suffered by them;
- the intentional character of the infringement;
- any actions taken to mitigate the damage;
- the degree of co-operation with the supervisory authority (European Parliament and the Council, 2016).

It is clear that it is in complete discretion of Supervisory authorities to evaluate the infringement of GDPR and determine the penalty amount they deem appropriate. This gives them a lot of responsibility on one side and a lot of power on the other. In also does not give companies much predictability on expected penalties for them to use in order to preform a cost-benefit analysis.

In October 2017, there was another important document published by the EU, triggered by the lack of practical guidance for Supervisory authorities on the subject – The Article 29 Working Party (which ceased to exist on the day GDPR came into force and has been replaced by the European Data Protection Board), published a document called Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, a 17-page document giving additional explanation regarding penalties "*intended for use by the supervisory authorities to ensure better application and enforcement of the Regulation and expresses their common understanding of the provisions of article 83 of the Regulation as well as its interplay with articles 58 and 70 and their corresponding recitals"* (Article 29 Data Protection Working Party, 2017).

The fact that we only have enormous maximum penalties defined and a clear incentive that basically *any* action or possible circumstance can affect its amount bring a lot of uncertainty for the companies. Needless to say, this makes it very far-fetched to do a cost-benefit analysis *ex ante*, if you can't predict whether you should be leaning towards 0 or 20.000.000 when assessing the non-compliance threats and no judicial precedency or supervisory authority decision to base the assumptions on.

The guidelines and principles that affect the penalties can, however, serve as a very good insight into what costs can bring more benefits than other and therefore which actions towards

compliance should have priority over others. If we know that factors like any "*actions taken to mitigate the damage"* and the "*degree of co-operation with the supervisory authority"* are one of the main 5 elements supervisory authorities will decide on the amount of penalties, then it makes sense for companies to allocate more of their (always limited) resources into GDPR requirements dealing with organisational measures and procedures related to breach related procedures, education and processes.

This understanding has been common among data breach cases even before GDPR. For example, such reasoning has been pointed out in a court case involving Yahoo: *"A federal judge confirmed just how beneficial Article 33 (mandatory breach notification within 72 hours) may prove to be in negating civil action costs. Yahoo was ordered to face a lawsuit claiming the personal information of three billion users was compromised in a series of breaches. The reason for facing this charge? Being too slow to disclose these breaches occurring from 2013 to 2016"* (Sirota, 2018). The Regulation does make it clear though, that while some factors may influence more than others, it the end, anything can define the final fine amount.

It seems, however, that people forget that even before GDPR's application, huge fines were waiting for the industry giants that were responsible or failed to act responsible for massive data breaches. In April 2018, Yahoo was order to pay a fine of 35 million USD by Securities and Exchange Commission (SEC). Of course, this fine was related to the Verizon investment deal and was not imposed by a SA-like institution – but still, it showed magnitude of data privacy breaches (Lynch & Volz, 2018).

We also need to keep in mind that penalties are not the only costs related to data breaches. If a company encounters a data breach, everything stops and revolves around relating the issue. It is clear that all this overhead can result in massive amounts – how big depends on the magnitude on the breach. These are non-compliance costs that bring huge opportunity costs for the company. If we take into account the goal of GDPR and its security measures, the companies who comply should have much less chance to encounter the data breach and therefore saving such potential costs (both direct and opportunity).

2.3.2 GDPR related penalties until now

While very scarce, there have already been a few cases where GDPR breaches were detected and penalised by the Member states' Supervisory authorities[7]. Until 2019, we can find reports of 3 fines in 3 Member states related to GDPR – Germany, Austria and Portugal and those 3 cases were the first examples of companies receiving fines on GDPR basis. They can give us the first peek into how we can expect personal data breaches to be treated.

[7] Data until January 25th 2019.

On 25th of January, the European Commission published an official infographic called GDPR in Number, which presents an overview of fines issued to (that) date and for that purpose, we will investigate the penalties that occurred until then. It provides a very good overview of GDPR effect – from fines, report to google searches, it is a great summary of its worldwide impact (European Data Protection Board, 2019). There were 3 known fines issued in 2018 already:

In Germany, a chat platform provider "knuddels.de" was attacked by hackers in July 2018. 2 months later, approximately 330,000 users' personal data (including passwords and email addresses) were stolen and made publicly available. The company's reaction was on point, as they informed both their users and Supervisory authority immediately. In their transparent and honest report, they also disclaimed the personal data was not encrypted (a security requirement from GDPR) (Schmidl, Lutz & Seidel, 2019). The company received a 20.000 EUR fine. This was interpreted as being a very modest fine considering the breach effect – the SA reported there were several factors influencing the lowering of the penalty: "*When deciding on the amount of the fine to be imposed, the DPA considered in particular that the platform provider:*

- *notified the breach to the DPA and to the data subject in due time*
- *cooperated fully with the DPA*
- *promptly followed the DPA's recommendations for how to increase the implemented level of data security"* (Feiler, 2018).

This case supports the guidelines mentioned before, as the actions after the beach were widely taken into account when the penalty amount was being determined by the SA of Germany. This is good news for companies, as it raises the level of predictability when it comes to SA's actions and decisions and the expected benefits of GDPR compliance.

The Austrian case dealt with an entrepreneur using a CCTV camera, which covered parts of public spaces in front of their offices. They did not have consent, but rather tried to justify this as legitimate interest. The Austrian SA disagreed with their interpretation of GDPR's legitimate interest, especially since the recordings was not properly marked. An interesting fact is exposed when we hear the justification of the SA deciding on appropriate penalty: "*Taking into account the annual income of the entrepreneur, the Austrian DPA imposed a fine of EUR 4,800 for illegal video surveillance activities"* (Feiler, 2018). This is revealing another important, but positive influencing factor - the SA actually gave the penalty according to the annual income of the entrepreneur. This is a pleasant direction that many smaller companies were hoping for. It is frightening that penalties mentioned in the Regulation are so high that you could end up shutting down your business due to 1 visit from SA. This gives hope, that all aspects will be taken into account and that is never the SA's intent to make penalties greater than necessary and could substantially hurt a company's future. If nothing else, this is proof of the proportionality principle.

The third and last case of GDPR violation in 2018 was discovered and fined by a SA happened in Portugal. A National Hospital did not comply with several GDPR requirements when they miss-used their IT system that help process patient's personal data. Due to many factors, the hospital was fined with a much higher penalty than other two cases, a whooping 400,000 EUR (Monteiro, 2019). While the hospital fought back on the claims, mostly emphasising they were using the IT system provided by the Portuguese Health Ministry, the defence was unsuccessful: *"the Portuguese DPA did not let the hospital off the hook that easily. It decided that it was the hospital's responsibility to ensure that adequate security measures were implemented"* (Feiler, 2018). Even though patients' data is considered a special category and standards for processing and protection are much higher for thus-related breaches, the fine was still quite high. But more than the penalty amount, there is another element of this case that is important for our research.

It is clear that GDPR gives Member states the obligation to officially appoint which public body shall have the Supervisory authority role. It makes sense to think that without this official appointment, no body has the authority to issue fines. Contrary to that, something else happened in the Portuguese case, IAPP reports: "*The defence submitted by the hospital referred that the CNPD could not be considered as the supervisory authority as per Article 51 because it had not yet been appointed formally. To this, CNPD responded that it is, for all purposes, the national authority which has the power to control and supervise the compliance in terms of data protection in accordance with the current Portuguese Data Protection Law"* (Monteiro, 2019).

While it is not with certainty that we can say this would argument would stand in other member states as well, especially if and how this would be interpreted by the judicial branch, but it definitely calls for some re-consideration of companies who are relying on that delay in possible penalties where national legislation has not been passed yet, like in Slovenia.

It is, however, interesting that the last Portuguese case is not mentioned on the official infographic from the European Commission, but we can find another one – Google. Google's fine is the biggest and most important GDPR-related fine that happened in January 2019. While it only remained a question of time when the supervisory authorities will fine one of the big tech companies, it might have come sooner than we have anticipated. The Supervisory authority of France fined Google with a whooping 50 million EUR fine for privacy related matters on the basis of GDPR. (European Data Protection Board, 2019). What's even more shocking is that the fine was not connected to any personal data breach (like with all other cases). According to Reuters: "*The French regulator said the world's biggest search engine lacked transparency and clarity in the way it informs users about its handling of personal data and failed to properly obtain their consent for personalized ads*" (Rosemain, 2019). CNIL, which is the French supervisory authority provided explanation and justification in a public statement, saying that: "*This is the first time that the CNIL applies the new sanction limits provided by the GDPR. The*

amount decided, and the publicity of the fine, are justified by the severity of the infringements observed regarding the essential principles of the GDPR: transparency, information and consent" (CNIL, 2019).

Not only is this a landmark case for its penalty amount, but serves as a statement of EU authorities that GDPR is much more than a threat on paper and that they more then intend to execute its power. Additionally, such cases give us more insight into the impact GDPR has and will continue to have for companies, as it brings official interpretation of the Regulation with every fine issued. On their official website, CNIL not only provided all the information on the issued fine, it presented the whole case – from its origins, official procedures to reasoning and logic behind both the infringement and penalty amount decision.

Here is what we know so far – the GDPR infringements were incentivised by groups of consumers, which emphasized Google's lack of legal basis for personalized ads. CNIL as the French SA had to cooperate with another SA in Ireland, as this is where Google's headquarters are located. Upon inspection, they found two data breaches:

- transparency and information, as the information on personalized ads are to hard to find, missing or disseminated across several document. It is also now clear to the consumer what the legal basis for personalized ads is;
- no legal basis for personalized ads, as the "consent" collected does not comply with strict rules on consent imposed by GDPR (for example, the box is pre-ticked).

When justifying 50 million EUR, they mention three very important factors that contributed to that very high number:

- these operations by Google reveal an enormous amount of people's private life due to amount of data and services and combinations between the two;
- violation is a continuous breach (ongoing);
- the importance of Google on the French market and the fact that personalized ads are one of the main parts of their business model (CNIL, 2019).

Such explanations provide companies with reasoning and logic, which at least for now seem to be quite coordinated among all 4 Supervisory authorities that issued fines until now. While the whole system is complex, we can definitely see that all penalties really did strive for the principle of proportionality.

Apart from these few cases, companies are mostly still waiting and wondering what the (GDPR) future holds. It's worth mentioning, that we can start observing consumer-related actions raising awareness of personal data importance also elsewhere. People are waking up and putting pressure on regulators to start imposing fines on the tech giants. In the end of November 2018,

Reuters reports: "Consumer agencies in the Netherlands, Poland and five other European Union *countries asked privacy regulators on Tuesday to take action against Google for allegedly tracking the movements of millions of users in breach of the bloc's new privacy law"* (Chee, 2018). A similar incentive already cost Google (at least) 50 million EUR and this does seem to show a lot of consumer power in that respect.

From what we can see and observe at the moments is two things. While hearing about issued fines can be frightening and serves as a reminder GDPR doesn't only exist on paper, it does highly contribute to predictability. The more cases that we know of, the more we will be able to rely on the reasoning Supervisory authorities show in their decision for penalty amounts. It is very important for companies to keep up with their decision and adapt accordingly, which is part of their maintenance cost as well. Additionally, it seems like all the things that the company did to prevent a breach or infringement will be positively taken into account for the calculation of the fine – the more you have spent and the better your implementation was, the more likely it is your sentence will be reduced and companies will be rewarded for trying. To put it in the cost-benefit perspective: the money you spent on GDPR will pay off by getting a smaller (or no) fine in cases where you are in breach. This logic implies for an unusual occurrence where costs are reflected as benefits by default, regardless of what they were spent on. Also, all factors that account for how much data has been compromised is considered and contributes (in both ways) to the final penalty.

2.3.3 Secondary benefits

2.3.3.1 Business benefits

Upon releasing their press release (which in practice looks more like an FAQ page), the European Commission answers one of the questions is exactly what we have been wondering all along – while everyone is talking about costs of the upcoming regulation for businesses and benefits for the citizens, is there something good in it for the companies too? European Commission sure does think so. For "What are the benefits for the businesses?" they do not have a problem coming up with more than a few ideas in their official answer.
In general, EC states, that GDPR brings harmonisation: "*The reform provides clarity and consistency of the rules to be applied, and restores trust of the consumer, thus allowing undertakings to seize fully the opportunities in the Digital Single Market*" (European Commission, 2018a). In practice, this is yet to be proven, but national legislation delays are not working in the favour of this argument. The digital single market's basic idea is to avoid having 28 "digital" markets, with each Member state having their rules and legislation in the digitally related matters.

Such regulatory dispersion makes it very hard for companies to be compliant with applicable laws while operating on the global (or even just European) markets. While harmonisation surely

is a huge benefit for companies, one could argue GDPR did not manage to provide that – at least not. GDPR has many open clauses, meaning that hypothetically a French legislation on data protection might differ to a Slovene one, complicating compliance for companies working on a global market. Perhaps this will be changes or at least improved when certification mechanism shall be implemented and available, but according to Information Commissioner of Slovenia, it is a complex and time consuming task without any clear timeline yet (Information Commissioner, 2019a).

Despite all issues, having a global standard on (personal) data protection – and GDPR has managed to become that – gives companies the same direction and a unified level of importance. The fact that its applicability goes beyond the territorial scope of Europe, also means companies that have high data protection standards (which cost them severe amounts) will no longer suffer and be uncompetitive due to their regulatory restriction. Now everyone has to do it. EC describes this aspect benefit as "***The same rules for all companies – regardless of where they are established"*** saying: *"Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business in our Single Market. With the reform, companies based outside of Europe will have to apply the same rules when they offer goods or services on the EU market. This creates a level playing field"* (European Commission, 2018a). Additionally, this does not only bring benefit for globally active countries that will now have the benefit of "*one continent, one law*", it works as a stimulator as well. Companies will now have less entry costs to enter the market of European countries, as the entry costs from the data protection regulation protection does not increase if you operate on 1 or 28 European markets. If companies do not decide the costs of complying will be too big and they'd rather exclude European markets completely, this might bring new businesses to the continent and make Europe a more active and important player in the global economic market.

Although not obvious at a first glance, there are also some rights of the data subjects (which seem as a negative element for businesses) that are seen as company benefits from EU's standpoint. One such example is the data portability right, described in Article 20 of GDPR. It describes the right of a person to get all their data from the data controller (which comes with the data subject's right to access) in a structured, commonly used and machine-readable format and transmit those data to another provider. This touches the subject of what we know in the marketing field as "consumer switching", which *"refers to customers abandoning a product or service in favour of a competitor's"* (Mack, 2018).

While making it harder to keep your customers and have a high retention rate seems like a bad thing for businesses, it's a great thing if you are the company the customer is switching to. Not being able to lock the users down to a single provider is something the regulators see as a positive thing for businesses as it creates a more healthy, competitive market, where companies can have more equal chances of attracting customers. This is extremely important for smaller companies or the ones just getting started in the business, especially when competing against

the tech giants: "*Start-ups and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions. This will make the European economy more competitive"* EC adds (European Commission, 2018a).

While strict regulation is always hard to comply with, it also makes the company "tidy up" their day to day business. The blessing and the curse of GDPR is that is omni-present and affects all departments and almost all processes – even if just checking a certain process does not include personal data processing. GDPR forced companies to take a look at their procedures, daily operations and decision-making processes, throw out what was "illegal" or irrelevant and simply have everything under control. *"Clean data will not only help you to target new customers more accurately, respond to SAR requests quicker, maintain ongoing readiness with regulations and build on the company's reputation for good practice with current and future customers, partners and investors"* (Jones, 2018).

One aspect of these technical and organisational measures is security of personal data. While definitely an obvious plus for data subject, it can prevent data breaches, which were always costly, even before GDPR. Security should be seen as a financial investment of any company: "*There is no company in the world that can afford to take the risk of cybersecurity ignorance, given the costs of data breaches and business downtime caused by theft or loss of critical data"* (Fimin, 2018).

Before continuing to the final part of our analysis, where we will look at known costs and benefits on a real company example, there are a few more beneficial aspects that we will consider. The benefits below may only not be true for all companies, but are worth mentioning regardless of their non-general nature.

2.3.3.2 GDPR as a service

In the panic and frustration before and after GDPR's Effective date, many companies looked outside for help in need for companies which could consult them or even execute GDPR related activities. Since GDPR created a new problem for companies, there was soon the recognition of that need, which was before long identified as a business opportunity by many. This trend was a school-case example of how a new external factor created a demand peak, and supply quickly followed. The magnitude of costs that we've identified before, gives as a feeling that this was a market that was worth a lot.
Just like the GDPR project task force was mixed with people from legal, IT, software development and C-level employees, companies from all these fields extended their portfolio that could now include GDPR. Reuters reports in January 2018: "*The cottage industry that's developed around GDPR includes lawyers who advise on compliance, cyber security consultants, and software developers that help firms conduct painstaking inventories of vast amounts of data to identify and index information so it can be made available to Europeans at*

their request" (Rodriguez, 2018).While it mentioned European companies in particular, the nature of GDPR makes it clear this is true for all companies affected by the Regulation. Oliver Smith also emphasizes the magnitude of the business by naming his 2018 Forbes article "*The GDPR Racket: Who's Making Money From This $9bn Business Shakedown"* (Smith, 2018). He includes quotes from firms providing such services - one example is Behnam Dayanim, a partner at international law firm Paul Hastings: *"The legal spend has ranged from as low as mid-five figures—$50,000 or $60,000 per project—to high six-figures and there have been projects we've scoped that have been beyond that"* (Smith, 2018).

Costs of many translated into a very direct benefit for some in the form of straight up revenue. And those who were successful in selling their services, could hand-pick their clients: "*People really aren't picking up the phone for less than $1.5 million to $2 million"* said Redmon, program director of cyber security and privacy at IBM Resilient, regarding legal and software consultancy firms advising on GDPR (Rodriguez, 2018). Companies were also spending on technological solutions that were now incorporated into internal system, probably with the intention to be used on an on-going basis. Again, those providers charged greatly for this technology.

There were even some companies who were founded on GDPR basis and dedicated only to that. There is not data available about how many companies are offering that, but searching with a keyword query "*gdpr service*" on Google offered me 267 million results on January 17th 2019.

2.3.3.3 Competitive advantage

No-one though more about benefits of GDPR compliance for companies than above mentioned companies that were selling GDPR compliance as a service. It can be observed from the way they communicate on websites, that they probably realised the fear of GDPR and the penalties for its non-compliance is not a good enough value proposition and there is more that can be "sold" to companies when it comes to GDPR relevance and its implementation strategy. Ernest Young, also offering GDPR services, has a document available explaining how they help you enable a strategy for compliance, implement it and maintain it and their title already reveals their selling point - it is called "*Developing your GDPR response for competitive advantage".* In the document, this is presented in the following way: "*As well as the urgency of working towards compliance there is also the opportunity to take a strategic approach to GDPR"* and *"By taking a strategic, risk-based approach to GDPR readiness, organisations can achieve both compliance and competitive advantage"* (Ernest & Young, 2017). Deloitte, one of EY's biggest competitor calls GDPR "*a blessing in disguise*" (Deloitte, 2017). Microsoft's Azure e-book series names their document "***Turning trust into competitive advantage****"* (Microsoft, 2018). PwC's blog post is titled ***"Creating a competitive advantage with GDPR"*** (Tiel, 2018). Looking from this content marketing material, it seems like all companies decided on a very similar communication strategy.

In some cases, companies support their claims on competitive advantage with market research finding. PwC, for example, mentions in their own study that "*The survey found that some companies see their GDPR programs as a potential differentiator in the market. Among companies who have finished their GDPR preparations, 38 percent have engaged their investor relations departments, a potential indicator that they hope to highlight early compliance to help drive a competitive advantage*" (PwC, 2018).

Viewing GDPR as a competitive advantage is often (further) defined in the context of all secondary benefits we have identified, repackaged and rephrased. While it is clear that being the first, only or both in the industry to claim GDPR compliance is beneficial, the amount of benefits such compliance brings varies from company to company. In the end, it matters how the company's customers view GDPR and privacy related matters. For many, they weren't so easy to impress and seemed more "annoyed" with opt-in emails than anything else.

Nevertheless, it is safe to assume privacy awareness will increase and gain importance among data subject as well in the following years. It is also possible, GDPR will go from a "competitive advantage" to simply being a new norm. But this does not depend (solely) on how GDPR as a regulation will be executed and enforced, but on the role of privacy in the global sphere.

Many benefits identified go beyond checking the regulatory boxes and only come to life once the companies embrace GDPR and start looking at it as an opportunity - even if something that you can use as an advantage over your non-compliant competitors. While this narrative might again be another effect of GDPR related marketing to make companies take it more seriously and comply with the regulation's requirements, it's good that we can start looking at regulation beyond its usual status from a company's view as a necessary evil that presents a big overhead.

In the final part of this chapter, we will summarize the effects of some company parameters on the costs, benefits or both, based on all that we have discovered during the cost benefit breakdown.

2.4 Main characteristics affecting costs and benefits

2.4.1 Organizational characteristic – company size

Due to cost structure we can see that it is in general easier to become GDPR compliant for smaller companies than it is for large companies. But the ideal in terms of company size and compliance is to start with the process while your company is being set-up. It's always much harder to change and organize the processes than to build them in a certain way from scratch. Companies who could start off with GDPR in mind can definitely benefit from that stand point. We will now take into account two groups of companies according to their size:

- small and medium sized companies (also known as "SMEs), which are companies that employ less than 250. This criterion has been defined by the European Union in Recommendation 2003/316 (The Commission of the European Communities, 2003);
- large enterprises or corporations, which employ more than 1000 people. In general, we will take into account the giant tech companies, which are Amazon, Facebook, Apple, Microsoft and Google. Even GDPR makes direct differentiation referring to the company size as the only factor. Specifically, there are a few obligations that are not required by SMEs. These differences are:

- **SMEs do not need to appoint a data protection officer by default.** They are only obligated to do it if their core activities require regular and systematic monitoring of the data subjects on a large scale, or if they process special categories of personal data such as that revealing racial or ethnic origin or religious beliefs. EC also states that: a DPO in this case "*will not need to be a full-time employee but could be an ad-hoc consultant, and therefore, would be much less costly"* (Jourová, 2016).

Appointing a DPO is, in fact, costly. Forbes reports that GDPR forces large companies to hire or appoint a 'data protection officer' (DPO), a role that commands a salary between £50,000 ($71,000) and £250,000 ($354,000) depending on the size of the company. (Smith, 2018). For comparison, a German company which specialises in being the DPO outsourcing partner, states on their website, a company can get their services from 500,00 euros per month, but the price comes only for companies with up to 25 employees (Deutche Gesellschaft fur Datenschutz, n.d.). This is a direct correlation of company size and GDPR related cost. However, we must keep in mind, DPO are also relevant for SMEs, so that cost can be applicable to them as well, they are just less likely to fall under the category of appointment obligation. The IAPP estimates around 75,000 DPOs will be required on a global scale (Heimes & Pfeifle, 2016).

- **SMEs need not keep records of processing activities** unless the processing they carry out is not occasional or likely to result in a risk for the rights and freedoms of data subject.

This obligation does not result in such cost reduction as with DPO, but nevertheless presents one less requirement.

- **SMEs will not be under an obligation to report all data breaches to individuals,** unless the breaches represent a high risk for their rights and freedoms.

Specific requirements are not the only things where SMEs shall some cost-related benefit – it is also in the more substantial recommendations for how application of the Regulation shall be treated in general. In Part (13) of the Preface, the Regulation defines a clear differentiation

according to company size: "*To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation"* (European Parliament and the Council, 2016). Such statements do not give SMEs any guarantee on how they would be treated, however it does represent an important guideline that size of a company is a parameter that should be taken into account when preparing national legislation (member states) or evaluating compliance (supervisory authorities). In some way, the Austrian case of the GDPR penalty supports this.

While we see, there are some costs we can correlate with company size by default, others are less straight forward. But it's no surprise that company size usually brings more complex processes and whenever something as wide-reaching as GDPR turns this giant structure upside down, this results in bigger financial consequences. *"The bigger an organisation is, the bigger a nightmare it is," says Julian Saunders, chief executive officer of Port, a U.K. startup selling software that helps clients control who gets access to data and creates audit trails to monitor privacy"* (Kahn, Bodoni & Nicola, 2018).

2.4.2 Business characteristic: SaaS businesses model

There are two reasons why the SaaS or "software as a service" business model has been chosen as one of the characteristics evaluated and compared to others:

- companies with a SaaS business model are very data driven, therefore GDPR affects most of their customers and departments;
- it was the rise of such companies and their digital products that was driven by technology that made previous regulations inefficient.

SaaS companies have more data processing by default due to the nature of their product and service, so we can also assume their implementation costs will be much higher. Their digital component makes their business operations more scalable, therefore such companies are mostly very data-centric. Every SaaS company needs a data protection officer by default, as offering a software usually means processing large amounts of identifiable data.

If we look at the phases of GDPR compliance, we can say that costs are higher for SaaS business in the following aspects:

- in many aspects, digital service and product provides had to spent more on the research and strategy part, as for many requirements it was not clear how to interpret them and apply

them for digital use cases. One such example is permanent deletion. While you can always shred documents, it is close to impossible to permanently delete data from backups;
- the implementation was costly as the technical and organizational requirements apply to almost every data, which due to the fact that its digital, is usually spread out across people and processes;
- the maintenance can be either very costly or completely automated (which IT companies are prone to in general), depending on the company strategy.

2.4.3 Company location: EU vs USA

US companies can be assumed to have higher costs, since their compliance gap was much larger than that of EU companies, which already had pretty high data privacy standards before GDPR. Forbes article explains this with the following words: "*This huge difference in cost compared to their European peers is because many of the requirements of GDPR already exist in EU law and companies have advanced systems in place to deal with them"* (Smith, 2018).

The increased territorial scope, however, represents a challenge to the European Union as well, when it comes to the Regulation's enforceability. While mostly a macro-economic issue, the enforcement realization can greatly affect the evaluation of compliance benefits for companies outside EU. How exactly will this enforcement work across the globe, is not yet clear: "*While we don't yet have U.S.- EU negotiated civil enforcement mechanisms for the GDPR (and it is unknown whether we ever will), there is still the application of international law and potential cooperation agreements between U.S. and EU law enforcement agencies, which have been increasing in recent years*" (Spikeworks, 2017).

It is true that one of the obligations of companies that are incorporated or operate outside EU, they need to have a legal representative in the Union and this is one way how the EU can enforce fines on such companies. The big questions, is, however, what if the company ignores the obligation or is unknowingly collection EU citizens data, making it impossible for EU authorities to operate under their jurisdiction. It seems like the only way to truly make it enforceable is with the help of local authorities, which as stated above has not yet been officially signed. In case of Google, the Ireland headquarter were the official representative of Google, so the penalty should be enforceable without complication, but we will have to observe how it unfolds.

One important affect and perhaps advantage of US companies is also the fact that they hypothetically do have the option to completely disregard GDPR. We should not forget that US companies are only bound by it, if they are processing personal data of people in the Union. While EU companies must comply by default, US companies can simply choose to no longer operate on the European market. And there were quite a few that did do that and it happened right before the GDPR's Effective date. On May 24th, one day before, the Guardian published

an article mentioning that companies made decisions to pull out of the European market - some claiming it was due to "business reasons", while others were more straightforward and providing GDPR as the reason for their decision (Hern & Waterson, 2018).

3 CASE-STUDY: IMPACT OF GDPR ON COMPANY X

The final aspect of looking at the effect of GDPR on companies, is to examine it not only from the perspectives of companies in general, but from analysing the impacts it had on one particular company. This will it bring new light on the research questions discussed, and put the previous analysis in practice, as we have been granted access to some internal business data revealing various aspects of the GDPR effects.

We will examine the impact the same way as before, hence focusing on all costs and benefits related to GDPR, only this time we will be able to compare the costs and benefits already occurred until a certain time point[8] and perform a cost-benefit analysis. All data presented in the thesis have been adjusted for the purpose of protection Company's confidential information.

A few basic characteristics of the Company on which we performed the case study on:

- The Company is EU based, however is very internationally oriented and performs a lot of business with the United States;
- The Company has 40 employees;
- The Company's main activity is software development as a service, however has a SaaS[9] product in their product portfolio as well.

3.2 GDPR related costs for Company X

3.2.1 Cost identification

The Company had no *direct financial costs*, which comes as no surprise considering there are almost no obligations related to activities connected with government or some other state authority in the implementation procedure. The only obligations companies potentially do have towards their member state in the process of implementing GDPR is to officially name a Data protection officer (if needed), but there is no fee related to that. As GDPR does predict, however in articles 40 and 42 of GDPR that Member States and their respective bodies may produce *codes of conduct* which will have the purpose of specifying the application of the Regulation in practice, which will give them to option to also officially certify for it.

[8] Data available until April 1st.

Administrative costs are also not observed at this point – while there were tasks performed, which were related to demonstration of compliance, this is in GDPR's case closely connected to each requirement as companies have a GDPR requirement to ensure demonstration of compliance by default. Additionally, no such task was done *solely* for demonstration purposes and are therefore counted as direct labour costs.

The only category that we witness and can analyse in case of Company X are therefore all substantive compliance costs. The Company confirmed they had no costs related to any external consultancy (which would fall under *external services cost*), meaning all their compliance related tasks were done in house. The main majority of these substantive costs were either *direct labour costs* and *overhead costs*. One of the main reasons for that is also a startegic decision of the Company to try and perform as much work and gain as much knowledge as possible in-house, as this is an investment in the long run. This is due to their belief that core business knowledge should always be present internally and they see data protetion as one of their core competences.

For identifying the actual costs that occurred, we will calculate the cumulative hours spent by all employees working on all GDPR related tasks. Based on different monetary value a unit of hourly work has for the Company, we will also divide the spent hours into two groups, based on different monetary value of human resources in case of Company X.

3.2.2 Cost measuring

The difference in company costs are related to two groups of employees, regardless of the work they are performing:

- Cost per employee hour for members of the development team (hereinafter: developers);
- Cost per employee hours for all other company employees (mostly coming from sales, marketing, support and legal departments, hereinafter: non-developers).

According to Company data, the total hours spent on GDPR equals to **686 hours,** out of which **196 hours** have been performed by developers and **490 hours** have been performed by non-developers.

The way we will calculate the costs is based on the calculations Company uses for their internal purposes of performing cost-benefit analysis and financial reports. The internal cost of one development hour is valued at **65 EUR**. This means that company cost related to development can be calculated in the following way:

$$\begin{aligned} &\textit{TOTAL DEVELOPMENT COST} = \textit{development hours} \times \textit{development hourly rate} \\ &= 196\ \textit{hours} \times 65\ \textit{EUR} = 12.583\ \textit{EUR} \end{aligned} \quad (1)$$

For non-development hours, the costs are not calculated per hours directly, but according to full time employee (hereinafter: FTE) units. Each company can define FTE unit differently, but in general it correlates to a number of *effective* hours per month. The IRS, for example, defines it as follows: "*For purposes of the employer shared responsibility provisions, a full-time employee is, for a calendar month, an employee employed on average at least 30 hours of service per week, or 130 hours of service per month"* (IRS, 2018).

Company takes a more conservative approximation, which is 115 hours. This means that if for project 1 person A is working for 115 hours, this is calculated as 1 FTE. The absolute cost taken into account for such work would not equal to cost of 115 hours, but to the cost of 1 month's work (standard is 140 hours). It is important to note that the cost for 1 FTE does *not* equal to monthly salaries, as it is supposed to cover all costs related to one employee, therefore also includes various costs we will referred to as *overhead*, such as: recruiting expenses, taxes, benefits, space and other equipment (Hadzima, n.d.). The company uses the calculation of **5000 EUR/FTE** for all non-developers**.** The calculated sum for all non-development GDPR-related hours is **490 hours**, which equals to 4,3 in FTE units. From this we can therefore calculate the cost for all non-development hours:

$$\textit{TOTAL NON-DEVELOPMENT COST = FTE units x Non-development cost per FTE = 4,3 x 5.000 EUR = 21.286 EUR} \quad (2)$$

Combining the two we can calculate all GDPR related labour costs for Company X:

$$\textit{TOTAL LABOUR COST = Developers cost + Non-developers cost = 12.583 EUR + 21.286 EUR = 34.341 EUR} \quad (3)$$

According to Company X, another cost was external education for designated employee(s), which had a cost of **472 EUR,** which was attended by an in-house legal employee.

3.2.3 Opportunity cost

Company X is a software development service company, so the hours spent by developers on GDPR could have otherwise been spent on billable hours performed for Company's clients. In reality, it is too optimistic to think all hours could have been spent for external project work, so we will take 70% of total development hours based on Company's assessment related to the comparison of billable vs non-billable hours in other projects.

For calculating opportunity costs, we therefore use the following formula:

$$\textit{OPPORTUNITY COST = (TOTAL DEVELOPMENT HOURS x 0.7) x HOURLY MARGIN= (194 x 0,7) x 24 EUR = 3.252 EUR} \quad (4)$$

3.253 EUR is therefore the expected revenue for Company X that Company X lost due to GDPR related work. We have not accounted for the work of non-developer, since their hours would have to be spent on selling the software development performed by developers and therefore, we cannot account for any additional benefit that is not already included in the software development profit margin.

3.2.4 Total costs calculation

We can now calculate the total cost of GDPR for Company X:

$$TOTAL\ GDPR\ COST = TOTAL\ LABOUR\ COSTS + TOTAL\ OTHER\ COSTS + OPPORTUNITY\ COST = 12.583 + 21.286 + 472 + 3.252\ EUR = 37.593\ EUR \quad (5)$$

The negative impact of GDPR on Company X, which directly translates to costs results to 37.593 EUR.

Table 1: GDPR costs for Company X

Type of cost	**Cost in EUR**
Development costs	12.583
Non-development costs	21.286
Other costs	472
Opportunity costs	3.253
Total costs	**37.593**

Source: Own work.

3.2.5 Qualitative cost analysis

Based on the data and they way the hours have been recorded, there a few other important insights we can notice:

- Out of 686 hours, 93,5 out of those hours have been spent on meetings (14 %) – this is one indicator that quite some time has been spent of strategy and research, since usually tasks are done individually, while most strategic decision and maintenance decisions are done involving multiple people.
- Out of 686 hours, 189 hours have been spent by development (28 %) – this shows that in IT-related companies the costs are much higher in general, as not only do we need a more interdisciplinary approach, but also many activities are related to IT matters, which can only be performed when company is digitally oriented. Since no other departments usually have the knowledge to perform such activities, the costs increase dramatically. Also, development opportunity costs play an important role in the total GDPR related costs.

- Out of 686 hours, 441 have been spent in relation to one SaaS product (64 %) – this shows a drastic role of SaaS related products in the cost scheme for a Company.
- Out of 686 hours: 22,5 have been spent in 2019; 62,5 have been spent in 2017 and the majority 597 hours have been spent in 2018 (3 % vs 9 % vs 88%).

This shows the company has started with activities quite early and that even though their "implementation" phase is complete, there are still activities going on to maintain compliance. *"There is a lot of on-going cost - our company is very agile and need to have an additional layer of quality assurance for every new project, process or activity is quite costly"* (Company representative A, 2019).

3.3 GDPR related benefits for Company X

The benefits of compliance for Company X are much less direct and therefore harder to properly identify, especially due to uncertainty and speculation already mentioned before. Despite all of that, there are benefits that can be identified and we will use the data available to try and measure the benefits in monetary terms. This will enable us to financially compare costs and benefits on an example of Company X.

3.3.1 Avoiding penalties

Company X has not been fined with any penalty related to GDPR, but we cannot equal this fact with the prescribed penalty to get a realistic evaluation. What we can do is help ourselves with available data and for that we can take two important numbers issued by The European Data Protection Board in January 2015:

- **Number of GDPR – related complaints** reported to any Supervisory Authority (or Data protection Authority as referred to by the EDPB, which is **95.180**.
- **Number of fines issued by Supervisory authorities** – although this source reports only three (without Portuguese case[10]), we will account for all **4 cases** (German, Austrian, French and Portuguese) (European Data Protection Board, 2019).

The third data that we need for the evaluation is the prescribed penalty, but as we've seen it depends on multiple factors and it's impossible to know in advance how much could we expect to be fined with as this changes every second due to the exact state of both the company and their compliance level. Due to Google's enormous fine, calculating an average penalty is not

[10] We assume this is due to the fact that Portugal still does not have their Member state legislation and hence not an official SA, so in the report they only accounted for penalties issued by official Supervisory Authorities, although the Portuguese body *de facto* is one.

helpful, as it accounts for 12.606.200,00 and is in no way representative due to the sample size. We will take the maximum relative fine prescribed, which is to 4% of the total worldwide annual turnover, as this is the only number relative to company size and therefore the best approximation available at the moment. We will calculate the current estimated penalty amount based on the predicted penalty for Company X multiplied by the probability of a fine turning into a penalty.[11]

Table 2: GDPR penalty avoidance (primary benefit) for Company X

Predicted penalty	**Amount in EUR**
Yearly turnover	2.000.000
Predicted penalty	80.000
Penalty probability	
Number of complaints	95.180
Number of fines issued	4
Penalty probability	0,000042
Total primary benefit (estimated penalty value)	**3,36**

Source: Own work.

We get to an almost absurd number of the benefit estimation that comes from avoiding penalties, evaluated at **3,36 EUR**. Regardless of the fact that we have made a lot of simplification and approximation in our calculations, it still shows the enormous gap between costs the estimated benefits compliance brings to outweigh those costs. We will now also try to quantify secondary benefits that have been identified by the company.

3.3.2 Secondary benefits

Apart from avoiding penalties, there are other benefits that have been recognized by the Company. As an Information Technology (hereinafter: IT) company, cybersecurity, defined as *"protection against digital attacks"* (Poggi, 2018) is related to one of company's biggest risks. Handling data is what was identified by the Company as their core business. GDPR has very strict standards (although loosely defined) of data security and implementing that to all data, not just personal can bring long term benefits.

For calculation of cybersecurity benefit, we will again take some publicly available data that will help us but those qualitative benefits into a monetary value estimation.

[11] As fines have a lag and we cannot predict how many will be solved from the total number, we will compensate this by taking the actual complaints instead of total number of companies (for which GDPR is applicable) to calculate the probability.

According to a Ponemon Institute study revealed that "*the total cost of a successful cyber attack is over $5 million, or $301 per employee"* (Poggi, 2018). For more accurate calculations, we will therefore take this estimated per employee cost estimation in EUR[12] and multiply it with the current number of employees of Company X, since the cost of a successful cyber security attack is the basis for benefit of GDPR compliance aimed to strengthen the risk.

SUCCESSFUL CYBER ATTACK COSTS = GENERAL CYBER ATTACK COST per employee x NUMBER OF EMPLOYEES = 270 EUR x 40 = 10. 800 EUR (6)

Now we must calculate the actual benefit of security implementation based on Company's estimate of how much less likely is the Company to endure these costs (meaning be a victim of a cyber attack) due to GDPR implementation in the next year. The Company estimated it at 50 %.

The actual benefit is therefore the cost estimated to occur in case of cyber attack, multiplied by the probability of the event:

CYBER ATTACK ESTIMATED COST = CYBER ATTACK COST of Company X x PROBABILITY = 10.800 x 0,5 = 5.400 EUR (7)

This is the yearly cost estimated to be avoided due to better cyber security implemented because of GDPR. Another benefit that has been detected is better sales conversion of their SaaS product, due to GDPR compliance, especially in the form of implemented security measures like encryption. The Company estimated security measures (e.g. encryption of data at rest) and GDPR in general have contributed to around 10 % of sales. However, while technical security measures have always been important, the relevance of GDPR compliance in general has been observed with a bit of lag: *"It was very evident that GDPR for companies looking for GDPR compliant data processors is becoming more and more important, but it was not until September that we noticed this new trend"* (Company representative B, 2019).

We will therefore take 10 % of sales from September to date to understand the revenue that has a direct correlation with GDPR and therefore presents a benefit:

GDPR-RELATED REVENUE = REVENUE FROM SALES x PERCENTAGE OF DEALS CLOSED DUE TO GDPR = 370.175 EUR x 0,1 = 37.017 EUR (8)

The Company therefore estimates that GDPR compliance contributed to **37.017 EUR** of revenue.

[12] The conversion was done using Google converter on May 2nd, 2019.

There are also other benefits that are being noticed, however it is too soon at this point to evaluate them in estimated revenue form. These benefits for example include the minimum amount of complaints by the data subject due to transparent privacy policies, more efficient organizational measures and a huge increase in data protection awareness within the Company (Company representative A, 2019).

We now have an estimation on all the measurable benefits to-date for Company X:

Table 3: GDPR benefits for Company X

Type of benefit	**Cost in EUR**
Avoiding penalties	3
Cybersecurity	5.400
Sales	37.017
Total benefits	**42.420**

Source: Own work.

Now we can compare the costs and benefits that Company X has been identified and are (at least approximately) measurable until now. The basic logic behind the cost-benefit analysis is that the benefits must outweigh the benefits for the project (in this case pursuing GDPR compliance) to make sense from a financial and managerial standpoint. The time value of money is an important aspect of any cost-benefit analysis, as we need to compare them in the same terms, which is the value of cash today. As we are doing the cost-benefit analysis for past data, these are all values that have been estimated at this point in time.

If we subtract the costs from benefits and get a positive number, that means that all the effort put by Company X into GDPR has paid off financially.

$$TOTAL\ GDPR\ BENEFITS - TOTAL\ GDPR\ COSTS = 42.420 - 37.593 = \mathbf{4.827} \quad (9)$$

Based on available data and calculation we've made (although with several limitations and estimations), we have come to the conclusion that benefits identified and quantified for now have been greater than costs for 4.827. If we estimated this in advance, we would have discounted the benefits and the result would be somewhere around a positive 0. Both costs and benefits are expected to grow in time and it will be important for Company to continuously analyse the costs and benefits as they unveil. They are expected not only grow for maintaining compliance, but with company growth in terms of size and operations. We can also expect for quantification of impacts to become easier as time passes, as things connected GDPR will become clearer and more predictable – at least this is a trend that we can observe now.

The case-study of Company's X GDPR compliance project should not be taken as a representative case, from which we could conclude that in general, GDPR financially pays off for companies in general. Insights from the general research on potential costs and benefits show us this very clearly, as variety and relativity of GDPR and its impact on each individual company is enormous and depends on an indefinite number of factors.

It is not hard to imagine many cases where the same cost-benefit analysis would have shown much different results. In Company X, most benefits actually came from sales revenue for a product, where the customers needed GDPR compliant solutions for their compliance as well. Companies without such product/service (where they are acting as a data processor) would have to rely on some other benefits to make up for the minimal percentage of benefits coming from avoiding fines. It also makes the most sense for companies to spend costs on measures and requirements that bring the most benefit to their business. This is why it is important to conclude our research analysis with potential cases, where costs are bigger than benefits and GDPR compliance does not represent a financially rational investment.

4 GDPR COMPLIANCE AS AN ETHICAL DECISION

While perhaps compliance often seems like a necessary burden that companies will go pursue regardless of its cost, we need to be careful to assume that companies will base their decision on ethics and morality instead of finance. If a company invests time and perform a very detailed, *ex ante* cost-benefit analysis for a regulation implementation and realizes that in all probability costs will outweigh the benefits by far, what can we expect such a company to do? And additionally, what do we believe would be the right thing for a company to do?

Profit maximization is still the underlining concept on which corporate finance theory is based, yet in practice we have come to a point (especially as consumers) where we often not only expect, but demand from companies to neglect this rationale and include social benefits into their decision making. Sometimes such pressure comes from legislation, while other times from social activism, as for example with the rise of environmentalism. In the European Union, it is often both at the same time (European Commission, 2019). Social impact is extremely important for overall benefits of our planet and should be included in corporate strategies in order for a sustainable future where individuals and corporations can co-exist. However, we cannot let this depend on personal morals and values of executives, especially when such ethical decisions presume "irrational" financial management and decision-making.

Policy makers need to understand that instead of making regulation without regards to the company impact financial aspect of legislation, especially once all those compliance costs from all fields add up. This will also help governments better predict company reactions to such regulation.

In the end, we must understand it will always be the end user who pays the price of compliance – if they don't, company will soon cease too exist. This is why it must bring as much benefits to the company as possible, while still reaching its high-level goals. But not just any benefits – as we have seen, any compliance could become financially viable if we increased either the penalty amounts or the probability of being penalized for long enough. But primary compliance benefits (e.g. avoiding penalties) are not benefits that actually add value, while secondary benefits (mostly) do. Focusing on regulation that included secondary benefits, would bring many more positive impacts for companies and we could expect them to follow requirements more, so enforcement could become less important, saving governments substantial amounts. However, if this was always the case, we would not need regulation at all, as companies would implement all those things that regulations require from them by default. The exact purpose of regulation is too "force" companies into bearing costs they would not have otherwise and enforcing them through penalties to achieve goals governments deem important. This is what we have accepted as a democratic society for greater good. But there needs to be a balance, especially if we want to positively influence the economic growth.

Investigating GDPR from all these different angles does shows some steps in this direction. Primary benefits are extremely low compared to costs, but this is only true due to current enforcement trends. At the same time, penalty amounts are exactly the reason GDPR has gotten so much attention worldwide and before the fine probability (as it is now) could have been recognized, the general awareness was already of the roof. The fact that there is so many loose articles in its text, especially in part which potentially opened the doors for many secondary benefits, although problematic at first, perhaps gave companies the option to find their own way of doing it in a way that made sense and was beneficial for them. If authorities will continue to penalize companies in the way that they did in these 4 cases, perhaps secondary benefits will take the leading role in GDPR strategy, which will bring benefits for data subject as well.

In the long run, it is important for all stakeholders to work together and come up with policies that create a win-win-situation: for governments, companies and individuals. For that, consensus is needed not only on high level goals (like protection of personal data), but on strategy, activity and enforcement level as well.

Last but not least, we must not undermine the role of individuals in this story. The Google case shows that governments will also put as much pressure on companies as individuals will deem necessary – which makes sense, especially when high level goals are directly related to benefits of individuals (CNIL, 2019).

GDPR is a great example of a regulation which aim to protect individuals and therefore it is only right for company's actions be evaluated in the light of their relationship towards data subjects. GDPR leaves a lot of room for interpretation, but for now it seems like this type of relativity will be the main guidance of its enforcement and we should welcome that.

If the main goal of the Regulation was personal data protection through very strong awareness, it managed to do it successfully. Perhaps through awareness of employees, data subjects to which employees turn to after 5 will also become more aware not only of possible threats to their privacy, but to the power the EU has given to them.

The way GDPR has been "launched" is either a lucky coincidence or one hell of a marketing strategy from the European Union. What we witnessed was a series of events that organically (or so it seems) turned into a massive awareness campaign of GDPR. It started with PR campaigns that consisted of headlines about penalty amounts, which grabbed companies' attention, while increased territorial scope made sure it was globally relevant. Companies started looking for answers on many ambiguous requirements GDPR set out for them, which created interest on the market. Without clear answers, this search turned into a mini panic of companies looking for any possible help with the subject. This created massive demand (especially due to GDPR's wide applicability), which was soon filled by companies promoting their service with content marketing, making GDPR appear everywhere.

Regardless of how closely companies will follow GDPR's requirements and how strict the enforcement will be, GDPR has forever changed global awareness and understanding of personal data and privacy. Even if companies choose to resist and ignore it as long as possible, perhaps they will now at least feel more guilty doing it.

CONCLUSION

GDPR regulates a very important field, as privacy is considered one of our basic human rights. Due to the speed of technological innovation and the 4IR, companies are coming up with endless options to monetize personal information and too often, privacy is being compromised as a result. GDPR managed to gain more attention than any other legislation in the past century, as data privacy is being one of the most controversial and talked about topics around the globe. Apart from its several macroeconomic effects, it severely impacted companies, which were the main subject to which GDPR was applicable through obligations it set out for them.

Firstly, GDPR has affected companies by some of its legal characteristics. Some of those were of formal nature, like the fact that it is a regulation and therefore entirely and immediately binding. Other characteristics were material and therefore connected to the content - the most important ones that we have identified were high penalty amounts, increased territorial scope and unclear requirement to achieve compliance that has not been properly filled by Member state legislation. This was just one group of elements that help us understand the impact GDPR had on companies, while others came from understanding how companies reacted to what was expected of them and try to understand why. The full impact could only be analysed if we looked at both sides – the positive and the negative, which for companies directly translate into costs and benefits. The costs that occurred were mostly substantive costs according to the

Standard Cost Model framework, in particular direct labour costs and overhead costs, while also long-term structural costs are predicted.

In general, the magnitude of costs and their exact nature depends on many different elements, such as company's own GDPR interpretation, company strategy and processing practices. We also saw that costs are expected to grow with company size and are normally bigger for US companies (compared to EU) due to bigger compliance gap and SaaS business, due to the default nature of digital data processing. Current cost assessments from companies show extremely high figures of resources put towards GDPR compliance, with estimations that Fortune's Global 500 companies will cumulatively spend about 7,8 billion USD to comply with GDPR.

Benefits come primarily from penalty avoidance, which is extremely high for GDPR (up to 20 million EUR), however GDPR only prescribes maximum penalties, therefore a lot of uncertainty remains for companies in to what fines can they expect for which level of non-compliance. The GDPR related fines have been issued 4 times until now, with 4 different Member states, 4 different breaches and 4 very different penalty amounts, ranging from 4800 EUR to 50 million EUR. Each case revealed a bit more about what is expected from companies and how authorities will be enforcing GDPR. For now, it seems like a holistic approach that we took in our research to understand GDPR's impact is being undertaken by Supervisory authorities as well, since every element can count in determining the final penalty amount. There are also many secondary benefits that can be identified, for example better business processes, raised level of security, competitive advantage, healthier competition etc., but again their applicability and magnitude is specific to each company individually. Additionally, due to such a high demand for GDPR related services, the costs of many companies resulted in revenue for others.

The practical part of our research showed that costs were slightly lower than benefits, however the benefits mostly came from secondary benefits, as the penalty avoidance is extremely low based on current penalty statistics. This shows that in order for GDPR compliance to make financial sense on current available data, companies had to find substantial benefits in improving their business practices to justify the costs.
Regardless of the cost-benefit analysis, GDPR managed to raise awareness to a level where it seems like most companies simply pursued compliance out of fear and ethical responsibility, rather than positive financial outcome.

LIST OF REFERENCES

1. Abela, R. (2018, April 12). *Netsparker Surveys US Based C-Levels on GDPR Compliance.* Retrieved August 27, 2018 from: https://www.netsparker.com/blog/web-security/gdpr-compliance-2018-survey-results/#WhoAnswered
2. Ambler, T., Chittenden, F. & Bashir, A. (2019). *Counting the Cost of EU Regulation to Business. European Economic and Social Committee.* Retrieved April 24, 2019 from https://www.eesc.europa.eu/resources/docs/costregulation_2009_bis-2009-00286-01.pdf
3. Armerding, T. (2018, December 20). *The 18 biggest data breaches of the 21st century*. *CSO Online.* Retrieved February 13, 2019 from: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
4. Article 29 Data Protection Working Party. (2017, October 3). *Guidelines on the application and setting of administrative fines for the.* Retrieved November 28, 2018 from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237
5. Asia-Pacific Economic Cooperation; Ministry of Justice. (n.d.). *Compliance Cost Measurement Framework.* Retrieved August 15, 2018 from: https://www.nesdb.go.th/download/RIA/ComplianceCostEN.pdf
6. Baker McKenzie. (2018, May). *GDPR National Legislation Survey.* Retrieved December 19, 2018 from: https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey_updated_june2018.pdf?la=en
7. Barnard, C., & Peers, S. (2014). *European Union Law.* Oxford: Oxford University Press.
8. Bender, D. (2018, June 7). *GDPR harmonization: Reality or myth?* Retrieved February 17, 2019 from IAPP: https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/
9. Bragg, S. (2018, February 13). *The difference between cost and expense*. Retrieved February 5, 2019 from: https://www.accountingtools.com/articles/what-is-the-difference-between-cost-and-expense.html
10. Business dictionary. (2019a). *Sunk cost.* Retrieved January 16, 2019 from: http://www.businessdictionary.com/definition/sunk-cost.html
11. Business dictionary. (2019b). *Gap analysis*. Retrieved February 27, 2019 from: http://www.businessdictionary.com/definition/gap-analysis.html
12. Campbell, H. F. & Brown, R. P. (2016). *Cost - benefit analysis - Financial and economic appraisal using spredsheets.* Abingdon: Routledge.
13. Carter, B., Flores, J. & Johnson, M. (2018, August 15). *Microsoft 365 GDPR action plan*. Retrieved December 14, 2018 from: https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-action-plan
14. Chee, F. Y. (2018, November 27). *European consumer groups want regulators to act against Google tracking*. Retrieved January 12, 2019 from:

https://www.reuters.com/article/us-eu-google-privacy/european-consumer-groups-want-regulators-to-act-against-google-tracking-idUSKCN1NW0BS

15. CNIL. (2019, January 21). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.* Retrieved April 26, 2019 from: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
16. Coletti, P. (2013). *Evidence for Public Policy Design: How to Learn from Best Practice.* London: Palgrave Macmillian.
17. CW Jobs. (2019). *What is the average salary for Data Protection jobs?* Retrieved April 30, 2019 from https://www.cwjobs.co.uk/salary-checker/average-data-protection-salary
18. Davis, N. (2016, January 19). *World Economic Forum*. Retrieved February 2, 2018 from: https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/
19. Deloitte. (2017, May 11). *Gearing up for GDPR.* Retrieved January 17, 2019 from: https://www2.deloitte.com/it/it/pages/risk/articles/gx-gearing-up-for-gdpr.html
20. Deutche Gesellschaft fur Datenschutz. (n.d.). *Costs for our Services as External Data Protection Officers*. Retrieved February 3, 2019 from: https://dg-datenschutz.de/services/external-data-protection-officer/costs-for-our-services-as-external-data-protection-officers/?lang=en
21. Ernest & Young. (2017). *EU General Data Protection Regulation.* Retrieved January 19, 2019 from: https://www.ey.com/gl/en/industries/financial-services/fso-insights-eu-general-data-protection-regulation
22. European Commission. (2012, January 15). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. Retrieved August 24, 2018 from: http://europa.eu/rapid/press-release_IP-12-46_en.htm
23. European Commission. (2018a, January 24). *Questions and Answers – General Data Protection Regulation*. Retrieved August 25, 2018 from: http://europa.eu/rapid/press-release_MEMO-18-387_en.htm
24. European Commission. (2018b). *What is personal data?* Retrieved December 14, 2018 from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en#examples-of-data-not-considered-personal-data
25. European Commission. (2018c). *The GDPR: new opportunities.* Retrieved December 16, 2018 from: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf
26. European Commission. (2018d). *Types of EU law*. Retrieved February 13, 2019 from: https://ec.europa.eu/info/law/law-making-process/types-eu-law_en
27. European Commission. (2018e). *Applying EU law*. Retrieved February 17, 2019 from: https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en
28. European Commission. (2018f). *EU law*. Retrieved February 17, 2019 from European justice: https://e-justice.europa.eu/content_eu_law-3-en.do

29. European Commission. (2019). *Corporate Social Responsibility & Responsible Business Conduct*. Retrieved June 6th, 2019 from: https://ec.europa.eu/growth/industry/corporate-social-responsibility_en
30. European Data Protection Board. (2018, November 16). *Guidelines 3/2018 on the territorial scope of the GDPR.* Retrieved January 27, 2019 from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf
31. European Data Protection Board. (2019, January 25). *GDPR in Numbers.* Retrieved April 26, 2019 from: https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf
32. European Data Protection Supervisor. (2016). *The History of the General Data Protection Regulation*. Retrieved December 17, 2018 from: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
33. European Parliament and the Council. (2016, April 27). *Regulation EU 2016/679 of the European parliament and of the council*. Retrieved June 12, 2018 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
34. European Union. (2019). *Regulations, Directives and other acts*. From European Union: https://europa.eu/european-union/eu-law/legal-acts_en
35. Feiler, L. (2018, December 19). *Takeaways from the First GDPR Fines*. Retrieved February 17, 2019 from: https://www.bakermckenzie.com/en/insight/publications/2018/12/takeaways-from-the-first-gdpr-fines
36. Fimin, M. (2018, March 29). *Five Benefits GDPR Compliance Will Bring To Your Business*. Retrieved January 7, 2019 from: https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#624f92a8482f
37. Forbes Technology Council. (2018, August 15). *15 Unexpected Consequences Of GDPR.* Retrieved January 15, 2019 from: https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#51947eb594ad
38. GDPR Beyond. (2017, September 5). *Who should manage your GDPR project?* Retrieved January 15, 2019 from: https://www.gdprandbeyond.com/blog-post/information-governance/manage-gdpr-project/
39. Google. (2019). *Google Ads Help*. From Google Support: https://support.google.com/google-ads/answer/9004451?hl=en
40. Granville, K. (2018, March 19). *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*. Retrieved February 13, 2019 from: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
41. Grimsey, S. (2019). *Economic Cost: Definition & Function*. Retrieved February 26, 2019 from: https://study.com/academy/lesson/economic-cost-definition-function-quiz.html

42. Hadzima, J. (n.d.). *How Much Does An Employee Cost?* Retrieved April 13, 2019 from: https://web.mit.edu/e-club/hadzima/how-much-does-an-employee-cost.html
43. Hawks, D. (2019). *Accounting vs. Economic Costs: Examples & Comparison*. Retrieved February 3, 2019 from: https://study.com/academy/lesson/accounting-vs-economic-costs-examples-comparison.html
44. Heimes, R. & Pfeifle, S. (2016, November 9). *Study: GDPR's global reach to require at least 75,000 DPOs worldwide*. Retrieved February 26, 2019 from: https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/
45. Hern, A., & Waterson, J. (2018, May 24). *Sites block users, shut down activities and flood inboxes as GDPR rules loom.* Retrieved August 17, 2018 from: https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect
46. Hewett, P. (2017, July 25). *How should non-EU businesses prepare for the GDPR?* Retrieved January 27, 2019 from: https://econsultancy.com/how-should-non-eu-businesses-prepare-for-the-gdpr/
47. Info Security Europe. (2019). *GDPR Best Practices - Implementation Guide.* Retrieved January 11, 2019 from: https://www.infosecurityeurope.com/__novadocuments/355669?v=6362897865747000
48. Information Commissioner. (2019a). *Frequently asked questions*. Retrieved January 5, 2019 from: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/najpogostejsa-vprasanja-in-odgovori/
49. Information Commissioner. (2019). *Information Commissioner*. Retrieved February 3, 2019 from: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/aktualne-novice/
50. IRS. (2018, July 2). *Identifying Full-time Employees*. Retrieved April 13, 2019 from: https://www.irs.gov/affordable-care-act/employers/identifying-full-time-employees
51. Irwin, L. (2018, May 21). *The GDPR: How the right to be forgotten affects backups*. Retrieved March 22 2019 from: https://www.itgovernance.eu/blog/en/the-gdpr-how-the-right-to-be-forgotten-affects-backups
52. Jones, J. (2018, April 5). *Four benefits of GDPR for your organization*. Retrieved January 7, 2019 from: http://www.globaltrademag.com/global-trade-daily/four-benefits-of-gdpr-for-your-organization/
53. Jourová, V. (2016, January). *European Commission.* Retrieved February 4, 2019 from: ec.europa.eu/newsroom/just/document.cfm?doc_id=41524
54. Kahn, J., Bodoni, S. & Nicola, S. (2018, March 22). *It'll Cost Billions for Companies to Comply With Europe's New Data Law*. Retrieved January 27, 2019 from: https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law
55. Kasprzyk, A. (2016). *Vacation legis institution - sense and meaning.* Retrieved February 2, 2019 from: http://www.pan-ol.lublin.pl/wydawnictwa/TPraw9/6_Kasprzyk.pdf

56. Kenton, W. (2018, April 18). *Compliance Cost*. Retrieved March 1, 2019 from Investopedia: https://www.investopedia.com/terms/c/compliance-cost.asp
57. Khan, S. (2014, June 15). *Economic profit vs accounting profit*. Retrieved January 28, 2019 from: https://www.khanacademy.org/economics-finance-domain/ap-microeconomics/production-cost-and-the-perfect-competition-model-temporary/types-of-profit/v/economic-profit-vs-accounting-profit
58. Klekovic, I. (2017, October 30). *EU GDPR vs. European data protection directive*. Retrieved November 18, 2018 from: https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/
59. KPMG, AIMA & MFA. (2013). *The Cost of Compliance.* Retrieved August 17, 2018 from: https://home.kpmg/content/dam/kpmg/pdf/2014/07/Cost-of-Compliance.pdf
60. Lindsey, N. (2017, December 1). *Global 500 Faces GDPR Compliance Costs of $7.8 Billion. CPO magazine*. Retrieved May 12, 2019 from: https://www.cpomagazine.com/data-protection/global-500-faces-gdpr-compliance-costs-of-7-8-billion/
61. Locke, A. & Barnes, C. (2018, February 2). *Understanding the Cost of Compliance: A Framework.* Retrieved August 15, 2018 from: http://viewpoints.io/entry/understanding-the-cost-of-compliance-a-framework
62. Lynch, S. N. & Volz, D. (2018, April 24). *U.S. regulator fines Altaba $35 million over 2014 Yahoo email hack.* Retrieved November 24, 2018 from: https://www.reuters.com/article/us-altaba-cyber-yahoo/u-s-regulator-fines-altaba-35-million-over-2014-yahoo-email-hack-idUSKBN1HV295
63. Macaskill, E., & Dance, G. (2013, November 1). *NSA Files: Decoded*. Retrieved May 29, 2019 from: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
64. Mack, S. (2018). *Concept of Consumer-Switching Behavior*. Retrieved December 13, 2018 from: https://smallbusiness.chron.com/concept-consumerswitching-behavior-65092.html
65. Magee, K. (2018, November 5). *Cambridge Analytica whistleblower Christopher Wylie: It's time to save creativity*. Retrieved February 13, 2019 from: https://www.campaignlive.co.uk/article/cambridge-analytica-whistleblower-christopher-wylie-its-time-save-creativity/1497702
66. Marr, B. (2018, August 13). *The 4th Industrial Revolution Is Here - Are You Ready?* Retrieved Dcember 13, 2018 from: https://www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/#89f9c9b628b2
67. Merriam - Webster. (n.d.). *Source of law*. Retrieved February 12, 2019 from: https://www.merriam-webster.com/legal/source%20of%20law

68. Microsoft. (2018). *Turning trust into a competitive advantage*. Retrieved January 17, 2019 from: https://azure.microsoft.com/mediahandler/files/resourcefiles/turning-trust-into-a-competitive-advantage/Turning-trust-into-a-competitive-advantage-GDPR.pdf
69. Monteiro, A. M. (2019, January 3). *First GDPR fine in Portugal issued against hospital for three violations*. Retrieved January 7, 2019 from: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/
70. Moreno, K. (2014, August 12). *Regulatory Environment Has More Impact on Business Than the Economy, Say U.S. CEOs.* Retrieved March 1, 2019 from: https://www.forbes.com/sites/forbesinsights/2014/08/12/regulatory-environment-has-more-impact-on-business-than-the-economy-say-u-s-ceos/#43328040684d
71. Morgan, J. (2014, May 13). *A Simple Explanation Of 'The Internet Of Things'*. Retrieved January 23, 2019 from: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#611bd54e1d09
72. Netapp. (2018, April 11). *6 Weeks to Go: GDPR Concern Still High as Deadline Approaches*. Retrieved August 13, 2018 from: https://www.netapp.co.uk/company/news/press-releases/news-rel-20180411-277386.aspx
73. ECJ, 5 February 1963, Case 26/62 NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration
74. O'Donoghue, A. (2018, November 7). *Driving revenue in the API economy*. Retrieved April 3, 2019 from: https://www.youtube.com/watch?v=3qEbp3zsCdU
75. OECD. (2014). *OECD Regulatory Compliance cost assessment guide.* Retrieved January 28, 2019 from: https://www.normenkontrollrat.bund.de/resource/blob/244032/444040/bb5c3d481212a08f42ccd07e0edc471e/oecd-regulatory-compliance-cost-guidance-data.pdf
76. Poggi, N. (2018, August 30). *24 Cybersecurity Statistics That Matter In 2019*. Retrieved May 2, 2019 from: https://preyproject.com/blog/en/24-cybersecurity-statistics-that-matter-in-2019/
77. Publications Office. (2019). *Legal acts – statistics*. Retrieved February 26, 2019 from: https://eur-lex.europa.eu/statistics/legal-acts/2017/legislative-acts-statistics-by-type-of-act.html
78. PwC. (2018). *Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies.* Retrieved November 17, 2018 from: https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html
79. Ramboll. (2018). *Create business benefits through complaince related projects.* Retrieved January 15, 2019 from: https://www.ramboll.com/-/media/files/rm/it-i-praksis---artikler/it-in-practice/create-business-benefits-through-gdpr-compliance-projects.pdf?la=en

80. Reference, O. (2019). *Oxford Reference*. From Oxford Reference: http://www.oxfordreference.com/view/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-243
81. Regulatory Policy Committee. (2015, April). *Evaluating costs and benefits for regulatory purposes.* Retrieved January 26, 2019 from: https://regulatorypolicycommittee.weebly.com/uploads/7/8/8/5/78855130/direct_and_indirect_impacts_of_regulation_on_business_dec_2016_version.pdf
82. Renda, A., Schrefler, L., Luchetta, G., & Zavatta, R. (2013, December 10). *Assessing the costs and benefits of regulation.* Retrieved May 2, 2019 from: http://ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/131210_cba_study_sg_final.pdf
83. Rodriguez, S. (2018, January 22). *Business booms for privacy experts as landmark data law looms*. Retrieved January 7, 2019 from: https://www.reuters.com/article/us-cyber-gdpr-consultants/business-booms-for-privacy-experts-as-landmark-data-law-looms-idUSKBN1FB1GP
84. Rosemain, M. (2019, January 21). *France fines Google $57 million for European privacy rule breach.* Retrieved April 26, 2019 from: https://www.reuters.com/article/us-google-privacy-france/france-fines-google-57-million-for-european-privacy-rule-breach-idUSKCN1PF208
85. Sandle, P. (2018, November 5). *Web creator Berners-Lee launches contract for better internet*. Retrieved February 12, 2019 from: https://www.reuters.com/article/us-portugal-websummit-berners-lee/web-creator-berners-lee-launches-contract-for-better-internet-idUSKCN1NA2CX
86. Schmidl, M., Lutz, H., & Seidel, H. (2019). *German Authority issues first fine under GDPR.* Retrieved January 2, 2019 from: http://www.bakerinform.com/home/2018/12/3/german-authority-issues-first-fine-under-gdpr
87. Schmitz, A. (2019). *When Should I Hire In-House Counsel?* Retrieved January 4, 2019 from: https://www.upcounsel.com/blog/hire-house-counsel
88. Schneier, B. (2017, August 24). *On internet privacy, be very afraid*. *The Harvard Gazette*. Retrieved February 13, 2019 from: https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/
89. Shaw, J. (1996). *Law of the European Union.* London: Palgrave; 2nd edition.
90. Sirota, D. (2018, April 23). *GDPR: A Cost vs. Benefit Analysis*. Retrieved November 11, 2018 from: https://www.informationweek.com/strategic-cio/security-and-risk-strategy/gdpr-a-cost-vs-benefit-analysis/a/d-id/1331616
91. Smith, O. (2018, May 2018). *The GDPR Racket: Who's making money from this $9bn shakedown.* Retrieved August 27, 2018 from: https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#7e2318d334a2

92. Spikeworks. (2017, June 21). *How the EU can fine US companies for violating GDPR.* Retrieved February 26, 2019 from: https://community.spiceworks.com/topic/2007530-how-the-eu-can-fine-us-companies-for-violating-gdpr?utm_source=copy_paste&utm_campaign=growth).
93. Standard Cost Model Network. (2019). *International Standard Cost Model manual.* Retrieved January 18, 2019 from: https://www.oecd.org/regreform/regulatory-policy/34227698.pdf
94. Statista. (2018, May). *Average estimated GDPR costs for FTSE100 companies in the United Kingdom (UK) in 2018, by company size (in million GBP).* Retrieved August 27, 2018 from: https://www.statista.com/statistics/869550/gdpr-implementation-cost-by-company-size/
95. The Commission of the European Communities. (2003, May 20). *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.* Retrieved February 3, 2019 from EUR -: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361
96. The Economist. (2017, May 6). *The world's most valuable resource is no longer oil, but data*. Retrieved February 14, 2019 from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
97. Tiel, B. v. (n.d.). *Creating a competitive advantage with GDPR.* Retrieved January 17, 2019 from: https://www.pwc.nl/en/insights-and-publications/services-and-industries/entertainment-and-media/dutch-entertainment-and-media-outlook-2018-2022/article-creating-a-competitive-advantage-with-gdpr.html
98. Translegal. (2019). *Territorial scope*. Retrieved February 17, 2019 from: https://www.translegal.com/legal-english-dictionary/territorial-scope
99. United Nations. (2013, March 21). *Deputy UN chief calls for urgent action to tackle global sanitation crisis*. Retireved January 4, 2019 from: https://news.un.org/en/story/2013/03/435102-deputy-un-chief-calls-urgent-action-tackle-global-sanitation-crisis#.VpzAAfkrLIX
100. United Nations. (2019). *Universal Declaration of Human Rights*. Retrieved April 29, 2019 from: https://www.un.org/en/universal-declaration-human-rights/index.html

APPENDICES

APPENDIX 1: POVZETEK V SLOVENSKEM JEZIKU

Naša zasebnost še nikoli ni bila tako ogrožena, kot je danes in to lahko med drugim pripišemo tudi monetarni vrednosti naših osebnih podatkov, ki jo podjetja s pridom izkoriščajo, napredek informacijske tehnologije pa še dodatno vzpodbuja.

Ozaveščenost o pomembnosti varstva naših osebnih podatkov postaja vse močnejša – poleg večjih zlorab, ki smo jih doživeli v letu 2018 (med najodmevnejšimi npr. Facebookova afera s Cambridge Analytico), je k temu močno pripomogla tudi Splošna uredba o varstvu podatkov (v nadaljevanju: Uredba), ki je bila sprejeta s strani Evropske unije leta 2016 in dokončno stopila v veljavo 25. maja 2018.

Velike odmevnosti Uredbe pa ne moremo pripisati samo področju njenega urejanja, temveč tudi drugim lastnostim – od tega, da Uredba prvič v zgodovini velja za vsa podjetja, ki obdelujejo osebne podatke evropskih državljanov (torej tudi za vse največje ameriških korporacije), do višine predpisanih kazni za kršitve, ki lahko znašajo tudi do 20 milijonov EUR oz. 4 % letnega prometa, če je ta višji.

V nalogi smo omejili področje raziskovanja na vpliv, ki ga ima Uredba na podjetja. Ker gre za aktualno področje, se stvari hitro spreminjajo, hkrati pa smo omejeni s količino (znanstvenih) podatkov. Zaradi tega je bil pristop do raziskovanja zelo holističen in je poskušal upoštevati vse možne vidike, ki so trenutno znani in nam lahko podajo celostno sliko vpliva in s tem razumevanja odziva podjetji tako v pretekolosti kot tudi za naprej.

Raziskovanje vpliva se začne s pregledovanjem glavnih pravnih lastnosti Uredbe, ki nam da splošen oris predmeta raziskovanja. Ugotavljamo, da so pravna narava Uredbe, razširjena teritorialna pristojnost ter prepočasen odziv zagotavljanja ustrezne nacionalne zakonodaje s strani držav članic najpomembnejše karakteristike Uredbe glede na njihov vpliv na podjetja.
Za podrobno razumevanje vpliva Uredbe pa se lotimo raziskovanja na dveh nasprotujočih si koncih – od skrajno pozitivnih (ki presegajo le klasičen izogib kaznim za kršitve), do vseh negativnih vplivov, ki se izražajo v nastalih stroških.

Ob pregledu vseh potencialnih stroškov vzamemo kot osnovo kombinacijo Standard Cost Model Framework ter kronološko nastajanje stroškov ob implementaciji skladnosti v podjetju. Pregled podatkov kaže, da je tako posamezna kategorija stroška kot tudi njegova višina odvisna od mnogih lastnosti podjetja, kar otežuje kakršnokoli generalizacijo glede stroškov. Med glavnimi faktorji smo zaznali velikost podjetja, naravo produkta/storitev, lokacijo ter lastno interpretacijo Uredbe s strani podjetja.

Pri pregledu vseh možnih koristi najprej raziščemo primarno korist skladnosti s katerokoli zakonodajo – izogib kazni ob potencialih kršitvah. Tu si lahko pomagamo s štirimi kaznimi, ki

so jo do sedaj izdali pristojni organi. Kljub močnim odstopanjem v višini kazni (od 4.800 EUR do 20 milijonov EUR) pa kazni kažejo na izjemno relativen pristop do vsakega podjetja in potrjujejo holistično ocenjevanje vsake kršitve, kot to predvideva tudi Uredba. Poleg kazni opravimo še pregled vseh t. i. sekundarnih koristi (konkurenčna prednost, storitev svetovanja, povezanega z Uredbo, izboljšanje poslovnih procesov etc.), ki se pri pregledu praktičnega primera izkažejo za veliko bolj dobičkonosne.

Tretji del raziskave vpliva Uredbe na podjetja opravimo na praktičnem primeru, in sicer z analizo podatkov izbranega podjetja. Stroški, ki so nastali, so v veliki večini povezani s stroški dela, koristi pa s povečanjem prodaje in varnosti na podlagi implementiranih ukrepov. Ob primerjavi stroškov in dobička z naslova Uredbe v manjši meri sicer prevladajo koristi, a je jasno, da odločitev za implementacijo zahtev pri večini podjetji ne bo utemeljena zgolj s finančnega vidika. Vse to kaže, da bodo podjetja usmerjala porabo sredstev, povezanih z zahtevami Uredbe, v tiste ukrepe, ki jim v poslu prinašajo največ koristi.

Za konec izpostavimo še vprašanje etične in moralne odgovornosti podjetij do varstva osebnih podatkov onkraj racionalizacije odločitev na podlagi maksimizacije dobička.