UNIVERSITY OF LJUBLJANA
FACULTY OF ECONOMICS

MASTER'S THESIS

THE EFFECTS OF THE GENERAL DATA PROTECTION REGULATION (GDPR) ON DIGITAL MARKETING PRACTICE IN SLOVENIA

Ljubljana, September 2020 DİLARA ÖZBAY

AUTHORSHIP STATEMENT

The undersigned Dilara Özbay, a student at the University of Ljubljana, Faculty of Economics, (hereafter: SEB), author of this written final work of studies with the title The Effects of The General Data Protection Regulation (GDPR) on Digital Marketing Practice in Slovenia, prepared under supervision of Assoc. Prof. Vatroslav Škare, Ph.D. and co-supervision of Prof. Vesna Žabkar, Ph.D.

D E C L A R E

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 FELU'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 FELU's Technical Guidelines for Written Works;

4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence 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 FELU in accordance with the relevant FELU 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 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 FELU 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 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, _____ Author's signature: _____

(Month in words / Day / Year,
e. g. June 1st, 2012

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

EC – The European Council

EP – The European Parliament

EU – The European Union

CCPA – The California Consumer Privacy Act

GDPR – The General Data Protection Regulation

ZVOP – (sl. Zakon o Varstvu Osebnih Podatkov); Personal Data Protection Act

INTRODUCTION

The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information.

Andrus Ansip,
European Commission vice president for the Digital Single Market

The General Data Protection Regulation (hereafter: GDPR) is the newest and toughest European Union (hereafter: EU) privacy and security law passed in April 2016 and came into force in May 2018. The GDPR introduced strict rules regarding the usage of personal data of European data subjects by organizations regardless of the location of organizations. The GDPR provides increased control for all EU data subjects over their personal data and how it is collected and used worldwide (Wolford, 2019). The GDPR unifies the European fragmented national data protection environment in one regulation. With this standard regulation, it was planned to reduce "the costly administration burden of complying with different national data protection laws for entities processing personal data across the EU" (Tamò-Larrieux, 2018, p. 83).

According to the GDPR, organizations must integrate data protection into all of their activities and new products; all companies regardless of their location have to comply with the law if they are processing the personal data of any data subject residing within EU; businesses have to obtain data subjects' consent before processing their data (Wolford, 2019). In case of non-compliance, a business could be fined up to 10 to 20 million Euro or two to four percent of the firm's worldwide annual revenue (Article 83 GDPR). Under the GDPR, EU data subjects gain more control over their personal data, including how it is collected and used worldwide. There are eight main new and extended rights granted which are (Chapter 3 GDPR);

- The Right to Be Informed,
- The Right to Access,
- The Right to Rectification,
- The Right to Be Forgotten,
- The Right to Restrict Processing,
- The Right to Data Portability,
- The Right to Object,
- Rights in Relation to Automated Decision Making and Profiling

Looking from the consumers' perspective, it is seen that online users are getting more and more privacy-conscious. In 2013, just 18 percent of online users stated they were worried about the internet eroding their personal privacy and this figure increased to 25 percent in 2018 (Hedencrona, 2018). Researches show that consumers perform a simple risk-benefit

calculation before deciding to disclose their personal data, trying to preserve their privacy as much as possible. If the benefit of sharing personal data outweighs the risk, then they are likely to disclose (Wu, Huang, Yen & Popova, 2012, p. 891).

Another striking statistical information is presented by the Federation of European Direct and Interactive Marketing (FEDMA). According to *Global data privacy: What the consumer really thinks* report which was commissioned by the Global Alliance of Data-Drive Marketing Associations (GDMA) in 2018, 51 percent across all the markets that were surveyed said trust is key in their decision to share information with a company. The research also highlights that 86 percent of consumers want more transparency and 83 percent of them want more control when it comes to their data in order to build trust (FEDMA, 2018). Knowing this situation, with the GDPR, Europe planned to ease the consumers' concerns and build trust between businesses and consumers by achieving transparency between them.

During these two years since the GDPR came into effect, businesses have been experiencing an increase in data requests from consumers to know what data a company holds on their file, a struggle to locate all data that a company currently holds across all channels and communication methods, reduced marketing databases due to people either unsubscribing from mailing lists or failing to reply to emails asking them to opt back in, and loss of important records due to the deletion of customer information (HR News, 2018).

For marketers, this meant updating their privacy policies, being as transparent as possible about how consumers' data is being used and maintained, and finding innovative new ways to connect with customers and gather their active consent to use their data in order to continue "marketing relationship" with them (Weiss, 2018).

Due to the fact that the GDPR is one of the newest and the most important regulations of 21st century regarding consumer privacy, the topic has a great potential that is not explored fully yet, especially regarding Slovenia. Therefore, the biggest motivation of this thesis to be written lies in its uncharted nature as well as the pure curiosity about how small and medium enterprises are dealing with the regulation. Therefore, the purpose of this thesis is to see how digital marketing is changing under GDPR and how companies are adapting to this new digital environment in Slovenia with the focus on small and medium enterprises.

The sources of data include both secondary and primary data. In order to grasp the core of the matter, the first part of this research starts with consumer's approach towards privacy so that the ideology behind the GDPR is understood better. Then it continues with the regulation itself with the reference to Slovenia to shed light on what the GDPR is all about, the rights the consumers have and Slovenia's attitude towards the regulation, which is followed by the application of the GDPR in context of marketing in order to evaluate the effects, opportunities and challenges that the regulation presents for the digital marketing practices.

In order to observe how the theory part reflects itself in practice, the second part of the thesis is shaped by the qualitative research to see how Slovenian small and medium businesses are

coping with the GDPR and how their digital marketing practices are transforming compared to each others'. For this reason, seven in-depth interviews are conducted in order to answer the following research questions:

- How did companies' marketing activities get affected due to GDPR?
- What kind of changes did the companies employ in their marketing practices because of GDPR?
- What are the threats and opportunities of GDPR in the context of their marketing activities?

Based on the analysis of the qualitative research's findings, several practical implications are presented in the last part of this thesis. These implications include education of employees, use of analytical tools, utilization of marketing channels, and gaining customer's loyalty, which can help Slovenian digital marketing teams gain and keep customers in the era of active consent.

1 CONSUMER PRIVACY CONCERN AND TRUST

In his book; *Privacy and Freedom*, Alan Westin (1967) defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). By keeping the personal information away from the others, individuals believe that they protect themselves from the possible threats. On the internet, privacy functions as a defence mechanism for individuals' anonymity. However, preserving anonymity in the Big Data era is almost impossible. As a result, customers online have been trading off between privacy and service.

According to "Global data privacy: What the consumer really thinks" report which was commissioned by the Global Alliance of Data-Drive Marketing Associations (GDMA) in 2018, half of consumers (51 percent) across all the markets that was surveyed said trust is key in their decision to share information with a company. The research also highlights that 86 percent of consumers want more transparency and 83 percent of them want more control when it comes to their data in order to build trust (FEDMA, 2018).

The argument supporting the consumer privacy protection is quite straightforward; as data subjects are not capable of protecting their own privacy in this highly networked and digitalized era, policymakers must take the responsibility to protect them (Tamò-Larrieux, 2018, p. 34). As a result, with the GDPR, Europe plans to ease the consumers' concerns and build trust between businesses and consumers by achieving transparency.

1.1 Consumer Privacy Concern

Until a decade ago, the robust anonymization assumption worked quite well both for the businesses and consumers online. Data administrators could protect privacy when sharing data with third parties and data subjects could be at ease that their data remained private. However, over the past years, computer scientists have proved that even anonymized data can often be re-identified and attributed to specific individuals easily (Tene & Polonetsky, 2012, p. 65). Computer scientists also state that it is almost impossible for any database to be perfectly anonymous as the utility of data increases, the privacy decreases, inversely (Ohm, 2010, p.1706). Furthermore, this easy re-identification can cause data subjects significant harm which is difficult to avoid.

Being aware that their data is not safe in the Big Data era, users online are getting more and more privacy conscious, now they care more about how their data is used, stored and shared. In 2013, just 18 percent of users online stated they were worried about the internet eroding their personal privacy and this figure increased to 25 percent in 2018 (Hedencrona, 2018). Users also have concerns specifically about the use of their data. Globally, over one in four internet users strongly agree with the statement "I worry about how my personal data is being used by companies" (Hedencrona, 2018). Part of the reason for these concerns may be that many consumers all around the world have been victims of identity theft and data breaches, with sensitive information such as email or credit card data being disclosed outside of their control.

Researches show that consumers perform a simple risk-benefit calculation before deciding to disclose their personal data, trying to preserve their privacy as much as possible. If the benefit of sharing personal data outweighs the risk, then they are likely to disclose (Wu, Huang, Yen & Popova, 2012, p. 891). Users online also are using a number of tools to protect their privacy. The most popular activity among today's users is deleting cookies as 46 percent of the consumers deleted cookies in April, 2018, one month before the enforcement of the GDPR. This situation prevents businesses from collecting their browsing information, shielding their digital footprint and blocking the processing of personal data with cookie deletion and opt out activity (Hedencrona, 2018).

Online privacy concern leads to a lack of willingness to provide personal information online or falsifying it. This situation affects the validity and completeness of consumer databases and limits the development of e-commerce. Furthermore, the incomplete or invalid databases lead to inaccurate targeting, wasted effort and time, and frustrated consumers (Wu, Huang, Yen & Popova, 2012, p. 890).

1.2 Impact of Trust on Consumer Behaviour

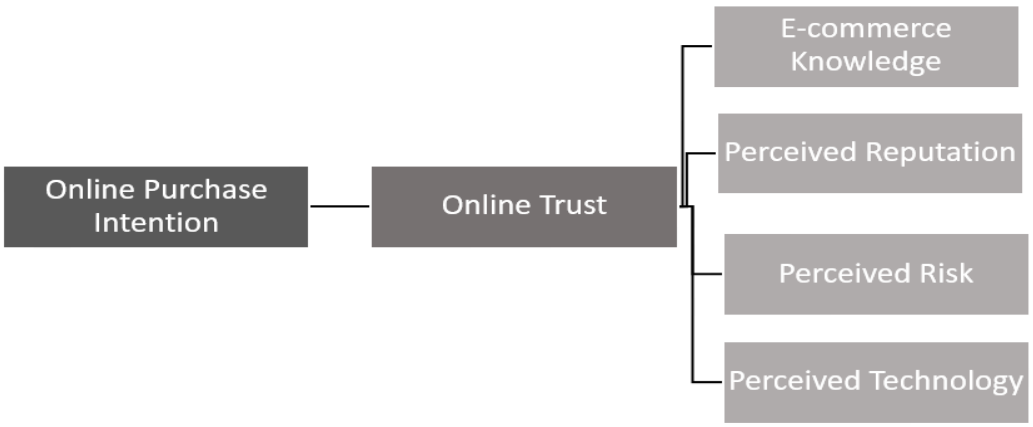
Cambridge Dictionary defines trust as "to believe that someone is good and honest, and will not harm you, or that something is safe and reliable". Looking at the definition, it is seen that

there are three elements that need to be present for trust to occur (Bauman & Bachmann, 2017):

- Two actors (trustee and trustor)
- Vulnerability (there should be a risky of uncertain situation in order trust to exist)
- Context (trust is context-sensitive so it depends on the context of the given situation)

While buying online, consumers (trustors) find themselves in a risky situation, as they have to submit their personal information in exchange with the product/service of companies (trustees). In online transactions, there are two uncertainties that are always present; the risk of losing money during the exchange and the threat of penetration of the private sphere (Kumar & Dange, 2012). This inevitability of risks/threats makes the cultivation of trust necessary if consumers intend to engage in online exchanges and enjoy the potential benefits without the fear of risks overshadowing the online experience.

Figure 1: Factors influencing consumer trust and its impact on online purchase intention



Source: Beldad, Jong & Steehouder (2010).

As Figure 1 shows there are four main factors which affects online trust and consequently, online purchase intention (Beldad, Jong & Steehouder, 2010, p. 860):

- *E-commerce knowledge*: Consumers who know the technologies related with e-commerce and have experience with e-commerce are more inclined to trust online transactions.

- *Perceived reputation*: Seller-based information and/or word-of-mouth provides assurance about the seller's ability and goodwill, and trust naturally follows if the perceived reputation is good.

- *Perceived risk*: The uncertainties of the Internet influence consumers negatively as they prefer not to participate in e-commerce if the level of risk (such as no-refund, danger of payment method and quality of the product/service) exceeds the potential benefits.

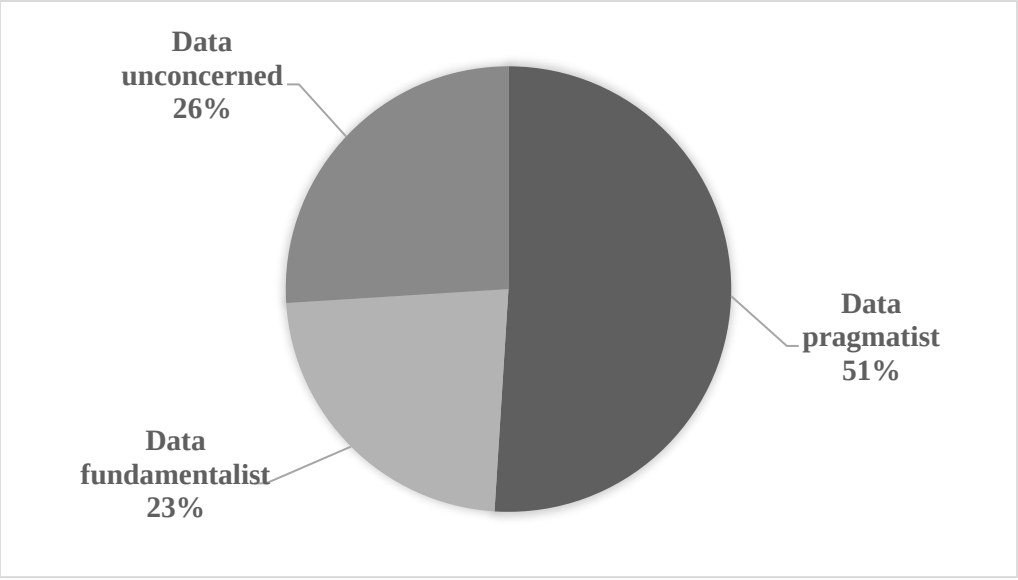
- *Perceived technology*: Information which is useful and easy to understand on websites, and ease of use the website reduces the asymmetric information, and promotes trust.

When e-commerce knowledge and perceived technology are high; perceived reputation is positive; and perceived risk is low, online trust is achieved. This trust brings the intention of online purchase which can be defined as consumers' willingness to build online relationships.

1.3 The Trade off Between Privacy, Risk and Trust

According to GDMA's report (2018), the majority of respondents across the 10 markets and four continents surveyed are "Data pragmatists" who will decide whether to share their personal information on a case-by-case basis, dependent on the benefits as it is mentioned before while one in four respondents have little concern about how their data is collected and used, which the study describes as the "Data unconcerned". On the other hand, those consumers who are unwilling to provide their personal information, even in return for service enhancement are referred as "Data fundamentalists" and they accounted for just under a quarter of respondents. Figure 2 shows the percentage distribution of key consumer online types.

Figure 2: Consumer segmentation according to their attitude towards privacy



Source: FEDMA (2018).

As the majority of users online are Data pragmatists, they fit to the loop of privacy, risk and trust. Their attitudes and perceptions about the site influence their actions when they believe that certain behavior will be linked to a specific outcome. Based on the same logic, users' perception and attitudes regarding privacy, risk and trust should influence their attitudes (Liu et al., 2005, p. 291). As "privacy as the major antecedent of trust" (Liu et al., 2005, p. 291), consumers enter the loop from privacy and then move towards trust through risk calculation.

The more the users online see their privacy is protected, the more they may allow services to use their data as they do not fear the privacy would be abused. Users start to share their patterns, preferences, routes, routines, shopping lists, location and other inputs that will improve services willingly (Fish, 2009, p. 96). The converse situation is also true; the more the users see someone or service abuse their privacy, friends, social groups and the media invading their privacy, the more they fear and doubt, and they stop using the service. Therefore, it is not surprising that according to Cisco survey in 2019, 90 percent of these privacy-active consumers believe the ways their personal data is treated reflect how companies treat them as customers, and as a result, they will not buy from companies if they do not trust the way their data is used (Redman and Waitman, 2020).

Looking at the risk calculations, it is seen that; risk that is rewarded in terms of service or product lowers fear, doubt and uncertainty about the service and allows the users online to share more data about them to engage more and demand better services (Fish, 2009, p. 96). On the other hand, risk that is failed and brings damage to the users' reputation or relationships will damage the trust and their willingness to take a chance on the next service.

Protected privacy, rewarded risk or the opposite are the determiners of trust as it is mostly based on previous experience. It determines how much the users online will be prepared to trust a service provider they have or have not previously used. The more the users trust them with their data, the higher the risk, the more privacy they impart, but the better the services they get (Fish, 2009, p. 97). Sharing more personal data such as routes, routines, patterns, preferences and recommendation makes services improve, and receiving better service makes the users trust and lowers their fears about privacy.

1.4 Privacy Policy and Trust

The development of trust between the consumers and marketers reduces the consumers' perceived risk and increases their willingness to share their personal information (Wu, Huang, Yen & Popova, 2012, p. 892). Privacy policies play an important role in trust development and as a result; consumer decision-making process. However, interestingly, consumers were used to misjudging privacy policy as data protection policy. The researches showed that when consumers saw the term "privacy policy," they believed that their personal information would be protected in specific ways (Tene & Polonetsky, 2012, p. 67).

Consumers online used to assume that a website that advertises a privacy policy would not share their personal information as the website giving them a sense of control. However, this was not the true; privacy policies used to simply inform consumers that unless they "opt out" of sharing certain information, the company would share their personal information to other commercial entities (Turow, 2007, p.724). It is important to highlight that this practice was before the GDPR as the regulation strictly bans it (Article 4 GDPR).

Although in this sense, consumers seem like they are more interested in the existence of the privacy policy rather than the content of it, they purport the opposite. According to RSA's 2017 Consumer Cybersecurity Confidence Index, 93 percent of the respondents wanted to be involved in the process of how their personal information and accounts were protected online (Bleau, 2017). Therefore, it is not surprising that according to Cisco's survey in 2019, 83 percent of the consumers stated that they read privacy policies if they can understand (Redman and Waitman, 2020).

1.5 Changing Perspectives of Consumers

Even though consumers seem to be very reserved about sharing their personal information online, more and more consumers are aware that providing personal information is beneficial as many know that when they provide detailed and accurate information, they get better service, more relevant messages and promotions (Ridley-Siegert, 2015). Although 74 percent of users online still have some degree of concern about their online privacy, 51 percent of global consumers are still happy to exchange their data with businesses, as long as there is a clear benefit for doing so. 41 percent of users also understand that sharing data is an essential part of the smooth running of modern society (FEDMA, 2018).

Still, it is important to state that becoming willing to share personal data does not mean that consumers are happy with the businesses' current practices of collecting data. Websites have to inform the visitors they are using cookies via online banners that appear when users enter the site. However, this approach is not perceived as the right approach as half of European consumers prefer to have access to information that explains how their data will be used for advertising, with the option of prevention of any use of their data that they object to (Davies, 2017). The users want a better option than having to approve the use of cookies every time they visit a site as the pop ups are perceived as interruption to the primary task which is the reason why the users visit a website (Pellat & Hoareau, 2019). The interruption mostly causes irritation and consequently, it affects the satisfaction with the website experience (p. 245).

In this sense, it can be stated that privacy is very much about customer experience as it is about privacy itself. Therefore, the feedback from customers not only regarding the products and services the companies provide but also the privacy policies is highly important in the process of convincing customers to share their personal data. As an unknown prognosticator stated once "privacy will be to the Information Age as product safety was to the Industrial

Age" (Redman and Waitman, 2020). Thereby, companies should efficiently invest into consumer privacy rights in order to survive as consumers are getting more and more conscious about their privacy and their tolerance level drops consequently.

1.6 Online Security

Privacy and security are persistent concerns for users online that continued to increase in recent years. Although businesses pay more and more money for cyber security, data breaches exposed 4.1 billion records in the first half of 2019 with the average hacker attacks of 2,224 times a day (Sobers, 2020). Being highly aware that their sensitive information is at risk every second they are on the web, consumers try to be precautious as much as they can. The easiest precaution that users online can take is to check webpage security.

At this point, SSL certificate steps in. SSL, which stands for 'Secure Sockets Layer', is the standard technology ensuring all data (passwords, credit card information, phone number, and other personal data) that passes between a server and a user stays private and guarantees protection against hackers (Kolowich, 2017). Starting from 2017, in Google Chrome, sites lacking SSL certificate have been marked with eye-catching red warning 'Not Secure' right inside the URL bar. This warning is quite important for many users online as according to HubSpot Research in 2017, 82 percent of respondents stated that they would leave the website if they see the warning that the webpage is not secured (Kolowich, 2017). Since Google Chrome accounts for about 68 percent of market share (Statista, 2020), businesses are aware of the necessity to acquire SSL certificates on the way to gain consumer trust.

Another online security system which is often heard is CAPTCHA, which stands for 'Completely Automated Public Turing Test'. While SSL protects users online, CAPTCHA protects websites. It is a type of challenge-response test (mathematical, image-based, reCAPTCHA, and several others) used to determine whether or not the user is human. CAPTCHA helps to protect websites from spam and abuse, including bogus comments, fake registration submissions and fraudulent purchases. As a result, CAPTCHA helps businesses to avoid higher transaction fees/rates and potential account termination/suspension (Wangen, 2017).

SSL and CAPTCHA are two well known examples out of many that businesses employ for website security. Although the security systems can change with the advances in technology, according to many researchers, there are five key security-control requirements of any online transaction, which never change (Suh & Han, 2003):

- **Authentication** is the ability to prove that an individual is genuinely who that person claims to be.

- **Non-repudiation** is the assurance that the sender of information is provided with the proof of delivery, and the receiver is provided with the proof of the sender's identity, so neither of them can deny having processed the information later.

- **Confidentiality** protects sensitive information from unauthorized disclosure.

- **Data Integrity** means ensuring and maintaining the accuracy and the completeness of data over its life cycle.

- **Privacy protection** is keeping the personal information from getting into the hands of businesses, hackers, government organizations, and other groups.

Even though the first four terms may not be known by consumers, the term of privacy protection is sure to be heard by many as starting from 2016, EU have been promoting the game-changer newest data protection regulation, the GDPR, which is discussed in great detail in Chapter 2.

2 DEVELOPMENT AND APPLICATION OF THE GDPR

The General Data Protection Regulation is the newest and toughest EU privacy and security law passed in April 2016 and came to force in May 2018. The GDPR introduced strict rules regarding the usage of personal data of EU data subjects by organizations regardless of the location of organizations. The GDPR provides increased control for all EU data subjects over their personal data and how it's collected and used worldwide (Wolford, 2019). The GDPR unifies the European fragmented national data protection environment in one regulation, aiming to simplify the regulatory environment to do business so both businesses and citizens in the EU can fairly benefit from the digital economy (Albrecht, 2016).

With this standard regulation, it is expected from the GDPR to reduce "the costly administration burden of complying with different national data protection laws for entities processing personal data across the EU" (Tamò-Larrieux, 2018, p. 83). There were (and still are) 28 countries in the EU, all of which has their own regulation; therefore, with "One Continent, One Law" principle, the European Commission estimates that the GDPR will save €2.3 billion per year across Europe (European Commission, 2015).

All businesses within the GDPR scope have no other chance but to comply as the European Commission showed its seriousness with the already imposed sanctions. According to the latest news in May 2020, the number of GDPR fines reached 273 with the total amount of almost 154M €. The biggest fine was implemented to Google France with 50M € while the smallest fine belongs to a Hungarian hospital with 90 € (Data Privacy Manager, 2020b).

Here, it is also important to note what the GDPR actually protects as the title; the GDPR is misleading. Contrary to the title, the regulation is not intended for the protection of the data itself but rather for the rights of the data subjects whose data is being processed (Tamò-Larrieux, 2018, p. 76). Still, these two principles are complementary. Businesses can be regarded as non-compliant of the GDPR if the data they process is not secure. But, being compliant with the GDPR does not always mean that the data is secure as the main focus of the regulation is the rights of individuals not data security (Biagini, 2018).

2.1 History of the GDPR

The history of the right to privacy goes back to the 1950 European Convention on Human Rights in which it was stated, "Everyone has the right to respect for his private and family life, his home and his correspondence" (Wolford, 2019). It was the first step of ensuring privacy right through legislation.

With the enhancement of technology and the invention of the Internet, the EU expanded the scope of right to privacy and passed the European Data Protection Directive (Directive 95/46/EC) in 1995 and it was implemented in 1998. The directive set the basic data privacy and security standards but gave freedom to each member state upon how to implement their own law (Wolford, 2019).

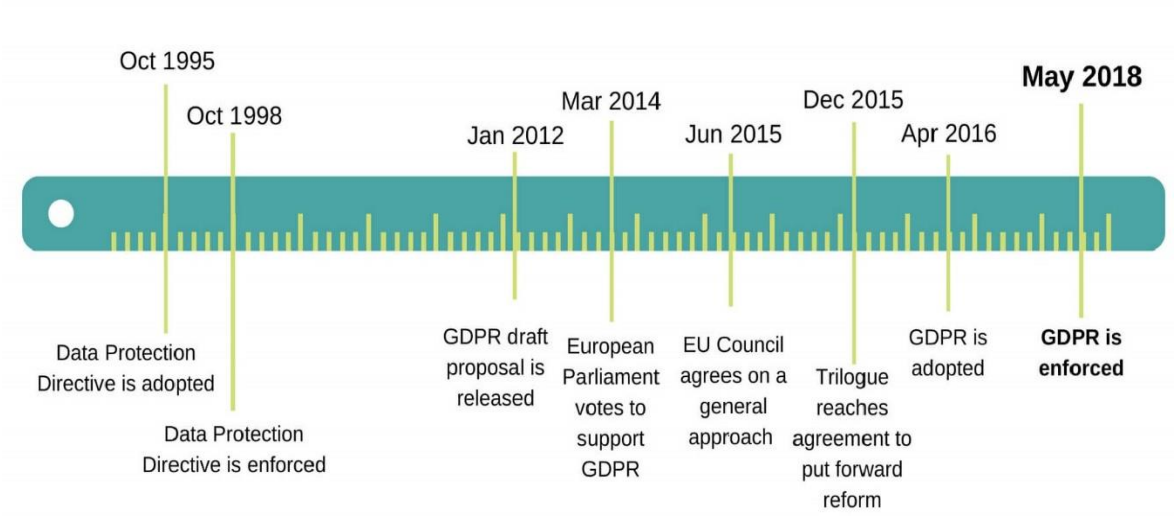
When Directive 95/46/EC was passed in 1995, the Internet was still in its infancy and mobile devices did not exist and therefore; it failed to respond to today's mobile-first world and consequently; it could not provide enough protection for the EU citizens' data and privacy rights. Interestingly, the data protection authorities did not take any steps to upgrade the directive until 2011.

Two months after a user sued Google for violation of privacy rights in 2011, the European Data Protection Supervisor published an Opinion, stating "a comprehensive approach on personal data protection" was needed and started to work on upgrading Directive 95/46/EC in June (Smith, 2017).

In January 2012, the European Commission (EC) proposed a comprehensive upgrade to Directive 95/46/EC which aimed to strengthen online privacy and security rights alongside boosting Europe' digital economy (Smith, 2017).

After the discussions, in March 2014, the European Parliament (EP) showed its support to the new law as the result of voting was 621 in favor, 10 against and 22 abstentions. One year later, EP, EC and Council reached the final agreement on the GDPR (Smith, 2017). In April 2016, EP passed the law named as the General Data Protection Regulation (the GDPR) across the EU and gave two years to all organizations within its scope in order to adapt to new regulation. The GDPR came into force on May 25, 2018 (Wolford, 2019). Figure 3 shows the timeline of European privacy actions' history starting from Directive 95/46/EC.

Figure 3: The GDPR timeline



Source: Akshita (2018).

Although it has been two years since its enforcement, the GDPR has still left a lot of questions which are unanswered even for those who read the law. As a result, the European Data Protection Board has issued several clarifications and guidelines in order to help companies ensure their compliance to the regulation, and additional clarifications on key topics are expected in the coming months (Uzialko, 2020).

Still, like it or not, the GDPR continues to change the digital world, and the EU is determined to remind the existence of the GDPR by the Data Privacy Day, January 28, (Council of Europe, 2020) which is celebrated more gloriously than it was for the last fourteen years.

2.2 GDPR Terminology

In this section, the key terms of the GDPR are defined in order to provide better understanding for the following sections. According to Article 4 the GDPR:

- **Personal data:** Any information related to an identifiable natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, a location data or banking details.

- **Data Controller:** A natural or legal person, alone or jointly with others, who determines the purposes and means of the processing of personal data.

- **Processing:** Any operation performed on personal data, whether or not by automated means such as collection, recording, organisation, structuring, storage, otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Data Processor:** A natural or legal person, public authority, agency or other body which processes personal data on the behalf of the data controller.

- **Profiling:** Any form of automated processing and use of personal data to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, behavior, location or movements.

- **Binding Corporate Rules (BCRs):** Personal data protection policies adhered to a controller or processor established on the territory of a Member State for transfers of personal data to a controller or processor in third countries within a group of undertakings or group of enterprises engaged in a joint economic activity.

- **Pseudonymization:** The processing of personal data in such a manner that the personal data can no longer be attributed directly or indirectly to a specific data subject without the use of additional information which is kept separately.

- **Biometric Data:** Personal data resulting from specific technical processing relating to the physical, behavioral or physiological characteristics of a natural person which allow or confirm the identification of that person.

- **Cross-Border Processing:** Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in EU where the controller or processor is established in more than one Member State; or processing of personal data that takes place in the context of the activities of a single establishment of a controller or processor in EU but affects or is likely to affect data subjects in more than one Member State.

2.3 Key Changes: How the GDPR Differs from Directive 95/46/EC

Directive 95/46/EC was the pioneer of accepting data privacy as a fundamental human right. The Directive aimed to protect EU citizens' privacy rights and provide basic level of data security inside and outside of Europe by harmonizing privacy laws among the all EU members (Fromholz, 2000, p. 462). However, although the Directive was approved by the EU itself, it was not self-implementing. Each EU member was expected to pass their own legislation in order to implement the Directive, so it did not have the power to enforce its articles (Fromholz, 2000, p. 467). As a result, the Directive failed to achieve a single international standard. Although the GDPR still holds the key principles of Directive 95/46/EC, in terms of design, scope, penalties, consent and data subject rights, the GDPR is more comprehensive, unifying, demanding and most importantly; it is legally-binding.

2.3.1 Data Protection by Design and Default

Privacy by design is not a new concept; it has always been a part of data protection law. The only change is that now it is a legal requirement. According to the GDPR, organizations must integrate data protection into all of their activities and new products (Wolford, 2019). Article 25 also states that data controllers must implement appropriate technical and organizational measures to guarantee that, by default, only the necessary personal information for each specific purpose is processed. This obligation applies also to the amount of personal data that are collected, the extent of their processing, the duration of their storage and their accessibility (Article 25 the GDPR).

2.3.2 Scope

According to the GDPR, all companies regardless of their location must comply with the law if they are processing the personal data of any data subject residing within the EU (Wolford, 2019). The Directive also had a similar attitude towards the data processing limitations, but it was highly ambiguous and far from legally-binding (Fromholz, 2000, p. 462). With the new regulation, the definitions are clear and certain. According to Article 3, if processors process data of an EU residents, offer goods or services to them (paid or free) and monitor their behavior within the Union, they are subject to the provisions of the GDPR regardless of the companies' location which is known as "extra-territorial effect" (Wolford, 2019).

2.3.3 Penalties

The GDPR implements heavy fines in case of violations in order to make sure all businesses are compliant with the regulation. There are two tiers of the fines as the GDPR acknowledges some violations are more serious than others. In case of non-compliance which includes the obligations of the data controllers and processors, a business could be fined up to 10 million EUR or two percent of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. The GDPR considers this type of infringement as less severe; therefore, the fines are relatively less. The more serious infringements are the ones going against the main principle of the GDPR; the right to privacy and the right to be forgotten. In case of negligence which includes the breaches of the conditions to process and transfer data, consent and data subject rights, the fine goes up to 20 million EUR or four percent of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher (Wolford, 2019 & Article 83 the GDPR).

2.3.4 Consent

The GDPR strengthened the conditions for consent and introduced new rules of what constitutes consent from data subjects in order to process their data. According to Article 7, these new rules are (Wolford, 2019):

- The request for consent must be distinguishable from other matters and has to be stated in an intelligible and a clear form.
- Consent must be freely given, specific, informed and unambiguous.
- Data subjects should be able to withdraw previously given consent whenever they want, and businesses have to respect their decision. They cannot change the legal basis of the processing to one of the other justifications.
- Children who are under 13 can only give consent with permission from their parents.
- Businesses have to keep documentary evidence of consent.

2.3.5 The Rights of Data Subjects

Under the GDPR, EU data subjects gain more control over their personal data, including how it is collected and used worldwide. There are nine main new and extended rights granted under Chapter 3 the GDPR, which are the following (Wolford, 2019):

- **Right to Be Informed:** Data subjects have the right to know who is processing their personal data.
- **Right to Access:** Data subjects have the right to access any personal data collected about them. If asked, data controllers must provide a copy of the personal data in an electronic form for free.
- **Right to Rectification:** Data subjects have the right to require organizations to correct inaccurate personal data or complete it if it is incomplete.
- **Right to Be Forgotten:** Data subjects have the right to require their personal data to be erased and to prevent further data collection.
- **Right to Restrict Processing:** Data subjects have the right to request organizations to restrict the processing of their data. In this case, organizations are allowed to store the data but not to use it.
- **Right to Data Portability:** Data subjects have the right to require organizations to move, transfer or copy their data to a recipient of their preference in a secure way.

- **Right to Object:** Data subjects have the right consent or withdraw consent to the processing of their data.
- **Right to Know When One's Data Has Been Hacked:** Data subjects have the right to be notified within 72 hours in case of data breaches which put individuals at risk.
- **Rights in Relation to Automated Decision Making and Profiling:** Data subjects have the right to opt out of the usage of their data by automated systems, including profiling.

However, there are several instances that the data subjects cannot exercise their rights as depending on the basis of the data processing, some rights do not apply which are demonstrated in Table 1 for a better understanding. Knowing which right applies in which situation, businesses can save time and effort when they need to process personal data. For example, if the processing is necessary for legitimate interests of businesses or for a task regarding public interest, businesses do not have to gain customers' consent for processing their data as it is shown in Table 1.

Table 1: Six lawful bases for processing

	Right to Erasure	Right to Portability	Right to Object
Consent			X (But have the right to withdraw consent)
Contract			X
Legal obligation	X	X	X
Vital interests		X	X
Public task	X	X	
Legitimate interests		X	

Source: Moore (2018).

2.3.6 Data Protection Authorities and Data Protection Officer

- **Data Protection Authorities (DPAs)** are independent public authorities who supervise the implementation and application of the data protection law through investigative and corrective powers. These authorities provide expert advice on data protection issues and handle complaints about the violations of the GDPR and the relevant national laws. In each EU Member State, there is one (Article 29 the GDPR).

- **A Data Protection Officer (DPO)** is given the formal responsibility for data protection compliance within a business. Not every business will need to appoint a data protection officer; it is necessary when an organization is a public authority; large-scale systematic monitoring of individuals is required or large-scale processing of special categories of data or data relating to criminal convictions and offenses is carried out (Article 37 & 39 the GDPR).

2.4 The GDPR vs The California Consumer Privacy Act

Although the GDPR only concerns with the European citizens, its effect has already become global. One by one, other governments are following the GDPR's lead to create their own data privacy law. Looking at the timeline, California is seen to precede as on June 28, 2018 –one month later from the enforcement of the GDPR- Governor Jerry Brown signed the California Consumer Privacy Act (hereafter: CCPA) and the regulation came into effect on January 1, 2020 (Hospelhorn, 2020).

As the CCPA is significantly inspired by the GDPR, both regulations have the same purpose; protecting the privacy of individuals. In the same way, the GDPR protects the European data subjects' rights, the CCPA serves to protect Californian consumer rights which are ownership, control and security over their personal data, as well as to encourage privacy and transparency (Hospelhorn, 2020). Very similar to the rights GDPR gives, the CCPA grants Californian consumers six main rights which are the following (the CCPA Section 1798.100-125):

- Right to request information
- Right to data portability
- Right to opt-out
- Right to access data
- Right to disclosure
- Right to deletion

Although the GDPR and the CCPA share a lot of common points, the differences between them bear more significance. The key differences include the territorial scope and application of the law; fines; nature and extent of collection limitations; and lawful basis requirement for all processing of personal data (Data Privacy Manager, 2020a).

2.4.1 Who Must Comply?

Unlike the GDPR, the CCPA leaves aside public institutions and non-profit organizations, and solely focuses on for-profit businesses that reside in California, or process personal information of California residents. If a business meets at least one of the following criteria (Hospelhorn, 2020):

- Has an annual revenue of $25M or more
- Collects, shares, buys or sells the data of 50.000 Californian consumers
- Derives at least 50 percent of its annual revenue from the sale of Californian consumer data

2.4.2 Territorial Scope

Looking at the territorial scope, it is seen that like the GDPR, the enforcement of the CCPA is not bound to the territory. As long as a company conducts business with Californian residents, it is subjected to the regulation, no matter where the company is located (Data Privacy Manager, 2020a).

2.4.3 Penalties and Fines

Depending on the violation, the GDPR fines can go from two percent of annual turnover or 10M € to four percent of annual turnover or 20M €, whichever is higher. In terms of fines, the CCPA follows a different system. For each unintentional violation the CCPA dictates $2,500 per record while each intentional violation costs $7,500 per record if not addressed within 30 days (Larose, 2019).

2.4.4 Opt-out vs Opt-in

While the GDPR is based on the opt-in system as it was discussed in Chapter 2.3.4/5, the CCPA focuses on an opt-out system. It means that the CCPA allows businesses to sell personal data of Californian consumers unless they exercise the right to opt-out from their data sold (Data Privacy Manager, 2020a). In this sense, it can be stated that the GDPR gives a lot more control to data subjects as the regulation requires opt-in for every data processing as long as the other lawful bases are not applicable.

2.4.5 Exclusion of Data

Unlike the GDPR which applies to all the personal data, there are several types of data exempted from the scope of the CCPA which are medical information; sale of information to/from consumer reporting agencies; information belongs to clinical trials; publicly available personal information; and personal information under the Gramm-Leach-Bliley Act and Driver's Privacy Protection Act (Data Privacy Manager, 2020a).

No matter the name is GDPR, CCPA or something else, the nature of the data privacy regulations are the same; protecting the privacy of individuals. As the term privacy marks the 21st century, there are many more privacy acts on the horizon, following the GDPR's lead.

2.5 The GDPR Myths

Due to the fact that the GDPR is a pioneer regulation in regard to personal data protection, there are lots of misunderstandings about the regulation, which the EC refers to as the GDPR myths. In order to clear these misunderstandings, in 2019, the EC released a fact sheet called *Mythbusting: General Data Protection Regulation*. Through this fact sheet, the EC invites everyone to stay with the facts one more time. Table 2 summarizes the most striking myths and their actual facts.

Table 2: The GDPR myths and facts

The GDPR Myths	The GDPR Facts
GDPR completely changes the way organizations need to handle their data	The EU has had data protection since 1995, so the GDPR is an evolution of Directive 95/46/EC, which is fit for the digital age
GDPR will stifle European innovation in the fields of artificial intelligence (AI)	The GDPR makes sure that personal data is protected in AI as the regulation is designed to be technologically neutral and provide the framework for the development of an AI respectful of citizens
Landlords cannot put the names of tenants on the doorbell	Consent is not the only legal basis for processing data as long as there is a legitimate interest
GDPR is overwhelming for small businesses	The obligations are calibrated to the size of the business and/or to the nature of the data being processed
GDPR makes journalism harder	The GDPR supports freedom of the press, only when necessary, EU members shall provide for exemptions or derogations to the press in their national laws
Well anyway, Facebook is based in the US	Non-EU companies have to comply with the GDPR too if they are operating in the EU market
GDPR does not give us more control as companies simply ask for consent once and then they do what they want with my data	Companies have to ask for consent a second time if they want to use your data for the second purpose or forward it to a third party. Also, at any point in time, it is possible to use the right to be forgotten

(Table continues)

(Continued)

Table 3: The GDPR myths and facts

GDPR hinders political campaigning	Political parties can process data for campaigns, but only for reasons of public interest and as long as appropriate safeguards are established
We need more time to adapt to these complicated rules	There was a two-year transition period from May 2016 to May 2018. As of now, the data protection authorities have the power to sanction in case of noncompliance
The fines under GDPR can kill a business	Breaking the rules does not automatically mean a €20 M fine as the amount of the fine depends on the circumstances in the individual case, and there are other corrective measures like warnings, reprimands and orders

Source: European Commission (2019a).

2.6 Slovenia and the GDPR

Slovenia is one of the EU member states that has not yet adopted a GDPR implementing law before May 25, 2018 (Koch, 2019). In fact, Slovenian government asked the parliament to fast-track the bill referred as Personal Data Protection Act II (hereafter: ZVOP-2) so that it would come into force before the GDPR. However, the matter was stalled after the parliamentary election in June due to the fact that the bill of such complexity and sensitivity required a regular procedure (STA, 2018b). Only after the adoption of ZVOP-2, there will be a legislation listing violations and providing a basis for enforcement of the GDPR (Miklavčič, 2019).

This situation means that until ZVOP-2 come into force, the current Personal Data Protection Act I (hereafter: ZVOP-1) will still remain in force in order to cover the parts that are not covered by the the GDPR; for example, the provisions on biometrics, protection of personal data of deceased, judicial protection of rights, direct marketing, video surveillance, registering of entries and exits and database linking (Miklavčič, 2019). ZVOP-2 is necessary to come into force as soon as possible in order to provide legal certainty because ZVOP-1 is already out of date as it came into force in 2004 (Informacijski Pooblaščenec, 2014), and in some issues it even contradicts to the GDPR.

In case of collision, The Information Commissioner stated that the European regulation will prevail but he/she does not have the power to impose any administrative fines or other sanctions for violations of the the GDPR but only for the violations of the ZVOP-1 in parts

that remain in force (Horvat, 2018). As a result, inspections which are initiated prior to the GDPR with regard to matters that are regulated by the GDPR also have to be suspended until ZVOP-2 is adopted (Miklavčič, 2019).

Looking from Slovenia's perspective, it is seen that like the other EU members, data subjects in Slovenia are very knowledgeable about the GDPR and determined to defend their rights in case they notice something amiss. According to Information Commissioner, from 2018 to present, the number of inquiries related to the GDPR are already for media; 27, email marketing; 60, and for direct marketing and prize games; 87 (Informacijski Pooblaščenec, 2020), and the numbers are increasing each day. This situation shows that companies need to fasten their compliance process before ZVOP-2 comes into force, otherwise the keen consumers are very likely to fill the GDPR complaint forms.

2.6.1 Slovenia's Attitude towards the GDPR

Although the GDPR is directly applicable, the fact that it entered into force without a prior legal framework (ZVOP-2) causes legal unclarity and confusion for Slovenian businesses. It seems that one of the biggest novelty for Slovenia in regard of the GDPR will be data protection officer (DPO), who however will not have to be appointed at every company but at those that process large amounts of sensitive personal data or whose core activity is processing such data such as banks, insurers, communication companies and retailers which has loyalty programs. According to Slovenian News Agency (sl. Slovenska Tiskovna Agencija), some of these companies have already assigned a person for data protection and they do not expect major difficulties as they had already given due attention to personal data protection up to now. Still, they plan to further improve their systems in line with the GDPR (STA, 2018b).

Different industries have different concerns when they try to be GDPR compliant. Insurer Adriatic Slovenica stated that they are to make the processes such as the collection and processing of clients' data more transparent while the travel agency Kompas consider new marketing approaches because it expects that many of the users will not give their consent to receive ads. Telecommunication companies, T-2 and A1 said that they expect their users to be displeased to receive large amounts of requests for consents. They are also concerned about the adjustments to ZVOP-2 as it can again affect their business operations and cause additional costs. Retailers with loyalty programmes such as Mercator expect that aside from obtaining customers' consent, the tracing of personal data processing to be the most difficult and technically challenging obligation as less than half of individuals open their mail, according to their information (STA, 2018b).

Another issue that the marketing teams have to deal with is the ethical dimension of the GDPR, which dictates that no matter how good and beneficial the marketing purpose is, personal data is personal property, so it should be data subjects' decision how to use it. Scrutinizing several important Slovenian websites, it was seen that most of them failed in

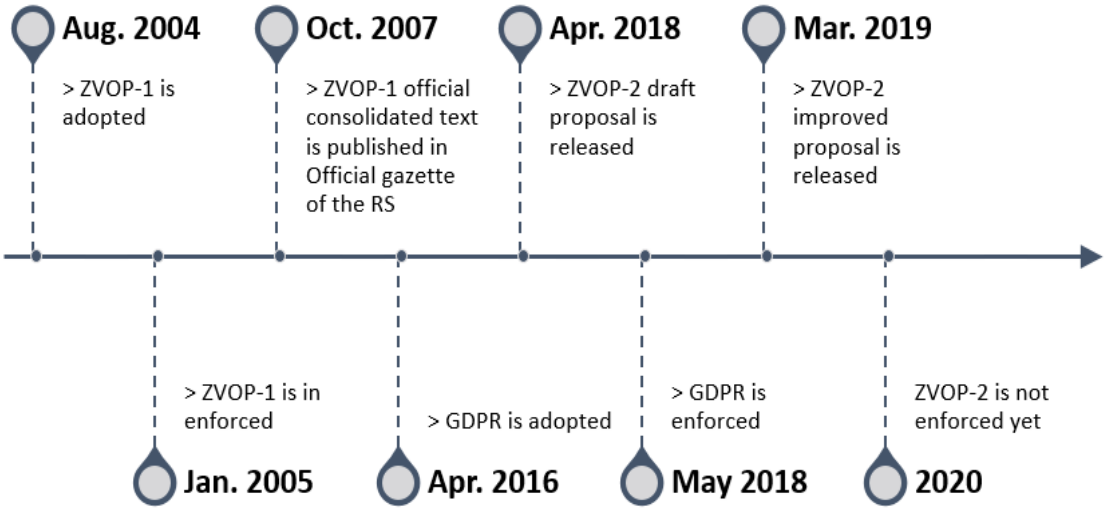
the ethical test. Mercator.si, Slovenia.info, 24ur.com, gov.si (Government of the Republic of Slovenia), ip-rs.si (Information Commissioner) are a few examples which still use invasive trackers, cookies, hidden opt-out options even though the GDPR forbids the businesses to do so (Vrban, 2019). The main reason for this situation is most likely the unsolved mystery of which data is necessary to generate page visits and sales. Due to the fact that, for a decade, Google has been pampering marketing teams with nicely drawn graphs of complex variables. As a result, Slovenian marketing teams are still heavily dependent on analytics tools provided by Google (Vrban, 2019), which are easy to use and low-cost, and reluctant to leave their comfort-zone.

Although ZVOP-2 has not entered into force yet and there are several serious problems caused both by the combined execution of the GDPR and ZVOP-1, and the unclarity of best digital marketing practices, it is seen that Slovenian companies are trying to do their best to improve their businesses to be in compliance with the GDPR and find the best way to utilize their websites for higher sales. But there is still a long way to go.

2.6.2 ZVOP-2 and the GDPR

In Slovenia, the draft proposal for ZVOP-2 was released in April 2018, one month before the enforcement of the GDPR. After the improvements, a new proposal of the Personal Data Protection Act (ZVOP-2) was published by the Ministry of Justice in March 2019 and was expected to be passed in the second half of 2019 (Jerman, 2019). However, in 2020, the proposal of ZVOP-2 is still in progress and waiting to be adopted by the National Assembly. Figure 4 shows the timeline of ZVOP-1 and ZVOP-2 in relation with the GDPR.

Figure 4: ZVOP timeline



Source: European Commission and Informacijski Pooblaščenec (2020).

With ZVOP-2, Slovenia aims to regulate the personal data protection and ensure the enforcement of the GDPR at a national level (Jerman, 2019). However, it seems that ZVOP-2, if adopted in the form of the published proposal, would overstep explicit authorizations granted by Recital 8 of GDPR where the regulation leaves the Member States with a margin of discretion in regulating some of the aspects of the respective national data protection regimes (Merc, 2018).

First of all, ZVOP-2 proposal handles various topics differently and/or in more detail than the GDPR, even where the GDPR does not allow for such specifications or restrictions. For example, ZVOP-2 regulates topics such as use of video surveillance (Article 111-115), processing of data for direct marketing purposes (Articles 109-110), the specific fines for violations of the foregoing (Article 136-141), conditions for the appointment of a data protection officer (Article 48) and expanded obligations data processors (Article 7), which are not regulated by the GDPR. Furthermore, it lowers the age from sixteen to fifteen for the validity for the consent of a minor.

ZVOP-2 does not only modify the GDPR but also adds specific provisions on providing personal data of the deceased to close relatives, the use of personal data for historical or scientific research, statistical or archiving purposes and automated decision–making (Article 44, 82, 83 and 84) (Jerman, 2019). These are just a few striking examples of differences ZVOP-2 possesses compared to the GDPR.

In January 2020, the Ministry of Justice announced that a new proposal was prepared and forwarded for reconsideration after receiving a number of key conflicting comments on the first bill. However, it is highlighted that although there is a good improvement, the proposal is still not good enough to be submitted to the Government of the Republic of Slovenia (gov.si, 2020). The main reason of the delay is due to the fact that the proposal still significantly contradicts with the relatively clear articles of the GDPR, especially about the publication of personal data in compliance with right to erasure and; therefore, it will surely create great confusion in the field of personal data protection if further improvements are not made (Svet Kapitala, 2019).

As a result of this situation, the Information Commissioner as the competent authority still does not have the power to impose administrative fines but it is noted that the regulation was already quite strict and the Slovenian data subjects are well acquainted with their rights, so the country does not face with major problems for now (Miklavčič, 2019). Still, ZVOP-2 needs to come into force to maximize the GDPR's radius of action.

3 APPLICATION OF THE GDPR IN THE CONTEXT OF DIGITAL MARKETING

In today's world, personal data is being collected at an incredible rate. The websites used, the calls made, the places visited and even the photos taken are all recorded, measured and leave a digital footprint which functions as a prized resource. Digital footprints have become so valuable that The Economist called personal data "the world's most valuable resource" ahead of oil (MacDonald, 2019), because of the fact that how much it shapes the way companies communicate with their customers in order to impact customer experience positively. In this section, the application of the GDPR in the context of marketing will be discussed both from the consumers' and marketers' perspectives through the effects of the GDPR on consumer behavior, and the changes it brings to digital marketing will be examined.

3.1 The Effects of the GDPR on Consumer Behavior

As it is discussed in Chapter 1, in line with the advances in technology, consumers are getting more and more privacy concerned and distrustful towards online transactions. The GDPR fully encourages this situation because it forces businesses to be law-abiding, transparent and reliable to gain consumers' trust and convince them to choose their products/services which is the ultimate goal of the GDPR.

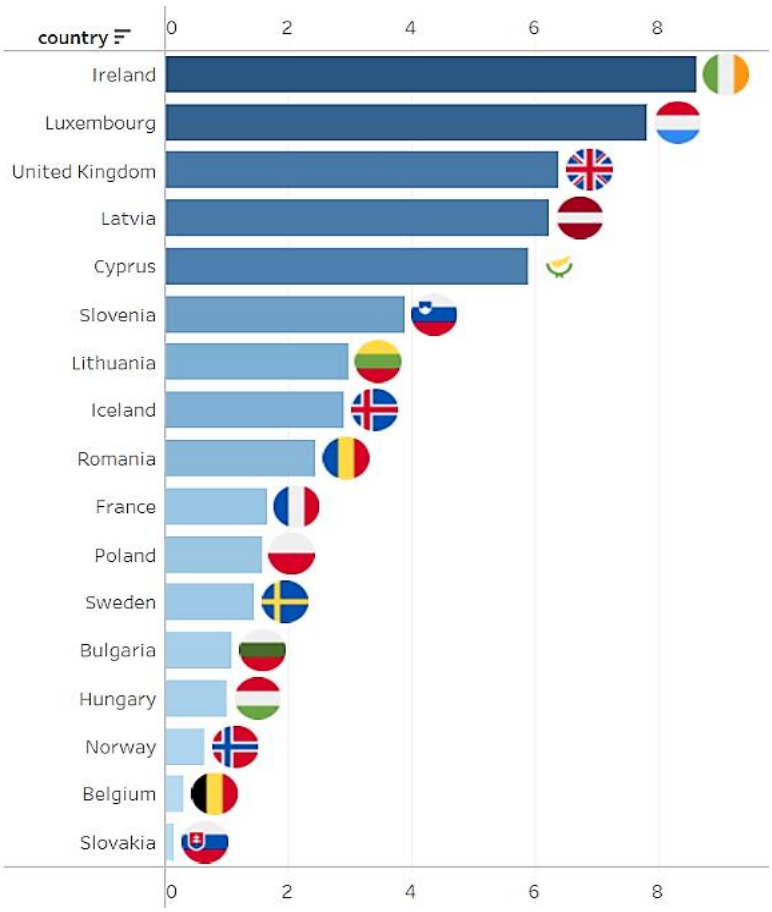
The awareness campaigns GDPR promotes have proven themselves quite effective as consumers have been acting more cautious about sharing their personal data with organisations since the GDPR came into effect. According to Deloitte's *A New Era For Privacy: GDPR Six Months On (2018)* report, globally on average 58 percent of the respondents agreed that they became more cautious about their data (p. 6) and they have a very high level of awareness as 78 percent of the participants on average are aware of the key rights the GDPR provides to them (p. 13). The right to know and the right to erasure are the highest voted rights which consumers planned to take advantage of (I-scoop, 2018).

Looking at the consumers' expectations from companies, the top three include; updated data protection policies, anonymized consumer data collection and stopped data selling to other companies (Dick, 2019). Even though most consumers expressed that the GDPR has not improved their interactions with companies at least for the past year, over 63 percent of consumers in the EU still believe that the GDPR has a positive impact on consumer data privacy (Dick, 2019). In this sense, it is seen that Europe's GDPR awareness campaigns and strong regulation managed to arouse interest among the public.

This strong interest also shows itself not only in the form of knowledge but also in the form of execution; the first month of GDPR saw a sharp increase in the number of complaints to regulators across Europe and it is likely to continue (Hern, 2018). According to The European Data Protection Board's infographics, since May 2019, the total number of queries

and complaints received is 144.376 and the top three types of complaints are about telemarketing, promotional emails and video surveillance (European Commission, 2019b). According to the results of the market research conducted by IntoTheMinds Marketing Agency, the rate of complaints concerning personal data in 25 European countries is presented in Figure 5, giving a sense how these total 144.376 complaints are distributed among the EU countries.

Figure 5: Number of complaints sent to national DPA per 10.000 inhabitants



Source: Schwab (2019).

The increasing numbers of complaints mean that consumers do not trust organisations' sincerity to improve their systems to comply with the GDPR. According to a Deloitte survey that was conducted in 2018, less than half of the respondents (44 percent) believe that organisations care more about their privacy now that GDPR is in force (p.6). As a result, organisations who are transparent about how they use their customers' personal data are rewarded with much-wanted and needed trust. The survey results indicate that 67 percent of respondents take into account the quality and transparency of privacy policies when they decide the level of trust to place in an organisation to handle their data correctly (p.18). The other factor affecting consumers' level of trust is an organisation's general reputation as an ethical organisation. 69 percent of respondents agreed that if an organisation launched as ethical, it will affect their opinion positively (p. 20).

The fact that consumers have more concerns about their privacy and are willing to use their rights granted by the GDPR does not mean that they do not understand the importance of data sharing as it is discussed previously at Chapter 1. Global Chief Data Ethics Officer at Acxiom, Sheila Colclasure states “The clear trend is towards greater acceptance of data exchange as part and parcel of everyday life. This is positive news for marketers who believe in data ethics and in greater transparency, access and control for the consumer as this will be key to achieving the win-win businesses and importantly, consumers really want” (FEDMA, 2018). The quotation indicates that the businesses who play according to data ethics not only manage to secure their customers’ loyalty but also attract other consumers through their good reputation which is the ultimate goal of businesses and aim of the GDPR.

3.2 How the GDPR Changes Digital Marketing

It has been more than two years since the GDPR entered into force and organisations of all sizes found themselves affected by it to some extent, especially marketing departments. In the first month of the GDPR, email inboxes flooded with messages requesting users to renew their consent to be contacted. They have been frantically attempting to contact their customers in an effort to update their consent agreements, with the fear that their marketing base could be drastically reduced by the GDPR (Lamb Brooks, 2018).

Analysts at Forrester say many companies have reported a decrease of between 25 percent and 40 percent of their addressable market for emails and other forms of contact (Palmer, 2019). For marketers, this situation implied the necessity of updating their privacy policies, being as transparent as possible about how their data is being used and maintained and finding innovative new ways to connect with customers and gather their consent to use their data in order to continue “marketing relationship” with them.

This means delivering personalized content and tailored products/ service recommendations to customers to assure them that they are reaping the benefits of this new regulation. Offering them the chance to update their marketing preferences, and focusing on the benefits they will gain by sharing such information enable them to see relevant offerings being delivered to them and as a result, they are more likely to stay engaged with the brand (Weiss, 2018). In this sense, it is believed that with the right attitude and process, the era of consent and the GDPR lead to stronger connections between organizations and consumers.

3.2.1 Challenges

The top components of GDPR that make life more difficult and increase operational uncertainty for digital marketers include the ban on automated decision-making in the absence of the customers’ meaningful consent; the new rights granted to individuals to access, rectify, and erase data about them held by businesses; the prohibition on processing of data pertaining to special protected categories as identified in the regulations; and the

stipulation that data collectors must demonstrate compliance with the regulations as a general matter (Ghosh, 2018). These components have been making the marketers life harder as they require operational changes.

The fact that there are many issues needed to be taken into consideration and the punishment for failing to comply with the GDPR is extremely costly, businesses have been trying to find their way in order not to fall victim to the law. The problem is that the majority do not know how to address the GDPR challenge. Although it has been two years with the GDPR in force, 41 percent of marketers admitted to not fully understanding neither the law nor the best practice around the use of consumers' personal data (Healey, 2020). Some businesses decided to reduce their exposure to potential GDPR punishments altogether by temporarily suspending services or cutting back the products which they offer to the European citizens (Lamb Brooks, 2018).

On the other hand, some businesses believed that consumers will give consent if their site access is reduced as a consequence of not consenting to advertising, which is a similar approach to what publishers have done to deter ad blockers. However, this option is bound to fail as the GDPR bans publishers from reducing site access if the users do not consent (Davies, 2017). Suspending services or denying access are short-lived solutions and cause loss of thousands of customers which is as harmful as the fines for any business.

The other major issue is loss of important records. Apparently, the customers are eager to use their right to erasure granted by the GDPR as a number of businesses have been forced to delete large swathes of important customer data both before and after the GDPR deadline, in order to ensure that they did not fall foul of the regulations (Lamb Brooks, 2018). Most of the businesses serving European consumers feel the bite of the GDPR, especially the top ones. The social network site, Facebook blamed the GDPR for a decline of about a million monthly users during the second quarter of the year, as well as a decrease in advertising revenue growth within Europe (Palmer, 2019). In this sense, not only gaining new customers but also holding the old customers are quite challenging under the watch of the GDPR.

3.2.2 Opportunities

Although the challenges are no joke, actually, GDPR compliance is very much aligned with digital marketing goals. The GDPR helps digital marketers to get rid of the noisy irrelevant data and keep minimum data which is valuable and correct in order for processing to take place (Gola, 2019). Focusing on the customer verified data to better target individuals will create higher quality authentic data. Better data will create better ad experiences.

By requiring users to opt in in order to be contacted for offers and services explicitly, there is greater possibility that the people who end up opting in will have higher intent leads. So, while lead volume at the top line may reduce, that would likely come alongside increased

conversion further down the funnel all the way to revenue (Aspillera, 2018). This situation will make digital marketing efforts not only more transparent, but also more efficient.

The need of customers' explicit consent to use their data helps marketers to provide their customers with a range of options so that they can find out what they are interested in. Through consent, marketers can gain insight into each individual's interests to provide them with information that they want to receive. It also helps marketers to further segment their customers and focus into communication based on their specific interests, rather than sending a "one size fits all" email campaign (MacDonald, 2019).

In view of foregoing, under the GDPR, content marketing is expected to rule digital marketing in Europe as its power lies in displaying ads not based on consumers' profiles, but based on the content that the users online are looking at in real time, such as a news articles, websites, news feeds and mobile app screens. As a result, the underlying routing of digital advertisements will likely to become increasingly quick, automated and seamless (Ghosh, 2018).

As well as avoiding bad public relations, the GDPR gives businesses the opportunity to show customers that they care about them as a person, reduce consumer mistrust and that trust will go a long way in gaining customer loyalty and reduce any disconnect with targeted audiences (Bryan, 2019). Forcing the digital marketers to develop compliant ad market infrastructures, the GDPR provides a good opportunity for marketers to improve their services as it leads to healthier customer databases with a clearer understanding of customers and a better insight into their behaviors.

4 RESEARCH ON THE EFFECTS OF THE GDPR ON DIGITAL MARKETING PRACTICE IN SLOVENIA

In this section, the research framework and methods used will be discussed in order to give the readers the insights of the data collection process and allow them to evaluate the reliability and the validity of this research.

Due to the fact that the GDPR is one of the newest and the most important regulations of 21st century regarding consumer privacy, the research about the GDPR is still limited especially regarding Slovenia, yet the topic is worth further exploring. Therefore, the biggest reason for this thesis to be written is the uncharted nature of the regulation as well as the pure curiosity about how small and medium enterprises are coping with the regulation. As a result, the purpose of this thesis is to see how digital marketing is reshaping under the GDPR, and how small and medium enterprises are fitting into this new digital environment in Slovenia. For this purpose, there are three main goals of this research that are the following:

- to determine in which ways digital marketing practice is changing as a consequence of GDPR in Slovenia
- to examine whether there are significant differences between various industries in terms of applying GDPR into their marketing practices
- to identify possible opportunities and threats for digital marketing under GDPR

In order to achieve these goals, this research tried to brings answers to the following research questions to see the Slovenia's way of adapting the new digital era under the GDPR:

- How did companies' digital marketing activities get affected due to GDPR?
- What kind of changes did the companies employ in their digital marketing practices because of GDPR?
- What are the threats and opportunities of GDPR in the context of their marketing activities?

4.1 Research Design

Even before coming into force, GDPR started to change the digital world. Businesses which fear the heavy fines and reputational damage already started in 2016 to look for the best solutions to comply with GDPR while retaining their customer databases. Due to the fact that the regulation is still new, the information on how companies are dealing with it and what kind of new digital marketing practices they created are still not known. This master thesis tried to address this problem.

In this thesis, an exploratory research was conducted to gain better insights about the topic. The sources of data include both secondary and primary data. The required data were collected by means of desk research and loosely structured in-depth interviews. As it is a relatively new subject, the literature is still quite limited, especially regarding Slovenia. Therefore, the in-depth interviews are the core of this thesis.

For this thesis, the biggest advantage of this qualitative research method was establishing rapport with the participants. Due to the fact that the topic is very sensitive, making the participants feel more comfortable was important to generate more insightful and valuable responses. In addition, as the interviews were face-to-face, there was opportunity to observe the attitudes of the interviewees towards the topic, ask follow up questions and gather additional information related to the subject. On the other hand, there was one drawback with the method; as the interviews were loosely structured, it was challenging to compile the notes and put them in the right manner in order to ensure integrity.

4.2 Methodology

As the purpose of this thesis was to see how digital marketing is changing under GDPR and how companies are adapting to this new digital environment in Slovenia, the focus of the qualitative research is on companies' point of views, not customers'. Because of the fact that in general opinion, small and medium enterprises are believed to be affected the most by the GDPR, for this thesis, seven small and medium enterprises from Slovenia were chosen in order to gather insights to decide whether this notion reflects the truth or not, as well as to gain deeper understanding of the subject.

The main criteria for choosing the companies were company size, industry and their relevance of the GDPR. As the focus of the research is on small and medium businesses, the size was the first criterion; all seven companies that were interviewed are small and medium enterprises. Company size was followed by industry, in order to gain insights from different industries and compare them with each other, six different industries which are digital marketing, e-commerce, simulation, manufacturing, media and food. Because of the fact that the digital marketing industry is the main focus, two companies from this industry were chosen so that different perspectives could reveal more information. The main reason for choosing these six industries was to see if there was a connection between these seemingly very different industries in terms of their GDPR compliance process and its effects on their digital marketing practices as well as their convenience to be reached.

The interviews were conducted with the key informants/employees from marketing departments who were also present in the GDPR compliance process with only two exceptions (but these two interviewees were active in the matter). Due to the Coronavirus outbreak, all the interviews were conducted via Zoom and took between forty five minutes to one hour. The recordings were used for a better analysis of the discussion with the promise of the identity of the interviewees and the names of the companies will not be mentioned in the thesis, and the trascripts of the recordings will not be published[1]. The interviews were loosely structured and the interview questions, which can be found in Appendix 2, were designed in four parts.

The first part (questions 1-5) is about the GDPR compliance process; the interviewees were asked about how their industry and company have been affected, how much time it took for them to be fully compliant, the measures/actions they took and the challenges they faced. The second part (questions 6-7) is about company-customers relationships to see if Slovenian consumers are eager to use their rights, and if so which rights. With the relation to the second part, the third part (questions 8-10) focuses on the consequences of the GDPR on company operations; how companies changed their digital marketing practices/communications, sales, pricing and product/service development. Last but not least, the fourth part (questions 11-12) deals with the future expectations of companies on

[1] The transcripts of the recordings are held by the author.

the GDPR and ZVOP-2 to observe their attitude towards the perceived future opportunities and challenges with regards to digital marketing.

4.3 Demographic Profile of Interviewees

The demographic profiles of the interviewees are demonstrated in Table 3 below which was formed according to the dates of the interviews. There are six interviewees from six different but somehow overlapping industries. The minimum year of experience the six interviewees had in their current companies was two, so they were involved in the GDPR compliance process, while one interviewee was not present in the first step of the GDPR compliance. While choosing the interviewees, the main criterion was them being active in the matters related with the GDPR and marketing practices of the company.

Out of seven companies interviewed, six of them have Slovenian origin and one from Ireland, and all the chosen companies are business-to-business (B2B). The number of employees varies from eight minimum to one hundred forty maximum. Looking at the yearly revenues, it gives a range between 400.000 and 25M €. All the interviews were conducted between March-June 2020, so the information they provided are up-to-date.

Table 4: Overview of the interviewees

	Industry	Origin of the company	Number of employee	Yearly revenue	Position of the interviewee	Year of experience	Date of the interview
Interviewee 1	Digital marketing	Slovenia	8	400.000 €	Digital strategist	2 in company/ 15 in industry	13.03.2020
Interviewee 2	E-commerce	Slovenia	15	2M €	Team leader	5	20.04.2020
Interviewee 3	Simulation	Ireland	14	500.000 -1M €	Business developer	2 in company/ 4 in industry	04.05.2020
Interviewee 4	Digital marketing	Slovenia	16	850.000 €	Project manager	5	10.05.2020
Interviewee 5	Manufacturing	Slovenia	140	100M €	Head of digital marketing	8	23.05.2020
Interviewee 6	Media	Slovenia	25	18M €	Digital marketing planner	3	28.05.2020
Interviewee 7	Food	Slovenia	90	1.5M €	Digital specialist	1,5 in company/ 4,5 in marketing industry	09.06.2020

Source: Own work. N=7.

4.4 Results and Analysis

In this section, the findings of the qualitative research findings are shared and then analysed with the help of the information, which was provided by the secondary data. The aim of the section is to observe in what ways Slovenia's digital marketing practices went through the same experience that the experts warned before the GDPR and in what ways, it differed from the expectations and why.

4.4.1 Findings of the Qualitative Research

Based on the findings of the qualitative research, it was found out that no matter which industry that the interviewees represented, the experience they went through was actually quite similar. All interviewees admitted that nobody understood the GDPR so they did not know what to do or how to do. They all stated that the regulation was highly unclear and complex; therefore, even the lawyers they are working with had difficulties to prepare the legal documents and inform the marketing department about the necessary steps they had to take. Interviewee 6 stated "we have a legal person in the company who also acts as a Data Protection Officer (DPO), but I am not sure if she understands the regulation completely" and the other interviewees except Interviewee 2 gave similar statements.

Unable to comprehend the GDPR, interviewees stated that they kept delaying their preparation until March 2018, two months before the enforcement of the regulation, hoping to get a clear picture about what to do. However, waiting did not provide any solution as Interviewee 1 stated "the biggest challenge of the GDPR is unclarity because the explanations are too general. As there is no one right way to do things, lawyers, experts and companies have different opinions, making things more complicated." Therefore, the legal and digital marketing departments had to take the initiative and hope to do everything according to the regulation.

According to the interview findings, the preparation process consisted of three steps which required one and half months to two months' time to be completed. As the regulation is legally binding, the first step was to assign a DPO. None of the interviewed companies hired an external lawyer/DPO, they rather assigned their lawyer (in case of Interviewees 5, 6 and 7, it was one of their lawyers) for the position, so it was the easiest and fastest step. Gradually, the second step was a bit harder as it involved educating the employees who work with consumer data with the help of DPO. Interviewee 2 stated "the biggest challenge was educating the staff. Together with the lawyer, we had to prepare the proper documentation on data protection as well as discussing the things we had to change, correct or update in our business operation." Other interviewees expressed that they also followed similar procedures although they did not agree that educating the employees was the biggest challenge.

For the six interviewees (except Interviewee 2), the most challenging part of the process was the last step which included updating Cookie and Privacy policies by explaining what kind

of personal data is collected, why it is collected, with whom it is shared, and how it is processed/used with a simple and understandable language; adding visible opt-in and opt-out options; preparing the GDPR request forms; and sending emails to the all customers to inform them about the GDPR and seek their consent in order to keep them in the database as well as continue to use their personal data for providing better services and marketing. Interviewee 4 proclaimed that the biggest problem of the process was cookie policies as she stated "digital marketing departments panicked a lot about how to collect users' data on websites with Google Analytics as users must now accept cookies, to start giving their data to analytics. We had to implement cookie notification on every website and then hope that users accept the terms."

Unfortunately, their fears proved themselves true. The emails the companies sent accumulated in customers' inboxes and the surfeit triggered the customers who were already eager to use their rights. Interviewee 6 affirmed this situation by declaring "one month before the GDPR, we had to face the grim reality: the level of tolerance dropped significantly and most of the clients preferred to opt-out from the databases." Other than Interviewee 2 and 3, the rest of them agreed that this intolerance caused the loss of significant amounts of data as only five to ten percent of the customers decided to choose opt-in. Panicking about the huge fines, companies gave the fastest and effective reaction they could think of: deleting the unconsented data. Interviewee 6 denoted "in a blink of an eye, everything changed. We had to renew our marketing list from zero for half a year," which showed the seriousness of the situation.

In this situation, it is not surprising that not all of the businesses are doing the things correctly. As large enterprises have more at stake because of the huge fines and market popularity, they are observed to be more careful with the GDPR. The interviewees agreed that the most law abiding industries are; banking, telecommunication and insurance. On the other hand, more than half of the small and medium enterprises in Slovenia still cannot keep up with the regulation. Interviewee 1 denoted "small and medium size business still are unaware about what needs to be done. They need guidance almost about everything from cookie management to privacy policies, but they do not have money to pay for these services. So, most of them are still not compliant to the GDPR."

Looking from the industry perspective, it is seen that the businesses which work only with data are quite happy with the regulation. Interviewee 4 explained it as "the GDPR works in reverse for us; it is us who want data privacy so we do not deal with the GDPR but our customers. So the regulation actually helps us." Although not all B2B companies are as lucky as the data industry as they also face difficulties with the regulation, they still feel fortunate as they already had a very strong customer loyalty so they did not experience any big change in customer expectations or received any GDPR related complaints. Compared to B2B, the interviewees stated that B2C is less fortunate because B2C is mainly dependent on email marketing and now the customers are keen to use their rights granted by the GDPR.

Related with the previous statement, when the interviewees are asked about the biggest setback of the GDPR, they shared the same opinion which was email marketing. According to the statements, before the GDPR, it was very easy to collect emails from all the channels and use them for marketing purposes without any consent. However, the GDPR put a period to this practice with the requirement of active consent. Interviewee 5 stated "we sent a consent email to 25.000 but only received 150 confirmations. So we had to delete the remaining. Also now Gmail has a new feature which sends you a notification asking if you want to opt-out in case you did not open the emails from the same company for a while." On this issue, the interviewees agreed that it is very difficult to allure consumers by using email marketing.

The dethronement of email marketing dragged down the cherished lookalike targeting and omnichannel marketing. Moreover, the updated cookie policies striked a major blow to Google Analytics. As a result, marketers had to find new ways to keep the existing customers, attract the potential customers and convince both to share their data. According to the interviewee statements, the most popular marketing approach after the GDPR is give-and-take card. Interviewee 7 stated that they are creating online prize games, creating additional content for subscribers as well as organizing offline activities while Interviewee 6 stated that they employed the method of implementing online events to encourage the data share. Interviewee 5 summarized the give-and-take method they are using as "we send six mails monthly with an 80/20 marketing campaign which is 80 percent is online help, promotional stuff or solution to their problems while 20 percent is about sales. Customers believe exchange is beneficial so they are willing to share their data."

Due to the fact that the mass advertising left its place to the targeting, the empty throne's new owner is Lead Generation marketing which targets consumers based on their behaviour that is shown in real time when they are looking at a content. In this sense, the data is not based on demographics but behaviour. But how to track the behaviour of whom visits the websites? Interviewee 2 explained the steps they took as "we use special cookies and beacons to display tailored advertising while ensuring data security by uploading SSL certificates and reCAPTCHA and integrating ERP systems to online commerce." As it is seen, it is not impossible to find solutions to track behaviour; however, these solutions require both effort and money and unfortunately bring fewer results. Interviewee 4 stated "after the GDPR, targeting as well as reaching customers demand more attention, strategic thinking, spending and time to implement to achieve the same results before the GDPR."

When the complexity and unclarity of the regulation combined with the inverse proportion between the money and effort used and the results and sales, it is only natural for businesses, especially their marketing departments to feel anxious for the time being. Although it has been two years since the GDPR came into effect, marketers argue that it is still too early for seeing the positive effects of the regulation. Still, marketers are optimistic about the future results as Interviewee 7 stated "the GDPR takes time and effort, but in long term, it is sure to help us to get quality leads which will increase sales and customer loyalty."

One way or another, the GDPR is already here and keeps changing the marketing world. So, there remains only one obstacle which is ZVOP-2. Interviewees hope that ZVOP-2 will be very much aligned with the GDPR so that it will not turn out to be a new challenge. After the GDPR experience, interviewees agreed that the Information Commissioner should provide clear guidance so the compliance will be easier and smooth, and also be ready to help the businesses in case they need it.

4.4.2 Analysis of the Findings

In this thesis, there were three research questions, which directed the research. Below, these three questions will be answered according to the findings of the exploratory research. It is important to keep in mind that the research is based on Slovenia so it is only indicative for Slovenia; and therefore, it might not reflect the general approach of the EU towards the issue in interest.

- **How did companies' marketing activities get affected due to GDPR?**

According to the findings of the qualitative research, no matter in which industry a company is, the GDPR experience is quite similar to each others'. The GDPR affected the marketing activities in a negative way at the very beginning because of the lost customer contacts. All interviewees admitted that they did not expect customers to be that much willing to use their opt-out right, but even before the GDPR came into effect, marketers lost around 90 percent of their marketing lists. Recreating these lists took half a year and marketers noticed that now it is more difficult to get customers to share their data with businesses. Marketers now have to come with creative as well as effective campaigns to convince the customers that the exchange is beneficial. In this sense, the effort and the money dedicated to marketing increased in order to achieve the same results before the GDPR. However, the participants in this research believe that this situation will change in the long term.

- **What kind of changes did the companies employ in their marketing practices because of GDPR?**

The GDPR started a new era in the marketing industry. According to the findings, the long existing marketing pillars; email marketing, mass advertising and lookalike targeting are not enough anymore, so lead generation marketing has been rising in popularity. This situation changed the process of buying as the roles of the marketers and customers are reversed. Instead of finding customers, now marketers are focusing on being found in the crowd. For this reason, the marketing campaigns are using both online and offline means of communication such as creating additional content for subscribers, providing solutions to their problems, online events and online/offline prize games. Through these channels, marketers are learning to gather insights about the customer behaviours rather than demographics so that they can build continuous relationships with the customers.

- **What are the threats and opportunities of GDPR in the context of their marketing activities?**

The components of the GDPR, including ban on automated decision-making in the absence of the customers' meaningful consent; the new rights granted to individuals to access, rectify, and erase their personal data have been making the marketers' life harder as they require operational changes. However, the interviewees believe that the majority of the marketers in Slovenia still do not fully understand the law so cannot decide how to do best these operational changes. Still, as the regulation is very ferocious, there is no excuse in case of failing to comply with it and it is extremely costly. Therefore, the threat of paying a fine is always lurking around the corner. In addition to these threats, the other major issue is loss of data. As the customers are eager to use their right to erasure, businesses cannot do anything but delete important customer data. In this sense, not only gaining new customers but also holding the old customers are quite problematic under the radar of the GDPR.

On the other hand, the GDPR helps digital marketers to get quality leads by requiring users to opt in in order to be contacted for offers and services explicitly. Now, there is a greater possibility that the people who choose to opt in will be the ones who are really interested in the services/products. Therefore, although the number of contacts may reduce, the sales are likely to increase. Also, through consent, marketers can gain insight into customers' interests and provide them with information that they want to receive, keeping the marketing communication active. Furthermore, the GDPR gives businesses the opportunity to show customers that they care about them as individuals, gaining customer loyalty.

5 DISCUSSION

It is very important to discuss the findings of the qualitative research in a broader context. Understanding how the GDPR reshaped the marketing practices in Slovenia is crucial for better business operations and providing flawless customer experience. The main proposition of this thesis for the companies is that the GDPR should not be underestimated as the better the companies understand and comply with it, the higher the flexibility will be for the future changes happening in this field.

5.1 Practical Implications

After analysing the qualitative research findings, it was seen that there are several good practices that the businesses can employ in order to improve their business operations as well as their relationship with their existing and potential customers.

Based on the statements of the interviewees and the statistical data, most of the marketers and lawyers still do not know well about the GDPR. Although right now Slovenian businesses have not been faced either with difficult consumer requests or with any lawsuits (ZVOP-2 is not in enforcement yet), it does not mean that this situation will last forever. Therefore, it is optimal for businesses to educate their employees as soon as possible. There are online courses, webinars as well as experts who are teaching about the GDPR which businesses can easily access. Ensuring that legal and marketing departments are aligned with the GDPR, businesses will eliminate the risk of paying fines and increase the operational efficiency as they will not waste time by checking the regulation to see whether the decision is in the scope of the GDPR.

According to the insights gathered from the interviewees, it is seen that another important problem is Google Analytics. Apparently, Slovenian marketing teams are still heavily dependent on analytics tools provided by Google, which are easy to use and low-cost, and reluctant to leave their comfort-zone. However, it is not possible to completely rely on Google anymore as it is the era of consent. With the enforcement of the GDPR, classical business-consumer roles do not apply anymore. The roles are reversed; now consumers find businesses rather than being found by businesses. In order to stand out in the mass, the responsibility falls on the shoulders of the marketers.

Now the marketers should use all the channels they can think of to attract the customers. Now, offline channels are as important as online channels because marketers are trying to be heard in the crowd of noises. As different industries have different charms, these activities differ from industry to industry. No matter if it is offline organizations, prize games or sponsorships, businesses must combine these activities with their digital marketing practices in order to increase their visibility and lure customers.

However, is luring enough? Of course not. Not only luring but also gaining individuals as customers is not enough. Marketers only can relax when they convince customers to share their data in the short run, and gain customer loyalty in the long run. However, how to do it? Especially when the collection of data is mainly dependent on consent, which can be taken back any moment. In order to prevent customers from leaving, businesses should take two steps; providing online security to gain customers' trust, and making customers satisfied with the product and services they provide for them.

As it is discussed in Chapter 1, for many consumers, trust is the key point which they pay attention to when they are involved in any online transaction. Because of the fact that the only element of trust that can be checked before an online transition is website security, businesses must obtain security certificates, especially SSL certificates as Google holds more than half of the market share. Furthermore, after the personal data is collected, businesses should ensure that it is stored in a secure manner to protect data against unauthorised access, processing, disclosure, alteration or accidental loss. Once the customers see that their data and privacy are safe in the hands of a business, they will continue their

relationship with that business and act as a brand advocate, helping the business gaining new customers.

The second part of keeping customers concerns marketing departments as the answer lies in content marketing. Regardless of the industry, targeting customers based on their interests seems like the most efficient marketing method. It is already discussed, customers acknowledged that there is no free lunch, so they have to give something if they want to get something. As more than half of the consumers are classified as Data pragmatists (Figure 2), it is marketers' duty to persuade customers that exchange is beneficial for both parties. When quality content and personalized advertising meet with reassurance of transparency and respect towards customer privacy, loyalty will most likely be the result.

5.2 Limitations and Future Research

In order to interpret the findings more objectively, in this session several crucial limitations will be presented. It is important for the readers to bear in mind these drawbacks while reading the paper so that the inference will be more on the point.

The most obvious limitation of the research is the research method. The interviews that were conducted carry a certain level of subjectivity as the interviewees are naturally biased. As a result, it is highly possible that during the interviews, consciously or unconsciously they kept some important information back to preserve the company image. Also, the fact that only one respondent was chosen from each company, adds more to the limitation of the information gathered.

Another drawback is the research scope. As only small and medium enterprises which are located in Slovenia are the focus of the research, the findings gathered should not be used to make generalization neither about the industries nor the other European countries. Furthermore, the results might have been varied if another company from the same industry was chosen.

Last but not least, the year boundary needs to be taken into consideration as the GDPR came into force in 2018. Therefore, the data is quite limited because most of the companies are still in the process of implementing and adjusting the GDPR into their business. Moreover, as the GDPR is still a new concept, the companies are still lacking the necessary information about how to comply with the regulation fully. This transition process; however, seems to last a while because of COVID-19 pandemic outbreak as the companies have to channel their efforts to deal with the outcome of the global crisis.

As the current research on the GDPR is highly limited, this field has a great potential and capacity for future research. The further development should put more focus on analyzing the real life case studies of companies which provide good practice. Additionally, a periodical study should follow how the GDPR reshape digital marketing among different

industries, as digital marketing is a fast-changing concept. Future research should focus on providing a wider perspective. This can be done by expanding the number of companies included in the research to provide more accurate analysis and comparison of industries. Not only comparing the industries within Slovenia but also comparing the same industries to the other EU members' should be another interest for the future researchers as the GDPR is directly applicable for all EU members.

CONCLUSION

The GDPR is the latest and one of the most formidable privacy regulations in EU law on the protection of natural persons regarding the processing of personal data which came into effect in May, 2018. Regardless of the territory, all the companies are subject to the GDPR if they are tracking European user behaviour for marketing and personalization, collecting personally identifiable information for digital marketing purposes and/or testing strategies to resurrect churned users.

As the GDPR is relatively a new regulation, the main purpose of this research was to see how digital marketing is reshaping under the GDPR, and how small and medium enterprises are fitting into this new digital environment in Slovenia in comparison to each other. In order to pursue this goal, a qualitative research was conducted and combined with the desk research. The gathered information helped to gain more in-depth understanding of the subject.

The research showed that data subjects in Slovenia are very knowledgeable about the GDPR and determined to defend their rights in case they notice something amiss. However, many of the small and medium businesses noted still not be fully compliant with the regulation due to the complexity of the bill as well as the time and money required. As the regulation is legally-binding, Slovenian small and medium size companies need to fasten their compliance process before ZVOP-2 came into force, otherwise the keen consumers are very likely to take legal actions, as Slovenia is already the sixth in the list of complaints sent to national DPA (Figure 5).

Being a GDPR compliance is of course not enough to coax consumers as the regulation is not only about law but also has a marketing aspect. According to the key findings of the in-depth interviews, now marketing departments have to shoulder more responsibilities as lookalike targeting and email marketing are tied up by active consent. The new era is marked with the phrase ‘content is the king’, so the lead generation marketing has become the new hit. Marketers are expected to create quality content to lure consumers, but this content should be based on the consumer behaviour not demographics. Indeed, this approach to marketing requires more time, effort and money as it involves online and offline marketing at the same time. However, a big challenge brings a big reward. As the GDPR's consent

requirement provides marketers with quality leads which have more potential to turn out to be sales.

Therefore, it can be concluded that businesses should be very careful with the GDPR as now the customers are aware of their rights and willing to use them. One wrong step can cause a snowball effect, so businesses should put more effort to their relationships with the customers by respecting their rights; ensuring safety for their data and privacy; being transparent; and pampering them with the quality content and tailor-made advertising.

REFERENCE LIST

1. Akshita. (2018, May 10). *What is GDPR? User Rights and Business Guidelines*: Opensense Labs. Retrieved June 8, 2020, from https://opensenselabs.com/blog/articles/gdpr-user-rights-business-guidelines.
2. Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review*, *2*(3), 287-289. doi:10.21552/edpl/2016/3/4.
3. Aspillera, M. (2018). *What Every Digital Marketer Needs to Know About GDPR.* Retrieved November 24, 2019, from https://www.brightedge.com/blog/the GDPR-digital-marketing/.
4. Bauman, A., & Bachmann, R. (2017). Online Consumer Trust: Trends in Research. *Journal of Technology Management and Innovation*, *12*(2), 68-79. doi:10.4067/s0718-27242017000200008.
5. Beldad, A., Jong, M. D., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, *26*(5), 857-869. doi:10.1016/j.chb.2010.03.013.
6. Benson, V., Saridakis, G., Tennakoon, H., & Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal of Human-Computer Studies*, *80*, 36-44. doi:10.1016/j.ijhcs.2015.03.004.
7. Biagini, L. (2018, July 20). *Don't Confuse the GDPR Compliance with Security*. Retrieved December 2, 2019, from https://www.forbes.com/sites/ciocentral/2018/07/20/dont-confuse-the GDPR-compliance-with-security/#6e0331cb613d.
8. Bleau, H. (2017, May 15). *New Survey: Consumers Increase Security Expectations in Wake of Password Breaches.* Retrieved September 11, 2019, from https://www.rsa.com/en-us/blog/2017-05/2017-consumer-cybersecurity-confidence-index.
9. Bryan, J. (2018, May 10). *GDPR - 5 Key Benefits for your Marketing Strategy.* Retrieved November 24, 2019, from https://www.corkchamber.ie/gdpr-5-key-benefits-for-your-marketing-strategy/.

10. *California Consumer Privacy Act - Full Text.* (2020). Retrieved June 19, 2020, from https://ccpa-info.com/california-consumer-privacy-act-full-text/.
11. Council of Europe. (2020, January 28). *Data Protection Day*. Retrieved April 6, 2020, from https://www.coe.int/en/web/data-protection/data-protection-day.
12. Data Privacy Manager. (2020a, January 8). *CCPA vs. GDPR - differences and similarities*. Retrieved June 19, 2020, from https://dataprivacymanager.net/ccpa-vs-gdpr/.
13. Data Privacy Manager. (2020b, August 18). *5 biggest GDPR fines so far [2020]*. Retrieved August 22, 2020, from https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/.
14. Davies, J. (2017, November 2). *European consumers' attitudes toward data privacy in 5 charts.* Retrieved September 23, 2019, from https://digiday.com/media/european-consumers-attitudes-toward-data-privacy-5-charts/.
15. Deloitte. (2018). *A new era for privacy - General Data Protection Regulation ("GDPR") six months on.* Retrieved October 13, 2019, from https://www2.deloitte.com/uk/en/pages/risk/articles/gdpr-six-months-on.html.
16. Dick, J. (2019, May 20). *The General Data Protection Regulation: One Year Later.* Retrieved October 13, 2019, from https://blog.hubspot.com/marketing/general-data-protection-regulation-consumer-attitudes.
17. European Commission. (2015, December 15). *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Retrieved November 26, 2019, from http://europa.eu/rapid/press-release_IP-15-6321_en.htm.
18. European Commission. (2019a, January). *MYTHBUSTING: General Data Protection Regulation.* Retrieved June 12, 2020, from https://ec.europa.eu/commission/sites/beta-political/files/100124_gdpr_factsheet_mythbusting.pdf.
19. European Commission. (2019b, May 25). *Infographic GDPR in numbers 2019.* Retrieved January 5, 2020, from https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.
20. Fedma. (2018, May 24). *New global study reveals consumers are happy to share their data*. Retrieved September 11, 2019, from https://www.fedma.org/2018/05/new-global-study-reveals-consumers-are-happy-to-share-their-data/.
21. Fish, T. (2009). *My digital footprint: A two sided digital business model where your privacy will be someone else's business*. London: Futuretext.
22. Fromholz, J. M. (2000). The European Union Data Privacy Directive. *Berkeley Technology Law Journal, 15*(1), 461-484.
23. Lamb Brooks. (2018, August 3). *The GDPR: How are Businesses Coping?* Retrieved November 26, 2019, from https://www.lambbrooks.com/the GDPR-how-are-businesses-coping/.
24. *General Data Protection Regulation (the GDPR) – Final text neatly arranged*. (2018). Retrieved October 3, 2019, from https://the GDPR-info.eu/.

25. Ghosh, D. (2018, May 21). *How the GDPR Will Transform Digital Marketing.* Retrieved November 24, 2019, from https://hbr.org/2018/05/how-the GDPR-will-transform-digital-marketing.
26. Gola, M. (2019, September 19). *GDPR has the power to transform the Digital Marketing*. Retrieved November 24, 2019, from https://www.curvearro.com/blog/gdpr-has-the-power-to-transform-the-digital-marketing/.
27. Healey, R. (2020). *GDPR 2 years on what challenges await in 2020*. Retrieved April 3, 2020, from https://relentlessdataprivacy.com/gdpr-2-years-on-what-challenges-await-in-2020/.
28. Hedencrona, S. (2018, May 29). *Data Privacy - How it is Changing and How Brands Can Measure Up.* Retrieved November 26, 2019, from https://blog.globalwebindex.com/marketing/data-privacy/.
29. Hern, A. (2018, June 26). *European regulators report sharp rise in complaints after the GDPR.* Retrieved January 23, 2020, from https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-sharp-rise-in-complaints-after-the GDPR.
30. Horvat, U. (2018, June 29). *Slovenia and the GDPR – what does the fact that Slovenia did not adopt a the GDPR implementing law mean for data protection in Slovenia?* Retrieved December 19, 2019, from https://www.jadek-pensa.si/en/slovenia-and-the GDPR-what-does-the-fact-that-slovenia-did-not-adopt-a-the GDPR-implementing-law-mean-for-data-protection-in-slovenia/.
31. Hospelhorn, S. (2020, June 17). *California Consumer Privacy Act (CCPA) vs. GDPR*. Retrieved June 19, 2020, from https://www.varonis.com/blog/ccpa-vs-gdpr/.
32. HR News. (2018, September 27). *4 Months on from the GDPR, How are Businesses Coping?* Retrieved November 26, 2019, from http://hrnews.co.uk/4-months-on-from-the GDPR-how-are-businesses-coping/
33. Informacijski Pooblaščenec. (2014). *Personal Data Protection Act of the Republic of Slovenia of 2004*. Retrieved December 19, 2019, from https://www.ip-rs.si.
34. Informacijski Pooblaščenec. (2020). *Search Opinions For GDPR*. Retrieved from August 14, 2020, https://www.ip-rs.si/vop/.
35. I-scoop. (2018, January 4). *The Million Euro Question: How consumers plan to exercise the GDPR rights*. Retrieved July 23, 2019, from https://www.i-scoop.eu/the GDPR/eu-consumer-the GDPR-rights-attitudes/.
36. Jerman, U. (2019, May 6). *Analysis of the Slovenian the GDPR Implementation Law in Light*. Retrieved December 19, 2019, from https://www.rppp.si/wp-content/uploads/2019/05/20190506_the GDPR-National-implementation.pdf.
37. Koch, R. (2019, July). *2020 developments for data protection and the GDPR.* Retrieved January 3, 2020, from https://gdpr.eu/gdpr-in-2020/?cn-reloaded=1.
38. Kolowich, L. (2017, November 16). *How & Why to Make Your Website More Secure*. Retrieved July 17, 2020, from https://moz.com/blog/how-to-make-your-website-more-secure.

39. Kumar, V., & Dange, U. (2012). A Study of Factors Affecting Online Buying Behavior: A Conceptual Model. *SSRN Electronic Journal*. doi:10.2139/ssrn.2285350.
40. Larose, C. J. (2019, December 18). *CCPA QOTD: What Are the Penalties for Non-Compliance with the CCPA?* Retrieved June 19, 2020, from https://www.natlawreview.com/article/ccpa-qotd-what-are-penalties-non-compliance-ccpa.
41. Liu, C., Marchewka, J. T., Lu, J., & Yu, C. (2004). Beyond concern: A privacy–trust–behavioral intention model of electronic commerce. *Information & Management, 42*(1), 127-142. doi:10.1016/j.im.2004.01.002.
42. MacDonald, S. (2019, June 15). *GDPR for Marketing: The Definitive Guide for 2019*. Retrieved November 24, 2019, from https://www.superoffice.com/blog/gdpr-marketing/.
43. Merc, A. (2018, March 9). *The Slovenian Personal Data Protection Act (ZVOP-2) proposal – overstepping the GDPR boundaries?* Retrieved December 19, 2019, from https://www.jadek-pensa.si/en/the-slovenian-personal-data-protection-act-zvop-2-proposal-overstepping-the-the GDPR-boundaries/.
44. Miklavčič, D. (2019, May 24). *Slovenia – The GDPR one year on*. Retrieved December 19, 2019, from https://theword.iuslaboris.com/hrlaw/viewContent.action?key=Ec8teaJ9Vaqds4LUYq9fc8xgHJMKLFEppVpbbVX+3OXcP3PYxlq7sZUjdbSm5FIeeqYUDMmQsgfdzoxprWhI6w==&nav=FRbANEucS95NMLRN47z+eeOgEFCt8EGQ0qFfoEM4UR4=&emailtofriendview=true&freeviewlink=true.
45. Ministrstvo za pravosodje. (2020). *Ministrstvo za pravosodje želi s pripravo Zakona o varstvu osebnih podatkov in Zakona o varstvu osebnih podatkov na področju obravnave kaznivih dejanj ohraniti visok standard na področju varstva osebnih podatkov*. Retrieved February 5, 2020, from https://www.gov.si/novice/2020-01-23-ministrstvo-za-pravosodje-zeli-s-pripravo-zakona-o-varstvu-osebnih-podatkov-in-zakona-o-varstvu-osebnih-podatkov-na-podrocju-obravnave-kaznivih-dejanj-ohraniti-visok-standard-na-podrocju-varstva-osebnih-podatkov/?fbclid=IwAR3uY-pqbyctWjr2bQn4FRWpfly9dhUnkcOc-Ai4LhvgO5O_rRgjYFRd2X4.
46. Moore, K. (2018, April 9). *6 Lawful bases for processing data under GDPR.* Retrieved October 14, 2019, from https://www.kgmoore.co.uk/6-lawful-bases-for-processing-data-under-gdpr/.
47. Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *57 UCLA L. REV. 1701*.
48. Palmer, D. (2019, May 17). *What is GDPR? Everything you need to know about the new general data protection regulations.* Retrieved October 13, 2019, from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.
49. Pellat, G., & Hoareau, E. (2019). How does the use of the GDPR affect consumer behavior during internet actions? *Proceedings of the 25th International Scientific Conference of PGV Network 2019*, 241-255. doi:10.2478/9788395720475-022.

50. Redman, T.C. and Waitman, R. M. (2020, January 28). *Do You Care About Privacy as Much as Your Customers Do?* Retrieved March 10, 2020, from https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do.
51. Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice, 17*(1), 30-35. doi:10.1057/dddmp.2015.40.
52. RSA. (2017, April). *2017 Consumer Cybersecurity Confidence Index*. Retrieved September 12, 2019, from https://www.rsa.com/content/dam/en/infographic/rsa-consumer-cyber-security.pdf.
53. Schwab, P. N. (2019, November 29). *European GDPR statistics: Evolution of the number of complaints per country*. Retrieved July 15, 2020, from https://www.intotheminds.com/blog/en/gdpr-statistics-europe/.
54. Smith, J. (2017, March 29). *The History of the General Data Protection Regulation*. Retrieved October 13, 2019, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
55. Smith, K. T. (2012). Longitudinal study of digital marketing strategies targeting Millennials. *Journal of Consumer marketing*, *29*(2), 86–92.
56. Sobers, R. (2020, May 18). *110 Must-Know Cybersecurity Statistics for 2020*: Varonis. Retrieved July 17, 2020, from https://www.varonis.com/blog/cybersecurity-statistics/.
57. STA. (2018a, April 7). *Slovenia Adopts the General Data Protection Regulation on Data Privacy*. Retrieved December 19, 2019, from https://www.total-slovenia-news.com/news/999-slovenia-adopts-the-general-data-protection-regulation-on-data-privacy.
58. STA. (2018b, May 4). *Some Challenges, Including the Election, for EU's New Data Protection Rules in Slovenia*. Retrieved December 19, 2019, from https://www.total-slovenia-news.com/news/1166-some-challenges-including-the-election-for-eu-s-new-data-protection-rules-in-slovenia.
59. Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of electronic commerce, 7*(3), 135-161. doi: 10.2307/27751068.
60. Svet Kapitala. (2019, May 20). *Kdaj bo sprejet zakon o varstvu osebnih podatkov in kaj nam to prinaša.* Retrieved December 19, 2019, from https://svetkapitala.delo.si/aktualno/kdaj-bo-sprejet-zakon-o-varstvu-osebnih-podatkov-in-kaj-nam-to-prinasa/.
61. Tamò-Larrieux, A. (2018). *Designing for privacy and its legal framework: Data protection by design and default for the internet of things.* Cham, Switzerland: Springer.
62. Tene, O., & Polonetsky, J. (2012). Privacy In The Age of Big Data: A Time For Big Decisions. *64 STAN. L. REV. ONLINE 63.*
63. Turow, J., Hoofnagle, C., Mulligan, D. K., Good, N., & Grossklags, J. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade. *I/S: A Journal of Law and Policy for the Information Society, 3*(3), 723-749.

64. Uzialko, A. (2020, February 4). *How Has the GDPR Affected Business?* Retrieved March 6, 2020, from https://www.businessnewsdaily.com/15510-gdpr-in-review-data-privacy.html.
65. Vrban, D. (2019, March 27). *Poraz ekip marketinga v etičnem izzivu GDPR*. Retrieved December 19, 2019, from https://kainoto.com/blog-digitalni-marketing/poraz-ekip-marketinga-v-eticnem-izzivu-gdpr.aspx.
66. Wangen, J. (2017, July 27). *Why's a CAPTCHA important?* Retrieved July 17, 2020, from https://www.back40design.com/blog/m.blog/83/why-s-a-captcha-important.
67. Weiss, E. (2018, May 25). *How to Convince Customers to Share Data After the GDPR*. Retrieved September 14, 2019, from https://hbr.org/2018/05/how-to-convince-customers-to-share-data-after-the GDPR.
68. Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.
69. Wolford, B. (2019, February 13). *What is the GDPR, the EU's new data protection law?* Retrieved October 13, 2019, from https://the GDPR.eu/what-is-the GDPR/.
70. Wu, K., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889-897. doi:10.1016/j.chb.2011.12.008.

APPENDICES

Appendix 1: Povzetek (Summary in Slovene language)

Splošna uredba o varstvu podatkov (v nadaljnjem besedilu: GDPR) je najnovejša in najstrožja zakonodaja Evropske unije (v nadaljnjem besedilu EU) o zasebnosti in varnosti, ki je bila sprejeta aprila 2016 in je začela veljati maja 2018. GDPR je uvedel stroga pravila glede uporabe osebnih podatkov evropskih oseb, na katere se nanašajo osebni podatki, ne glede na lokacijo organizacij, ki jih uporabljajo. GDPR zagotavlja povečan nadzor vseh posameznikov, na katere se nanašajo osebni podatki, nad njihovimi osebnimi podatki in načinom zbiranja in uporabe po vsem svetu (Wolford, 2019). GDPR združuje evropsko razdrobljeno nacionalno okolje za varstvo podatkov v eni uredbi. S to standardno uredbo je bilo načrtovano zmanjšanje "dragega upravnega bremena za spoštovanje različnih nacionalnih zakonov o varstvu podatkov za subjekte, ki obdelujejo osebne podatke po vsej EU" (Tamò-Larrieux, 2018, str. 83).

Po GDPR morajo organizacije varstvo podatkov vključiti v vse svoje dejavnosti in nove izdelke; vsa podjetja, ne glede na njihovo lokacijo, morajo ravnati v skladu z zakonodajo, če obdelujejo osebne podatke katerega koli posameznika, ki prebiva v EU; podjetja morajo pred obdelavo njihovih podatkov pridobiti soglasje posameznikov, na katere se nanašajo osebni podatki (Wolford, 2019). V primeru neupoštevanja bi bilo lahko podjetje kaznovano z denarno kaznijo v višini do 10 oziroma 20 milijonov EUR ali dva do štiri odstotke celotnega letnega prihodka podjetja (člen 83 GDPR). V skladu z GDPR posamezniki, na katere se nanašajo osebni podatki, dobijo večji nadzor nad svojimi osebnimi podatki, vključno s tem, kako se zbirajo in uporabljajo po vsem svetu. Podeljenih je osem glavnih novih in razširjenih pravic (poglavje 3 GDPR);

- Pravica do obveščenosti,
- Pravica do dostopa,
- Pravica do popravka,
- Pravica do pozabe,
- Pravica do omejitve obdelave,
- Pravica do prenosljivosti podatkov,
- Pravica do ugovora,
- Pravice v zvezi z avtomatiziranim odločanjem in profiliranjem

Če pogledamo z vidika potrošnikov, je razvidno, da se uporabniki spleta vse bolj zavedajo pomena zasebnosti. Leta 2013 je le 18 odstotkov spletnih uporabnikov izjavilo, da so zaskrbljeni, ker internet ogroža njihovo osebno zasebnost in ta številka se je v letu 2018 povečala na 25 odstotkov (Hedencrona, 2018). Raziskave kažejo, da potrošniki pred odločitvijo o razkritju svojih osebnih podatkov izvedejo preprost izračun tveganja in koristi, s čimer poskušajo v čim večji meri ohraniti svojo zasebnost. Če korist od izmenjave osebnih podatkov odtehta tveganje, potem jih verjetno razkrijejo (Wu, Huang, Yen & Popova, 2012, str. 891).

Druge presenetljive statistične podatke predstavlja Zveza evropskega neposrednega in interaktivnega trženja – *Federation of European Direct and Interactive Marketing* (FEDMA). Glede na poročilo *Globalna zasebnost podatkov: Kaj potrošnik v resnici meni*, ki ga je v letu 2018 naročilo Globalno združenje marketinških združenj za prenos podatkov – *Global Alliance of Data-Drive Marketing Associations* (GDMA), je 51 odstotkov vseh raziskovanih trgov trdilo, da je zaupanje ključno pri odločitvi za izmenjavo informacij z nekim podjetjem. Raziskava tudi poudarja, da si 86 odstotkov potrošnikov želi večjo preglednost, 83 odstotkov pa si jih želi več nadzora, ko gre za njihove podatke, da bi lahko vzpostavili zaupanje (FEDMA, 2018). Glede na to situacijo je Evropa z GDPR načrtovala, da bo omilila skrbi potrošnikov in vzpostavila zaupanje med podjetji in potrošniki z doseganjem preglednosti med njimi.

V teh dveh letih, odkar je začel veljati GDPR, se pri podjetjih veča število zahtev potrošnikov po vpogledu v podatke, ki jih ima podjetje o njih v svoji dokumentaciji, podjetja si prizadevajo najti vse podatke, ki jih trenutno hranijo po vseh kanalih in komunikacijskih metodah, tržne baze podatkov se zmanjšujejo zaradi ljudi, ki so se odjavili s poštnih seznamov ali niso odgovorili na e-poštna sporočila, v katerih jih prosijo, da se ponovno prijavijo, obenem pa podjetja izgubljajo pomembne evidence zaradi izbrisa informacij o strankah.

Za tržnike je to pomenilo posodabljanje njihovih politik o zasebnosti, čim bolj pregledno uporabo in vzdrževanje podatkov potrošnikov ter iskanje novih inovativnih načinov za povezovanje s strankami in zbiranje njihovega aktivnega soglasja za uporabo njihovih podatkov, da bi z njimi ohranjali "odnos trženja" (Weiss, 2018).

Glede na to, da je GDPR eden najnovejših in najpomembnejših predpisov 21. stoletja glede zasebnosti potrošnikov, ima ta tema velik potencial, ki še ni v celoti raziskan, zlasti v zvezi s Slovenijo. Zato največja motivacija za to tezo, ki bo tu razvita, sloni v njeni nedoločeni naravi oziroma lastnostih, kot tudi v čisti radovednosti, kako se mala in srednja podjetja spopadajo s to uredbo. Namen te magistrske naloge je torej videti, kako se digitalni marketing spreminja v okviru GDPR in kako se podjetja prilagajajo temu novemu digitalnemu okolju v Sloveniji, predvsem osredotočeno na mala in srednja podjetja.

Viri podatkov vključujejo sekundarne in primarne podatke. Da bi dojeli jedro zadeve, se prvi del te raziskave začne s potrošnikovim pristopom do zasebnosti, tako da je mogoče ideologijo, ki stoji za GDPR, bolje razumeti. Nato se nadaljuje s samo uredbo s sklicevanjem na Slovenijo, da osvetli, kaj sploh pomeni GDPR, pravice potrošnikov in odnos Slovenije do uredbe, čemur sledi uporaba GDPR v okviru trženja, da bi ocenili učinke, priložnosti in izzive, ki jih uredba predstavlja za prakse digitalnega trženja.

Da bi opazili, kako se teoretični del odraža v praksi, je drugi del diplomske naloge oblikovan s kvalitativnimi raziskavami, prek katerih vidimo, kako se slovenska mala in srednja podjetja spopadajo z GDPR in kako se njihove digitalne tržne prakse spreminjajo v primerjavi med

seboj. Zaradi tega je opravljenih sedem poglobljenih razgovorov, da bi odgovorili na naslednja raziskovalna vprašanja:

- Kako je GDPR vplival na tržne dejavnosti podjetij?
- Kakšne spremembe so podjetja uporabila v svojih tržnih praksah zaradi GDPR?
- Kakšne so nevarnosti in priložnosti GDPR v okviru njihovih trženjskih aktivnosti?

Na podlagi analize rezultatov kvalitativne raziskave so v zadnjem delu diplomskega dela predstavljene nekatere praktične aplikacije. Te vključujejo izobrazbo zaposlenih, uporabo analitičnih orodij, izkoriščevanje tržnih kanalov in pridobivanje zvestobe kupcev, ki lahko pomaga slovenskim ekipam, ki se ukvarjajo z digitalnim marketingom, pridobivati in ohranjati kupce v današnji dobi aktivnih soglasij.

Appendix 2: Interview Questions

The interview questions used for the qualitative research are the following:

1. How has been the industry dealing with the GDPR?
2. How has been your company dealing with the GDPR?
3. Which actions/measures did you undertake in order to be a GDPR compliant?
4. How much time did it take to get ready for the GDPR?
5. What was the biggest challenge to become a GDPR compliant? How did you overcome the problem?
6. What are the most frequent customer requests after the GDPR? How do you deal with them?
7. Did you face a loss of important records or customer data before and after the GDPR?
8. How did your company change the existing digital marketing practices in order to convince consumers to give consent to use their data and/or not to use their right to be forgotten?
9. How did the GDPR change your:

   Sales
   Pricing
   Product/service development
   Marketing communications
   Customer loyalty

10. Did you benefit from the GDPR or did it harm your company so far?
11. What are the future threats and opportunities of the GDPR you are expecting with regards to digital marketing?
12. Do you think ZVOP-2 will create further challenges for your company/industry?