Haaga-Helia
University of Applied Sciences

The Impact of General Data Protection Regulation (GDPR) on Businesses
Case: Industrial News Service - INS Oy/Ab

Tien Vuong

Bachelor's Thesis
Degree Programme in
International Business
2019

Haaga-Helia
University of Applied Sciences

Abstract

November 12, 2019

Author(s)
Tien Vuong

Degree programme
International Business

Report/thesis title
The Impact of General Data Protection Regulation (GDPR) on Businesses.

Number of pages and appendix pages
45+4

About over a year ago, the entry into force of the EU General Data Protection (GDPR) on May 25th was one of the biggest evolution of data privacy. Adopted by the European Union (EU) Member States, it replaced the Data Protection Directive (DPD) which had been applied for over a decade. Since the emerging of new technologies, the wide-spreading development of the internet and globalization, the implementation of the new Regulation is both necessary and imperative in order to secure the protection of personal data from being misused and harmonize the discrepancy of data protection laws in each Member State.

As a big step forward in the regulatory landscape of data privacy, GDPR had brought major changes to the way businesses used to operate, regardless of their industries. GDPR applies to all organizations that store or process EU citizens' personal information, even if they do not have any business presence within the EU. Failure to comply with the GDPR requirements will result in stiff penalties and fines – up to €20 million or 4% of global revenue, whichever is greater.

The paper reviews a comprehensive information package on the GDPR and main changes that the new Regulation imposes. Based on that, the purpose of the thesis is to study the impacts of the GDPR on the business, in particular, SMEs in the B2B sector.

The thesis consists of theoretical and empirical parts. Database for the theoretical part covers comprehensive information on the background, and main changes of the GDPR to support a better understanding of the research. The empirical part, on the other hand, is set to determine whether these major changes brought by the new legislation can affect the business, which might lead to challenges or opportunities for organizations. The empirical part consists of two phases: a qualitative questionnaire and an interview. The questionnaires were sent to SMEs in B2B business located in the EU and non-EU countries. An interview with a case company on the subject was conducted to gain more insights.

The findings reveal many challenges that organizations have to overcome to ensure the GDPR compliance. On the other hand, there is also a possibility to embrace opportunities brought by the GDPR to gain competitive advantages and thrive in the new regulatory climate by building trust and reputation from the commitment to data protection as well as the GDPR. The research also finds out that the majority of the organizations assume the challenges outweigh the opportunities. Based on these findings and the interview result with the case company, more discussion and suggestions for the case company are given to achieve the GDPR compliance with less hindrance of these challenges and seize quickly the opportunities.

Keywords
GDPR, data protection, data privacy, business, B2B, SMEs, challenge, opportunity

Table of Contents

1 Introduction

The implementation of the European General Data Protection has been a positive response to the concerns over data security in recent years. In this chapter, an overview of thesis topic is introduced with details of research questions and investigative questions. In accordance with scope of the thesis topic, a demarcation is also defined to give the case company and readers clear benefits gained from the research.

1.1 Background

A number of about 3 billion Yahoo accounts leaked in 2013 and a loss of approximately $350 million of the company's sale price were recorded as the biggest data thief case in the 21st century (Statista 2019). That is not to mention several cases of data breaches such as Marriott Hotels, Facebook, Equifax, and even Angela Merkel as well as many German officials as targeted victims. Along with the increase in number of data breaches, the average annual cost of cybercrime went up more than 12% from 2017 to 2018 at 13 million dollars (Ponemon Institute LLC 2019). Data security has never been more crucial after those serial events of data security threat that alarms not only the governments but also many companies and billions of people all over the world.

Awareness of personal data security existed before the age of digitalization (Bennett 2018). In the early 1980s, there were already two international agreements to regulate the cross-border flow of personal data: the 1981 Guidelines from the Organization for Economic Cooperation and Development (OECD 1981), and the 1981 Convention from the Council of Europe (1981). Until 1995, the EU Data Protection Directive was adopted and stipulated for the use and processing of personal information within the EU and only to the countries have "adequate level of protection" (Directive 95/46/EC 1995).

Global diffusion of data protection called more comprehensive guidelines for organizations to have better awareness and responses to breaches of data privacy. Therefore, General Data Protection Regulation (GDPR) was adopted in 2016 and finally enforced on May 25th, 2018. The GDPR aims to harmonize data privacy laws across Europe, in order to protect and empower all European Union citizens' information confidentiality and to reform the way organizations deal with data privacy. However, not every organizations prepares themselves properly for the changes (Lingard 2017).

In the era of digitalization, cross-border data flows have been soaring with 45 times growth since 2005 and made up a largest impact of global GDP growth, about $2.8 trillion in value,

according to a report by McKinsey Global Institute (2016). Marketing also cannot stay away from the digitalization's wave. Digital marketing becomes important strategies for almost of international firms. With the implementation of GDPR, marketers have to be more aware of obtaining, dealing and processing clients and customers information. Otherwise, potential fines can be up to €20 million or 4% of their global annual revenue (European Commission 2018).

Industrial News Service - INS Oy/Ab is a SME for B2B and international trade media marketing. With the nature of work, the company is now owning a database of over 100000 media, many clients and partners. They are now upgrading their internal database to Salesforce's which is known as the cloud system. The company is also improving their website and their marketing strategies for the goal of expansion. That is why, a good preparation for the changes causing by GDPR is very crucial for avoiding complaining and the severe penalties. (INS Trade Media Service 2018)

This thesis will be a final study as a reward of a well-done studying path and will be a part of my career's development. This also support other study for further researches or other related topic researches. My motivations which are derived from these, together with knowledge and experience, are expected to go along the process of this thesis.

1.2 Research Question

This thesis aims to analyze the impacts of GDPR on businesses, especially the case organization to determine solutions in order to avoid or overcome challenges and facilitate opportunities yet still ensure the compliance of the Regulation.

The research question can be worded as **What impacts does the GPDR have on the business, especially for SMEs?** RQ is divided into investigative questions (IQ) as follows:

IQ 1. What are the requirements of GDPR that make the differences toward businesses?
IQ 2. What do other organizations in the same sector react on GDPR?
IQ 3. How does organization perceive GDPR?
IQ 4. What are the suggestions and solutions to help the firm avoid the challenges and make the best use of the opportunities?

Table 1 below presents the theoretical framework, research methods and results chapters for each investigative question.

Table 1. Overlay matrix

Investigative Question	Theoretical Framework	Research Methods	Results (chapter)
IQ 1. What are the requirements of GDPR that make the differences toward the company?	GDPR	Own desktop research	2 and 3
IQ 2. What do other organizations in the same sector react on GDPR?	GDPR	Qualitative method questionnaire Respondents are representative of other firms	4
IQ 3. How does the company perceive GDPR?	GDPR	Interview	4
IQ 4. What are the suggestions and solutions to help the firm avoid the challenges and make the best use of the advantages?	GDPR	Questionnaire and desktop research	2, 3 and 4

1.3 Demarcation

This study will focus on how the implementation of GDPR influences on organizations. The main point of this research is to find out how should the trade media firms like INS react on the advantages and challenges the GDPR makes up, which can be understand as the mutual relationship/affect between the firms and the new regulation on data protection.

The element of criteria that should not be reached and exceeded are theories and discussion about other trends in Data Protection, such as the leak of information, the in-detailed process of development of GDPR and the regulation. Since the topic also relates to IT perspective, it should be also excluded from this thesis.

1.4 International Aspect

INS is a company providing services specialized in trade media and industrial marketing to gain highly targeting international publicity of its clients as well as connecting businesses with the most suitable trade media anywhere in the world (INS Trade Media Service 2018). Base on the GloBBA Curriculum Requirements, the thesis topic absolutely fulfils the GloBBA thesis topic requirement of an international aspect.

1.5 Anticipated Benefits

This thesis is meant to provide value to the case company that they can recognize the benefits and risks as well as barriers when GDPR is in effect. The knowledge and awareness of INS towards the new regulation provided by this study will help the company avoid violating any provision in the GDPR. Overall, INS will obtain the new understanding and recommendations on how the company adapts to the rules.

The firm's clients, media partners and other small and medium companies will get to know GDPR and its impacts in order to have more well-prepared data privacy plans or justify the implementing procedures to facilitate benefits as well as minimize risks due to potential challenges that the GDPR brought. In addition, these stakeholders will see how serious INS is taking their private information. Because of that, INS will certainly gain more credits and its shareholders' loyalty.

Finally, to the student's field of specialization, while GDPR has been a hot topic in the last 2 years, yet not everyone, or importantly not every marketer, be aware of it. Moreover, there are not many documents and academic papers about this topic. This study will contribute to the resource of GDPR in the future.

1.6 Key Concepts

Personal Data is clearly defined by the General Data Protection Regulation (2016, Article 4) is as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

General Data Protection Regulation (GDPR) is a new legislation set by the European Commission to standardize many different privacy legislations across the EU into one set of regulations in order to have better protection on EU citizen's personal data. It demonstrates how the companies, both European firms and international firms, use, process and transfer personal information of people within the EU. (General Data Protection Regulation 679/2016 / EU.)

Data breach is defined as "an incident in which an individual name plus a Social Security number, medical record or financial record (credit/ debit cards included) is potentially put at risk because of exposure. This exposure can occur either electronically or in paper format." (Identity Theft Resource Center 2018, 3.)

B2B marketing or business-to-business marketing, sometimes referred to as "B-to-B", "B2B", "business marketing" or "industrial marketing", is the practice of individuals or organization marketing products or services to other companies or organizations (Hall 2017, 1).

Small and medium-sized enterprises (SMEs) are defined in Commission Recommendation 2003/361, based on two main factors: staff headcount and turnover or balance sheet total. The SMEs are determined as companies with less than 250 staff headcount and turnover of less than €50 million or balance sheet total of less than €43 million.

1.7 Case Company

Industrial News Service - INS Oy/Ab is a 40-year-old firm specialized in gaining companies highly targeted international publicity in trade media. It was founded in Stockholm, Sweden with the mission of connecting businesses with the most suitable trade media anywhere in the world. With a unique trade media database that comprises more than 100 000 media titles in 160 countries and many key clients such as Nokia, Avtech, Iggesund, Targano and so on, the company is well trusted in their B2B communications. (INS Trade Media Service, 2018)

Recently, INS has upgraded their database from a single internal database to Salesforce's and has developed more drastic marketing strategies in many communication platforms like Facebook, LinkedIn, and business events. Therefore, the company will have better exposure as well as better Customer Relationship Management (CRM) with the help of such the new technology as cloud database. This might be a risk for INS if they have not prepared

themselves to comply with GDPR as it “applies to every business across the globe that provides goods and services to, or tracks or creates profiles of, EU citizens, regardless of whether or not that business is EU-based” (IQ in IT 2017). The results of this study will assist INS in finding out risks as well as benefits that they can take into accounts in order to comply with the legislation and still better grow.

2 Understanding GDPR from Scratch

This chapter will explain all the related concepts to identify keys points of the GDPR in general. These findings will clear the potential benefits, yet the risks also need to be avoided.

2.1 Data Protection Directive – The Predecessor to GDPR

Adopted in 1995 by European Union, the Data Protection Directive (DPD) is officially named as Directive 95/46/EC to protect individuals regarding “the processing of personal data and the free movement of such data” (EUR-Lex 1995). DPD is complied with whenever personal data is processed, that is, collected, stored, used, organized, transferred, disclosed, modified, combined, protected, erased, destroyed or otherwise acted upon. It is built on the six principles of the Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data introduced by the Organization for Economic Cooperation and Development (OECD) (OECD 2013). These principles are fall into 3 categories in details are as follow:

- Transparency means that individuals’ consent should always be required when their personal data is collected, processed or shared with third parties. Data subject has the right to access their data, make correction and even “demand the rectification, deletion or blocking of data, which is incomplete, inaccurate or not being processed incompliance with the data protection rules”. (Directive 95/46/EC.)
- Only for specified, explicit and legitimate purposes should the collected data be used to process. There is no other further purpose that the data can be processed for. (Directive 95/46/EC.)
- Data storing security has to be ensured against abuse or compromise such as unauthorized access, accidents and altercations. Personal data should not be stored for a longer period than the primary purpose for which the data were collected or processed. Member States are responsible for providing appropriate safeguard and security for personal data stored longer time than its expiration period for statistical, historical or scientific use. (Directive 95/46/EC.)

These principles of DPD standardizes at a minimum level for data privacy and security in the EU, upon which more provisions were added by each member state to form its own legislation (IT Governance Privacy Team 2017, 2). Therefore, the requirements in the

DPD is non-binding and interpreted differently across the Member States. This made not only organizations difficult to decide how many laws and provisions they should comply with; but also, EU citizens confused about their data privacy rights across the EU (IT Governance Privacy Team 2017, 2). As a result, data cannot easily flow even within the EU, even under the same directive, until appropriate conditions are met to fill the gap between different data privacy laws (Gantz 2014, 129). Realizing the obstacle for the flow of data not only within EU but also between others non-EU countries especially US and EU, the European Commission had been planning for a comprehensive reform of data protection legislation by a first draft proposal since January 2012.

2.2 GDPR – The New Era of Data Security

As the robust progress of technologies and the wide spread of online services as well as digitalization challenges, Data Protection Directive is seemed to be inapplicable in this digital age. Only in a decade, the world saw the first banner add online in 1994, online banking offered by most of financial institutions since 2000 and the emergence of such social media platforms as Facebook in 2006. Later in 2011, a lawsuit of a Google user to the firm for scanning her email rang the bell for a need of a more comprehensive and more effective law on personal data security (Seshagiri 2013). After about 4 years of planning, measuring, proposing drafts to update the 1995 directive, on December 15, 2015, the European Parliament, Council and Commission reached an agreement on a single, unified and EU-wide data protection legislation, named as EU General Data Protection Regulation (GPDR). (European Data Protection Supervisor 2019.)

The GDPR superseded the Data Protection Directive and has been officially enacted by May 25, 2018 with a mission, as being explained by IT Governance Privacy Team (2017, 2) that is to achieve “two keys goals:

- Protecting the rights, privacy and freedoms of natural persons in the EU.
- Reducing barriers to business by facilitating the free movement of data throughout the EU.”

GDPR is built on the fundament of the Data Protection Directive that are the principles introduced by OECD. With more detailed and specific legal terms and definitions, data protection requirements, bigger global scope, and tougher enforcement with severe non-compliance penalties, GDPR becomes a new modern privacy setting which gives EU citizens more control over their personal information and also facilitates businesses by letting data flows more easily across EU, cutting red tape and creating a competitive

environment for businesses in the digital market. Companies now just need to contact one DPA instead of the previous 28, which brings huge savings (IT Governance Privacy Team 2017, 4-5.)

2.3 The Requirements of GDPR

The entry of the new EU-wide Data Protection Regulation brings major changes to the way businesses used to operate, regardless to their industries. GDPR applies to all organizations that stores or processes EU citizens' personal information, even if they do not have any business presence within the EU. Organizations that infringe "the basic principles for processing, including conditions for consent" are subject to stiff penalties and fines – up to €20 million or 4% of global revenue, whichever is greater" (IT Governance Privacy Team 2017, 91).

GDPR is known as the evolution of the Data Protection Directive. Although GDPR remains the same set of six data protection principles from the DPD, the regulation's requirements are more detailed, more comprehensive and stricter to create more consistent protection of personal data throughout EU. As Giovanni Buttarelli (2015) stated during his speech "GDPR will be one of the longest negotiated EU laws ever. And, with 139 recitals and 91 articles, it is also going to be one of the longest EU laws on the statute book."

The requirements of the EU Data Protection Regulation are summarized these six following principles and can be found in Article 5 of the Regulation:

- The processing of the data must be lawful, transparent and reasonable
- Data must be collected or processed only for intended use and not for any other purpose.
- Only necessary information is allowed to be collected
- The information collected must be correct and up to date
- Data must be kept only for the necessary or agreed period of time
- Data must be carefully processed or stored under security to ensure appropriate integrity and confidentiality
- The controller is responsible for being able to interpret GDPR compliance with all of these principles.

2.3.1 Legality, Reasonableness and Transparency of Information

According to the EU GDPR Article 5, section 1, personal data must be processed lawfully, transparently and appropriately. The three components of this principles are closely linked to the obligation of data controller to provide information to the data subject (IT Governance Privacy Team 2017, 93). Transparency requires that the data controller communicate clearly and openly to the data subject when and how the data is processed. Thus, the data subject is well aware of whether their data is collected, how it is used and to which purposes, whether it is transferred to the third parties as well as knows how to exercise their right. (Voigt & Bussche 2017, 88.)

Moreover, the data subject has the right to know the controller's identity as the "fairness" principle. It's also required that the controller must obtain data from legally authorized sources, "handle data in way the data subject would reasonably expect" and only process if and to the extent that at least one of the provisions in Article 6 is met in order to ensure the "lawfulness" principle. (IT Governance Privacy Team 2017, 95.) The lawfulness of the processing of personal data is fulfilled under the Data Protection Regulation (General Data Protection Regulation 679/2016 / EU, Article 6) when any of the following criteria is met:

- The data subject has given his consent to the processing of his data
- The data subject is a party of the contract or at threshold of entering into a contract.
- Processing is a legal obligation of the controller.
- Processing is necessary to protect the vital interests of the data subject or another natural person.
- Processing is needed for the exercise of public authorities or for the performance of a task carried out in the public interest
- Processing is required for the purposes of the legitimate interests of the data controllers or a third party, unless fundamental rights and freedoms of the data subject are superseded by those interests, especially in the case of a child is the data subject. This paragraph shall not apply to data processing carried out by public authorities in the performance of their duties.

2.3.2 Purpose Limitation

The legislation states that personal data can only be collected for "specified, explicit and legitimate purposes" which are stated for the data subject (General Data Protection

Regulation 679/2016 / EU, Article 5). The information about the extent of processing involved should be provided unambiguously to the data subject in forms of privacy notices, terms and conditions and consent forms (IT Governance Privacy Team 2017, 101).

However, GDPR does permit of processing of personal data "for scientific, statistical or historical research purposes" (General Data Protection Regulation 679/2016 / EU, Article 5). If the purpose of the processing goes beyond the scope of the original purpose for which the data was collected, the data subject must be informed detailly, and in this case, has the right to decide to whether prohibit the use of the data (Voigt & Bussche 2017, 89).

2.3.3 Minimization and Accuracy of Information

Only personal data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" should be collected (General Data Protection Regulation 679/2016 / EU, Article 5). It means that no additional data should be collected or processed if it exceeds the scope of what is strictly required. For example, it would be irrelevant to obtain information about a person's workplace to use for the purpose of marketing for an installation and reparation service. In order to minimizing the amount of data to be obtained, it is critical to make sure how the data produces the results for that purpose and data mapping can facilitate to determine that (IT Governance Privacy Team 2017, 103)

Moreover, the regulation also requires that personal data must be "accurate and, where necessary, kept up to date". Data subject has the right to rectify any inaccurate personal data and complete any incomplete personal data at any time without delay. (General Data Protection Regulation 679/2016 / EU, Article 5.)

2.3.4 Data Retention Restrictions, Data Integrity and Confidentiality

Under GDPR, it is required that personal data may only retained until the legitimate purpose for which the data was collected is fulfilled, and this retention period of time should also be informed to the data subject (General Data Protection Regulation 679/2016 / EU, Article 5). Deletion or destruction of all personal data is preferably required after the retention period. Data subject is also permitted to gain legitimately copies of stored, archived or backed-up data (IT Governance Privacy Team 2017, 107).

Processing must be done in such a way as to ensure that the data is protected from unauthorized and unlawful processing, loss, destruction or damage. Thus, to guarantee appropriate security of the data, both technical security measures and organizational measures need to be implemented. (General Data Protection Regulation 679/2016 / EU, Article 5.)

2.3.5 Accountability

While these principles above might be classified as material requirements, accountability is perhaps the most crucial organizational requirement in the Regulation. It is also the considerable improvement compared with the former Data Protection Directive to have one principle of accountability laid out comprehensively in Clause 2 of Article 5 (Voigt & Bussche 2017, 31). It addresses the obligation of the data controller not only to ensure compliance with the GDPR, but also to be able to demonstrate GDPR compliance with all of these principles above to Supervisory Authorities (General Data Protection Regulation 679/2016 / EU, Article 5).

Together with the accountability principle, the non-compliance fine is also the main and important change brought by the new Regulation. Failure to ensure that all the data protection principles are met at every stage the personal data goes, from collecting, processing, storing, transferring and deleting, can be fined with up to €20 million or 4% of the total worldwide annual turnover (General Data Protection Regulation 679/2016 / EU, Article 83). This creates a more significant burden on the data controller to make sure everything complies with the law. In order to secure that, the controllers must have well-qualified understanding and practical commitment to data protection since appropriate technical and organizational measures, data mapping, the adoption of internal policies and corporate culture, and others complicated tasks must be done well to avoid the fines (Voigt & Bussche 2017, 32).

The obligation to prove compliance with GDPR has to be fulfilled upon request of Supervisory Authorities by documenting the processing activities which includes details of the data flows (Voigt & Bussche 2017, 32). These recordings should be maintained and made available to the requesting Supervisory Authority as an obligation, so that “it might serve for monitoring those processing operations” (General Data Protection Regulation 679/2016 / EU, Recitals 82).

3 The Main Changes

In the earlier chapter above, the fundamental requirements including six data protection principles and the introduction of accountability principle are addressed. However, the GDPR is known as the reform of data privacy in order to adopt into the era of new advanced technology, such as not just merely internet, but also cloud computing and the Internet of Things. Thus, some extended provisions and rules were supplemented into it to become one unified and comprehensive law across the EU.

In this chapter, the major changes that make every organization has to take into consideration to ensure the compliance with the new legislation will be discussed in detail.

3.1 Redefined Definitions

The initial change should be taken into account is that a number of definitions is clearly updated under the GDPR, in particularly “personal data”, “consent” and “processing”. GDPR expands the definition of “personal data” to cover “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (General Data Protection Regulation 679/2016 / EU, Article 4, (1)). In short, this data includes IP addresses, mobile device identifiers, and geolocation, biometric data (fingerprints, retina scans, etc.), as well as every data related to an individual’s physical, psychological, genetic, mental, economic, cultural, or social identity. Hence, nowadays, there is even higher possibility of removing the anonymity of the subject by just unintentionally gather enough information linked to the subject (IT Governance Privacy Team 2017, 10). For example, in the online marketing industry, using cookies and tracking IDs means that the organization is gaining users information through their online activities.

The definition of “consent” of data subject is also clarified in Article 4 of the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by statement or by a clear affirmation action, signifies agreement to the processing of personal data relating the him or her”. The update of many definitions is

necessary as the former of the GDPR – the Data Protection Directive was born in the age of predominant offline world with filing cabinets and folders and the internet was still infant. The same can be applied to the definition of “processing” which is defined more specifically since the technological changes facilitate the way of processing personal data to be more various. So that, “processing” is defined generally yet detailly “to make the scope of the application independent from technological changes” (Voigt & Bussche 2017, 10). “Processing” means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (General Data Protection Regulation 679/2016 / EU, Article 4, (2)).

3.2 Higher Bar for Quality of Consent

There is a number of available lawful basis for processing personal data in order to comply with the GDPR, yet consent is the simplest and was already stated in the old Directive (IT Governance Privacy Team 2017, 205). Despite that, the conditions for consent under the GDPR are amended and much more strengthened, which results in the emerging of legal difficulties for organizations, especially the data controllers. Consent are no longer abused and unfairly gained by such long text of illegible terms and conditions provided by organizations. As defined by the Regulation, consent for the use of personal data must be “freely given”, “specific”, “informed” and “unambiguous”, which is described in the figure below.

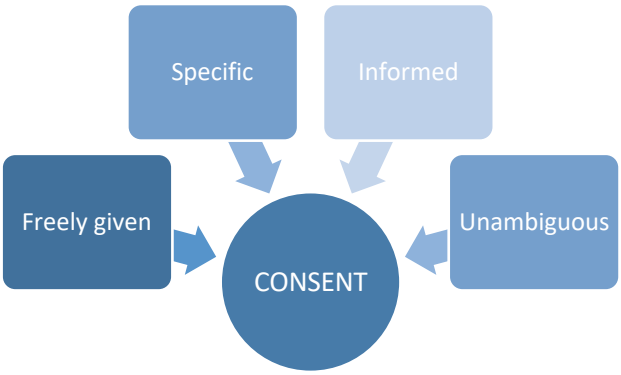

Figure 1. Requirements of a valid consent

According to Article 7 of the GDPR, descriptions of data use are required to be clear, short, straight to the point, and more importantly, distinguishable from other matters like terms and conditions or other issues, so that the data subject understands thoroughly

when and how their data is going to be processed and for what purposes. The explanation of all the purposes for processing of personal information should be also included in the consent wording, in an intelligible and easily accessible form, using clear and plain language (General Data Protection Regulation 679/2016 / EU, Article 12). Additionally, different purposes require separate consent for each of them (General Data Protection Regulation 679/2016 / EU, Recital 32). These requirements fulfill the “unambiguous” and “specific” criteria to gain valid consent under GDPR. Customers nowadays cannot be asked to agree to any terms and conditions in exchange for their consent. Moreover, in order to having a certain proof about the unambiguity that the data subject is aware of the processing of the data, it is mandatory that consent is given by a statement or a clear affirmative act of the data subject (General Data Protection Regulation 679/2016 / EU, Recital 32). It secures that the data subject has been “informed” and aware of the processing as well as which consent is given to whom (Voigt & Bussche 2017, 94). Explained by the Regulation in Recital 32, the statement or the affirmative act could be ticking an unticked box or choosing technical settings in an app or an Internet browser for information society services, and any other oral or written statement or conduct that clearly indicates the consent of the data subject. However, it also imposes that silence, pre-ticked boxes, inactivity or failure to opt-out should not constitute a valid consent (General Data Protection Regulation 679/2016 / EU, Recital 32)

Obtaining data subject’s consent is a vital but simple step to make sure the processing is lawful as the first principle addresses. Hence, consent must be given voluntarily from the data subject. Consent is likely to be regarded as “freely given” when the data subject has freedom of choice to either agree, refuse or withdraw consent without detriment at any time. In contrast, it is not the case that consent is obtained from the data subject who is in such imbalanced relationships as between an employee and an employer, or between an individual and a public sector organization or authority (General Data Protection Regulation 679/2016 / EU, Recital 43). Nevertheless, the Regulation does not mention precisely other cases of a clear imbalance, so this will be a point to be specified in the future (Voigt & Bussche 2017, 95).

Furthermore, if the performance of a contract which, for example, is to provide a service, is made conditional on consent to processing activities that are not necessary for the performance of that contract, the consent is also invalid as it is unlikely to be regards as “freely given”, according to Article 7 Section 4 GDPR. In other words, organizations cannot offer their services or provide their content in exchange for the consent of individuals for using their personal data. It is clearly stated in the Annual Report 2017 of the European Data Protection Supervisor that “fundamental rights such as the right to the

protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity" that people can pay or exchange. In practice, this builds a barrier for the online services largely depending on the contribution of personal data input which will become a valuable asset for firms (Voigt & Bussche 2017, 96). In order to prevent violating this section of GDPR, companies are forced to find solutions to limit the collection of unnecessary data.

Consistent with a "freely-given" consent, Article 7 Clause 3 of the GDPR states that the data subject has the right to withdraw the consent at any time. The right of withdrawal must be informed to the data subject at the time when the consent is given. It also must be as easy for the data subject to revoke the consent as it was for them to give it. Moreover, the legislation also determines that the processing of the personal information that took place while the consent was in place, is definitely lawful and not affected by the withdrawal.

3.3 Enhanced Rights

The new GDPR provides individuals with new and expanded rights to have greater protection on their personal data or even to complain and seek judicial remedies from supervisory authorities against controllers and processors for damages (General Data Protection Regulation 679/2016 / EU, Article 77, 79). Therefore, it is vital for both data controllers and processors to be aware of these enhanced rights and ensure the data subject's rights are informed clearly and separately from other information at first and are protected throughout the processing. The rights will be explained in detail which includes seven rights as we can see in this figure:

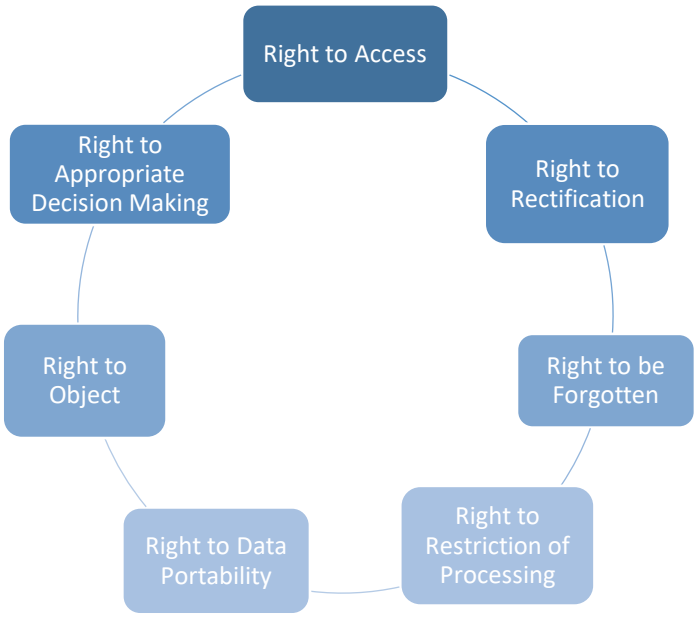

Figure 2. Data subject's rights under the GDPR

Under GDPR, transparency is especially concentrated and known as one of the core building blocks of GDPR's enhanced rights for individuals to ensure the fair processing. The GDPR's requirements regarding transparency are already addressed in chapter 2.

In order to increase the transparency and the fairness of the use of personal data as well as empower the data subject, the GDPR expands the data subject's right to access their personal data. In more details, data subject can request confirmation or information from the data controller. Such information that the data subject can request to access is as the following:

- A copy of the personal information
- The purpose to process personal data
- The categories of the data being processed
- Any available information about the source where personal data is collected from instead of from the data subject.
- The third parties or the categories of third parties that will receive their data (General Data Protection Regulation 679/2016 / EU, Article15, Clause 1, and Directive 95/46/EC, Article 12).

A marked change from the former directive is that information requested to access should be provided in a variety of formats like electronic or hard-copy format, and free of charge. Unless the access request is manifestly unfounded, excessive or repetitive, the controllers are allowed to refuse an information request or charge a "reasonable fee" to cover the administrative cost of providing information (General Data Protection Regulation 679/2016 / EU, Article 12, Section 5.) Naturally, the identity of the data subject must be verified before the information is disclosed (Voigt & Bussche 2017, 152). Recital 63 of the GDPR also includes cases when there is any occurrence that the right to access can harm other rights or the freedom of others, including trade secrets, intellectual property or professional secrecy, for example, lawyers' documents might contain data of the opposing party of their client (Voigt & Bussche 2017, 153). Thus, it is vital for the controller to be careful when handing out the information to the data subject, by concealing such data that might adversely influence others (Voigt & Bussche 2017, 153).

Crucially, one of the noticeable changes regarding the right to access of the data subject is that the response to a data subject access request by the data controller must be "without undue delay", instead of "without constraint at reasonable intervals and without excessive delay or expense" as of the Data Protection Directive (Directive 95/46/EC,

Article 12). And in any circumstance, the time for organizations to respond to subject access requests to exercise rights is limited explicitly to 30 days under the GDPR (General Data Protection Regulation 679/2016 / EU, Article 12, Clause 3).

Parts of the expanded rights of data subjects outlined by the GDPR is the right of data subjects to rectification, erasure and restriction of processing their personal data. The right to rectification is explained in Article 16 of the GDPR as the right to require inaccurate or incomplete personal data concerning the data subject to be corrected, completed, or to record a supplement statement, “without undue delay”. This right is likely link to the right to access, so that the controllers must ensure the availability of the systems used to support the access and the rectification in a timely manner. In addition, there also the right of data subject to restrict the processing of personal data, which means as a medium between the conflicting interests of data subject who wants to rectify or erase the personal data, and of the controller who wants to continue the processing of concerned personal data (Voigt & Bussche 2017, 164). Empowering by the right to restriction of processing, data subject is allowed to prevent controllers from further processing of the data, yet only under certain circumstances. Examples for each circumstance are listed under Section 1 Article 18 of the GDPR:

- If the individuals concern about the accuracy of their personal data held by a certain organization and they contest it, the restriction shall take place for long enough to enable the controller to verify its accuracy;
- The processing of personal data is unlawful, but the data subject objects to erasure and instead requests the restriction;
- The controller has no further need with the purposes of processing for the personal data, but the individual requires the controller to retain the personal data to establish, exercise, or defend legal claims.

Besides, one of the most controversial recent issues in data protection law which drew a greater attention of the public is the reinforcement of the right to be forgotten, as known as the right to erasure, compared to the former directive (Voigt & Bussche 2017, 156). While the Data Protection Directive simply require data to be erase “as appropriate” (Directive 95/46/EC, Article 12 (b)), the new legislation underlines clearly that this data erasure right entitles the data subject to require the controller to delete the personal data “without undue delay”, possibly require also third parties to stop processing it. However, based on Article 17, Clause 1 of the Regulation, this can only be exercised when the controller does not have any legal ground for the processing, which is contained in a number of specific circumstances such as:

- Personal data is no longer necessary for the purpose of processing;

- The personal data are processed unlawfully, which is seen as breach of the law but anyway a right to erasure is granted by this provision;
- The personal data must be erased due to a legal obligation under the European Union or Member State Law which applies to the controller;
- The individual withdraws consent to the processing and there is no other legal reason for processing;
- The data processing is based on legitimate interest to which the data subject objects, and the controller is unable to interpret that there are overriding legitimate grounds for the processing.

This right to be forgotten might lead to difficult tasks for organization and especially the controller in the era of internet and online world. This will be discussed further in the research findings section. Also, there are not so many options for organization to refuse the obligation of erasure personal data, unless the holding or processing the personal data is necessary:

- For protecting the right of freedom of expression and information
- For compliance with an EU or Member State legal obligation
- For the performance of a task in the wider public interest or exercise of official authority.
- For public interest reasons in the area of public health
- For archiving, scientific, historical research or statistical purposes.

Together with those three rights above, there are two other rights that already existed under the Directive: Right to object and Right not to be subject to automated decision taking. In addition, the GDPR grants the data subject the right to object not only to the processing of personal data for direct marketing purposes as in the Data Protection Directive (Directive 95/46/EC, Article 14 b), but also to the processing either based on legitimate interests of the controller or in the public interest, and for the purposes of research or statistic. Once the objection is raised by the data subject, the controller's obligation is to make sure the processing of the concern personal data is suspended until the controller carries out justification by demonstrating compelling "legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims" (General Data Protection Regulation 679/2016 / EU, Article 21). Similarly with the former directive, the GDPR also gives the data subject the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affect him or her" (General Data Protection Regulation 679/2016 / EU, Article 22). This right under the GDPR protects the individual's rights and freedoms as

a minimum including the right to trigger human intervention, to express their point of view and to contest the decision.

In order to reinforce the data subject's power of control over the personal data in the digital age nowadays, the GDPR introduces a new data subject right, namely the right to data portability. This right shall give the data subject the possibility to control personal data wherever processing carried out by automated means, by enabling the data subject "to receive the personal data concerning him or her, which he or she has provide to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from controller to which the personal data have been provided" (General Data Protection Regulation 679/2016 / EU, Article 20). Briefly, under the GDPR, the data subject is able to access the particular data, which is hold by a controller, and to transmit that data easily and safely to another controller or even across different services. Nevertheless, article 20 of the GDPR clarifies that the application of this right is narrowed to some circumstances:

- The individual has provided the data to the controller themselves;
- The original processing of the personal data is based on the data subject's consent or for the performance of a contract;
- The processing is automated, so no paper records can be applied in this case.

Unlike other rights under the GDPR, although the right of data portability also has some restrictions regarding the violating of others' rights and freedoms, trade secrets and intellectual property or the negative impact on the third parties, it is not restricted by any "processing necessary for the performance of task carried out in the public interest or for compliance with a legal obligation to which the controller is subject or in the exercise of official authority vested in the controller" (General Data Protection Regulation 679/2016 / EU, Article 20, Section 3 & Recital 68). In practice, the transferring data across different service providers is likely prevalent throughout many parts of Europe, especially in Finland where most of the information of an individual is linked from places to places. Its impact will be discussed further in the later section.

3.4 Extra-territorial Reach

One of the biggest changes to the data privacy regime brought by the new GDPR is the expansion of territorial scope of application. GDPR explicitly states in its Article 3 that all provisions in the GDPR apply to all the processing of personal data of the data subject carried out by both controllers and processors, regardless of where the processing takes place and where the controller and processor is established. As long as the data subject is

EU citizen, the GDPR subjects to all the organization or natural person that handles personal data of that individual for the processing activities related to “the offering of goods or services, irrespective of whether a payment of data subject is required” or “the monitoring of their behavior as far as their behavior takes place within the Union” (General Data Protection Regulation 679/2016 / EU, Article 3). This means that any organization in the world might be caught by the Regulation, so that organizations based outside the EU have to consider if they fall into this category, to implement necessary steps to ensure compliance with the GDPR. This includes the requirement of the GDPR to nominate in writing a representative organization who must be located within the EU where the data subject is based. The liability of the representative under the GDPR are for the breaches of the Regulation and follows the specific instructions from the controllers. (Kolah 2018, 7-8.)

3.5 Responsibilities of the Controller

As described earlier in the section 2.3.5, the accountability principle, which is newly reinforced and introduced by GDPR, imposes the heavy liability to both data controller and data processor to comply with the Regulation. Different from the old data protection legal framework, the GDPR places the role of the data controller as well as the data processor at the center (IT Governance Privacy Team 2017, 235). Under the GDPR, not only the controller who are responsible for “determining the purposes and the means of the processing of personal data” according to Article 4 of the legislation, but also the processors who are contracted by the controller to process personal data must abide by the Regulation (General Data Protection Regulation 679/2016 / EU, Article 8). However, it is a main obligation of the data controller to make sure that the processor like cloud service providers, marketing agency or SaaS vendors processes personal data in accordance with the legislation by providing sufficient guarantees for implementing appropriate technical and organizational measures (General Data Protection Regulation 679/2016 / EU, Article 28).

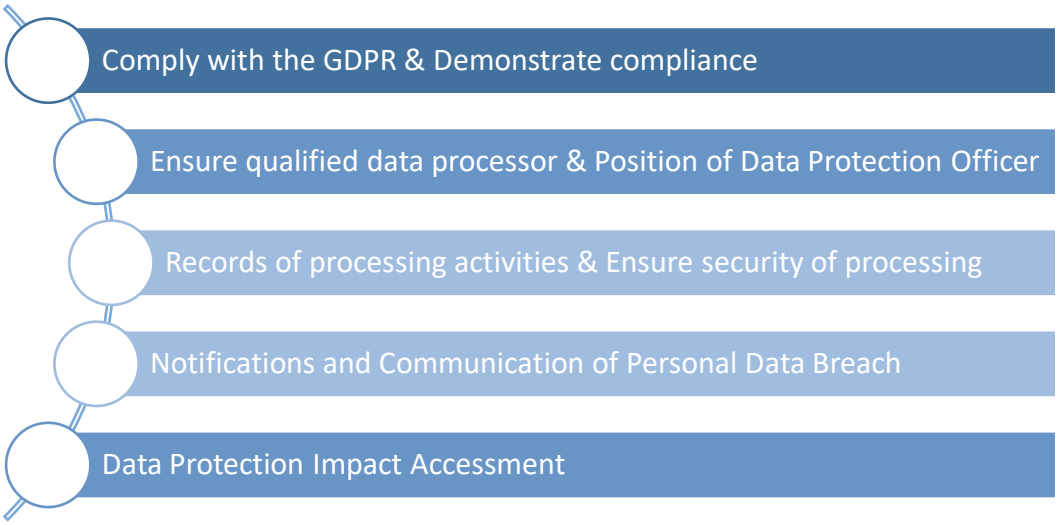

Figure 3. Data controller's obligation under the GDPR

The liability of the data controller does not stop at ensuring the compliance with the GDPR. The new Regulation has extended it to include the ability to demonstrate compliance. It means that the controller must be able to prove the data processing is complying to supervisory authorities. The proof might be a burden if the controller does not have appropriate measures in place, and especially the records of processing activities. The records help increase transparency and lawfulness of the data processing activities. They act as evidences of compliance which may consist of data protection policy documents, risk register, fair processing notices, retention policies, evidence of consent, Data Protection Impact Assessment reports, and so on (IT Governance Privacy Team 2017, 242). However, for some organization, maintaining those records might be time-consuming and potentially costly, so that there is an exemption from obligation of documenting data processing activities for organizations that employ fewer than 250 people as being stated by Recital 13 of the GDPR. Additionally, the Data Protection Impact Assessment (DPIA) just mentioned above is also one of the important records that organization must consider. It must be carried out when the processing of personal data, especially when using new technology, "is likely to result in high risk to the rights and freedoms of the data subject" (Voigt & Bussche 2017, 47). Also, it is necessarily conducted when there is any risk which is potentially derived from changes such as of the processing purposes or of the personal data. It plays an effective role accordingly with the general risk-based approach of the GDPR.

Apart from those duties, the extended jurisdiction of the GDPR includes the notion for breach notification. Clearly stated in the Regulation (2016, Article 33 & 34), it must be implemented as an onus of the data controller and the data processors for the sake of the data subject to prevent or cease the risk for the rights and freedoms of the data subject at

the minimum. As data breach might harm the rights and freedoms of the data subject, it is now mandatory under the GDPR for the controller to notify data subject as well as the supervisory authority “without undue delay” and typically “within 72 hours of the first having become aware of the breach” (General Data Protection Regulation 679/2016 / EU, Article 33 & 34).

In order to ensure GDPR compliance, it is responsible for the data controller and the processor to carry out appropriate controls by adopting applicable technical and organizational measures which help meet the data protection principles and conform to Data Protection by Design and by Default. Article 25 of the GDPR prescribes explicitly the concept of Data Protection by Design and by Default which entire practices and policies of the organization are required to embed, particularly when data processing uses digital technology. Data Protection by Design concept requires organization to take data protection and the privacy rights of the individuals into account from the onset of the system designing stage. Data Protection by Default concept looks closer to the necessity of inclusion of data privacy protection in default settings of any digital interface like websites or apps. (General Data Protection Regulation 679/2016 / EU, Article 25; Kolah 2018, 149-151.) Even though the technological progress might facilitate the data collecting and processing better with greater amount of information, data controller must keep data minimization in mind to limit the amount of data being obtained adequate for the purpose of the data processing, as well as pseudonymization personal data as soon as possible. Usually, companies take advantages of the default settings to gain as much personal data as possible, more than what they need. Thus, the privacy-friendly default settings protect users from that common problems when they do not have technical knowledge or time to change the settings of a service or product at the first use or access. (Voigt & Bussche 2017, 63.)

There are more specific steps which can be used to achive the embed of Privacy by Design and by Default into the organization culture. According to IT Governance Privacy Team (2017, 18), the initial step is definitely creating an appropriate “compliance framework” which acts as a structured guidelines and practices to ensure the core of the organization’s behaviour really has the perception of data protection. It is also an useful mean to deliver the all complex requirements of the GDPR to the organization, so that the organization can determine its actionable roadmap for achieving compliance and mature the overall data protection capabilities including its business processes, policies and controls.

Figure 4. Three categories of activity: people, process and technology (IT Governance Privacy Team 2017, 17)

There are always three categories of activities including people, process and technology in a compliance framework, as illustrated by Figure 2. An efficient information security management system might be built from these technical measures above such as staff training, audits, and specific procedures including data life cycle management, risk assessment, incident response processes and so on. The figure focuses on the importance of people and process rather than technology for the organization to align with the legal requirements. However, technology is also a vital component for data controller to sufficiently and effectively implement the GDPR requirements and to protect the rights of the data subject. (IT Governance Privacy Team 2017, 16-18.)

4 Study on the Impacts of GDPR on Businesses

In this chapter, the impacts of GDPR on business as well as on marketing-related activities will be looked into by combining the findings of the theorical part in Chapter 2 and 3 and research on the topic in reality. The results of this will be a conclusion and suggestion for the case company on turning the GDPR compliance headache to opportunity.

4.1 Research Design & Method

This part will explain clearly the details of how data was collected and how the data was analyzed. The starting point of plaining for data collection was to look in general about the issue to figure out what questions should be asked to find the answer and solution for the issue in the end. Based on that, the research objectives and investigation questions for the matter can be produced as the following:

An analysis of GDPR's impacts on businesses with the case company Industrial News Services is followed by the investigation questions:

IQ 1. What are the requirements of GDPR that make the differences toward businesses?
IQ 2. What do other organizations in the same sector react on GDPR?
IQ 3. How does organization perceive GDPR?
IQ 4. What are the suggestions and solutions to help the firm avoid the challenges and make the best use of the opportunities?

From those questions, the research approach should be decided to use in this thesis is qualitative method including both interview and qualitative questionnaire as well as desktop research. The use of qualitative method is seemed to be effective for this topic since there are many concrete statistics of the topic in both wide and narrow scope conducted and published by trusted organization such as European Commission (EC), the Office of the Data Protection Ombudsman or European Data Protection Board (EDPB). For the research method, risks and limitations of the methods were also evaluated, together with the reliability and validity of the research.

The study will be divided into 3 phases which are illustrated in figure 5 below. In phase 1, own research from primary resource and appropriate secondary resource will be used to statistically analyze and answer the IQ1 with the main source from the GDPR documents.

IQs 2 and 3 will be conducted through qualitative analysis as well as from desktop research in phase 2 and 3. For IQ2, a qualitative questionnaire will be given to representatives of a few company in different countries. Some of the questions can be done with Likert scale from 1 to 4 and multiple choices. The rest of the questions might be some open-ended questions to obtain more insight of the answers. For IQ3, interview and discussion will be organized with INS to gain unique understanding of INS's customer relationship management system and INS's awareness towards the GDPR. Finally, IQ4 can be done by combining all the analysis and conclusion from IQs 1, 2 and 3, and theoretical support from desktop resources.

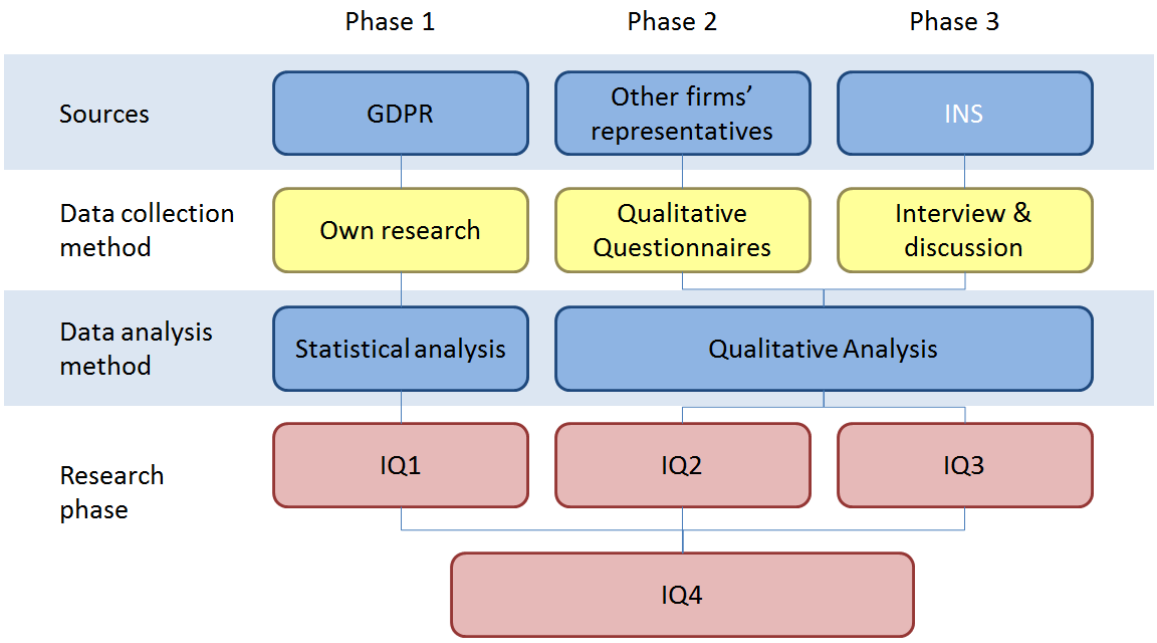

Figure 5. Research methods.

4.1.1 Desktop Research

For this topic, it is important to dig into both primary literature and secondary literature as the topic relates to law document. Primary sources include text of laws, other original documents, original research as well as datasets, survey data and so on, that are immediate and first-hand accounts of a topic. In the other hand, secondary sources are books, reports, journals and articles, based on primary sources but they analysis and interpret on the same topic with more different layers. That is why secondary literature are more suitable for wider audience. (Saunders, Lewis, & Thornhill 2012, 84.)

Looking into primary literature like the text of law is likely to be hard and stressful to locate the necessary information. Thus, the use of secondary literature as well as the support of

valuable internet sources are absolutely necessary to gain a deep understanding on the theoretical framework as the new Regulation – the GDPR. Those secondary sources were critically chosen, so that the information providing to this thesis is current and accurate.

4.1.2 Qualitative Questionnaire

Among the variety of collecting data methods, qualitative research method was used for this topic as a mean to deliver special value with complex textual description of how organizations experience the issue (Saunders, Lewis, & Thornhill 2012, 361). The focus of this study is to achieve deep understanding of how the legislation changes the business activities and in which ways. Hence, in-depth investigation should be conducted by qualitative questionnaire.

The questionnaire was used in this thesis for the answer of how far other SMEs organization catch up with the preparation for the GDPR compliance and how this changes their business activities. The qualitative questionnaire is more effective to acquire valuable information than the quantitative questionnaire as the investigation is based on information provided by companies, not by general population, and there is availability of valuable and reliable data and statistics from the authorities. The designing of the qualitative questionnaire includes multiple choice questions, Likert scale question and mostly open-ended questions which also have to be easy enough to get the answer, but hard enough to obtain more insight. It was sent via email to 20 different Business-to-Business (B2B) SMEs in Finland and in other countries including non-EU countries and EU countries. The answer of the questionnaire was anonymously provided by representatives of the companies who are responsible for data processing, collecting, and any activities related to deal with personal data such as DPO, marketer, sales representative, manager and so on. Data protection issues are often something that companies do not want to talk about openly. Therefore, the answers would be accurate as well as able to give a better overall picture of the situation.

4.1.3 Interview

Interview is also one of the qualitative research methods. It is defined by Saunders, Lewis, & Thornhill (2012, 372) as a conversation with purpose, in which the interviewer is required to ask precise and unvague questions. The answer is given willingly by the interviewee. In this thesis, personal interview with a marketing and sales coordinator of INS, Chris Thompson, was conducted to study the background and current situation of the case

company. The interview was conducted with structure and the communication was going well to eliminate misunderstandings.

4.2 Risks and Limitations

Risks are sometimes inevitable, but a better preparation will give a chance to avoid it. The risks and limitations of this study have to be evaluated, and if it is possible, an elimination need to be applied. Secondary data research is potentially one of the risks in this research. Some sources were out of date with inaccurate, non-factual or valueless information to the study (Saunders, Lewis, & Thornhill 2012, 82). As the topic is quite new, the risks of out of date information might barely occur. In order to ease this risk, critical preview of the literature had to be done properly and only high-qualified and reliable sources should be used in the thesis. These sources that provides rich information are the authorities' website like the European Union, European Commission, and other authorized organization handling the GDPR-related matters. High-qualified books, articles and journals was also used to gain information for the theoretical part.

In terms of limitations, it is necessary to consider low response rate and validity and reliability of the answer of the qualitative questionnaire as risks and limitations which might lead to biased results. It was sent via email which is known as one of the easiest ways of communication in business environment. However, among 20 SMEs organizations, there was only 9 responses given even though a reminder for each organization was delivered. Due to the limited timeframe, no other solution can be given to increase the response rate. All in all, the information acquired from the questionnaire is adequate with in-dept understanding for the subject to conclude to suggestions.

4.3 Validity and Reliability

A study is reliable based on how stability the results bring; whereas validity is evaluated based on accuracy of the measurement (Burns & Bush 2014, 214). Validity and reliability of this study have been guaranteed throughout this study from research planning, designing and methodology, to data collection and analysis.

All primary and secondary literature have been critically chosen and referenced correctly in accordance with the Haaga-Helia UAS referencing guidelines. All tables, figures and appendices are correctly attached to gain deeper knowledge of the study. Research design and methods are also unambiguous explained in a comprehensive structure. In

order to obtain a stable result to create the validity of the study, questionnaire was built carefully with structure and questions can be interpreted easily with the consistent meaning for all respondents.

While the information acquired from the questionnaire is well-qualified with adequate information for the study, it is crucial to analyze critically the questionnaire results due to the low number of respondents. However, the availability of current statistical researches from authorities and reliable organizations can be used for greater support to this study.

4.4 Research Findings

This section will present and explain the key findings of the research. An analysis for the impacts of the new legislation – the GDPR on businesses especially SMEs in B2B sector will be carried out. As being addressed in the previous chapter, the entry into force of the GDPR has brought many changes to business, in particular, the activities related to personal data handling and processing. The question of whether these changes can become opportunities or challenges will also be answered in this section. Based on the analysis of collected data, the results of the research are outlined with the discussion from case company's interview.

4.4.1 Challenges on Business and Marketing-related Activities

It has been more than a year since the enforcement of the GDPR was adopted by the European Union Member States. The regulation creates a crucial benchmark for the field of data protection across the EU in the era of advanced digital technology. It has been observed as going towards the right direction in harmonizing the data protection law within the EU and providing greater protection to the personal data and the rights of the EU citizen (Birer 2019); however, personal data breach, of course, still happens and increases about the size of breach. An advancement of technology facilitates many inventions and positive developments for human being, yet it also enables the misuse of those technologies to obtain unlawfully even a greater amount of personal data.

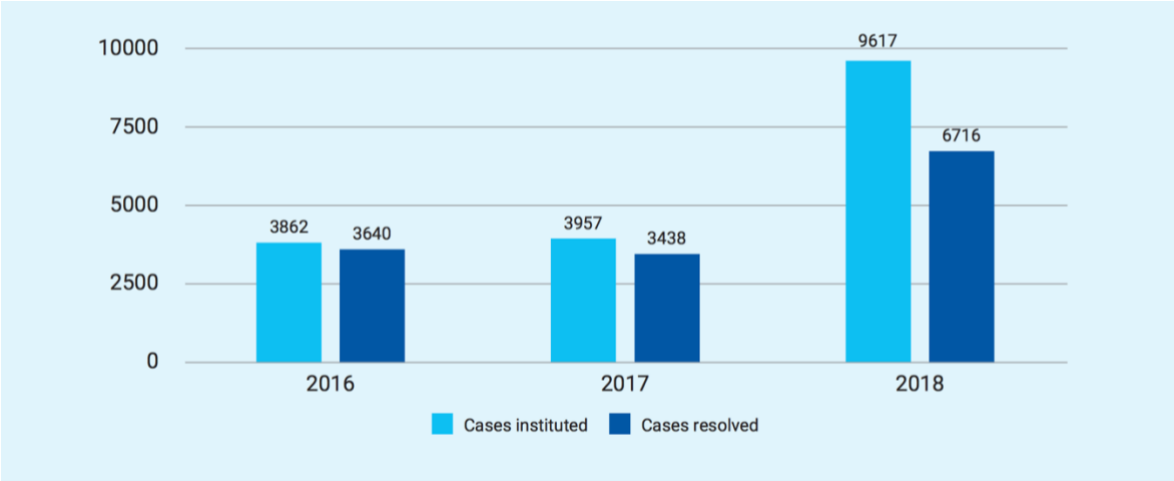

Figure 6. Cases instituted and resolved in Finland from 2016 to 2018 (The Office of the Data Protection Ombudsman 2019, 5)

Reported by The Office of the Data Protection Ombudsman that there was an explosive growth in case number - total of 9617 cases of data breach in 2018 in Finland. It was more than double the number of cases in the year of 2017. This remains a challenge for both organizations and authorities to handle, manage and secure date more effectively to protect the rights of the data subject.

For organization, the entry into force of the new data privacy protection law has drawn many challenges to the way organization used to handle personal data to comply with the legislation. The new Regulation has brought many extended jurisdictions in order to strengthen the rights of the data subject. The key changes have been discussed clearly in section 3.1. Nevertheless, it is challenging for most of the organizations to adopt with those changes to ensure their compliance with the GDPR. In terms of the right to access, the one-month deadline to respond to the data subject access request might be quite tight for organization that handles a huge amount of information, but unfortunately also receives a large number of requests at the same time. In that case, although the organization is allowed to extend the timeframe to two more months to response, it might be costly and time-consuming (IT Governance Privacy Team 2017, 190). It is also a difficult task for the controller to implement the protection to the right to rectification and to restriction of processing when the personal data has been disclosed to the third parties. The controller must notify about the restriction to as many third-party recipients as possible (General Data Protection Regulation 679/2016 / EU, Article 18.) The similar problem occurs when the controller handle erasure requests. In this digital landscape, it is almost impossible to have one's personal data which has been made available to the public deleted. Article 17 of the GDPR imposes the using of available technology and any possible method to "take reasonable steps" to achieve this. Since the GDPR has deep

technology implications, more investment is needed to improve technology tools and systems to guarantee the data subject's rights is protected in accordance with the GDPR.

Additionally, more problems and risks emerge when the organization comply to the right to object as the data subject can object to particular types of data processing, especially direct marketing including profiling in relation to behavioral advertising. Even though the change might seem good for data privacy, it is the bad news for existing marketing and sales techniques. Adding business cards received from business events or conferences into a CRM system of a company without consents of data subject is heretofore an effective method to acquire more prospects. Profiling or developing a snapshot of an individual's interests using browser history or cookies now need the explicit consent given by the individual concerned; otherwise these methods are no longer be acceptable under the GDPR. (Beaumont 2018.)

The results of the qualitative questionnaire also bring some insight. When asking the respondents about which requirements of the GDPR they concern the most, the answers surprisingly vary. One out of 9 respondents said they are not sure about all the requirements while the rest of the answers are "valid consent", "right to be forgotten", "cross-border data transfer" and "restrictions on profiling". From these answers, "valid consent" and "right to be forgotten" were mostly mentioned as the substantial concerns with the companies.

On a bigger view, GDPR is constituted by 99 articles supported by 173 recitals outlining specific requirements for organizations that process personal data. As a long piece of text with a number of provisions which have been justified and updated, the complexity of the legislation presents as one of the onerous undertakings for organizations. There are also some remained unclear provisions and insufficiency of non-compliance and breach cases, which creates confusion for organization to comply with the law.

As being described in the previous section, three components of the compliance framework that all organizations have to consider when implementing any set of legislative, regulatory or contractual requirements are people, process and technology. The GDPR competency of human resource from top down of the hierarchy of the organization is significantly crucial to ensure the GDPR compliance (Kolah 2018, 44). Since the GDPR has been implementing for only one year, it is difficult for organization to have sufficient qualified staff who can understand thoroughly this long and complex Regulation (Barclay 2019). Moreover, investing in human resource, in processes such as legal bases for processing, data auditing and privacy policies, as well as in technology

means that the burden is heavier placing on the organization to invest more time and money to achieve those, especially the SMEs (Information Commissioner 's Office 2019, 6).

These above possible challenges are, therefore, used in this research to evaluate more precisely their affects to organizations. By utilizing Likert-scale question form, some interesting points regarding the biggest concerns of the companies in order to comply with the GDPR were revealed. As being showed in Figure 7, there were two obstacles that all of the respondents concerned about: the complexity of law and the lack of well-qualified employees, which account for the highest two mean scores at 3,44 and 3,22 respectively. In details, five out of nine SMEs in the research of this thesis think that the complexity of GDPR made them worried the most (56%) and three others (33%) said that they 'moderately concerned' about that challenge. This meant the complexity of the law is the most onerous challenge in this research. Besides, as the lack of qualified staff was an extreme concern of four out of nine companies (44%) and a moderate concern of three others (33%), it was the second most challenging barrier to achieve GDPR compliance. The insufficient budget and the time limit for the preparation to the GDPR compliance were also the difficulties that were concerned differently among the respondents. While there were totally seven companies having concerns about the insufficiency of budget (mean score 2,44), only six companies had some concerns about the limitation of the preparation time (mean score 2,00). Technology shortage was not the main barriers to businesses especially SMEs. None of respondents extremely concerned about the technology shortage. Most of the answer for it were 'Not at all concerned' and 'Somewhat concerned'.

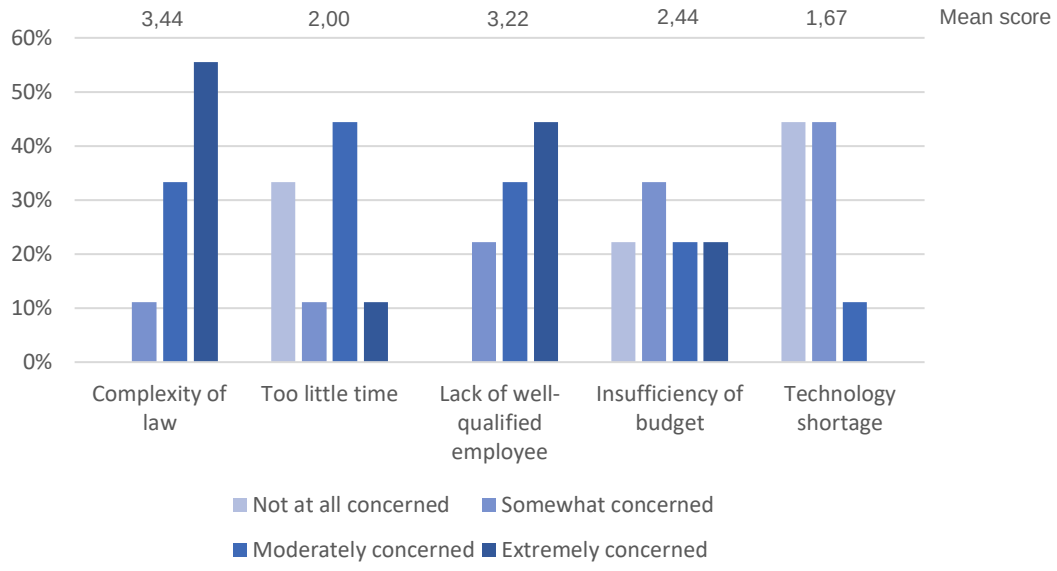

Figure 7. Possible challenges for organization to GDPR compliance (Mean score on 1 – 4 scale: 1= Not at all concerned; 2= Somewhat concerned; 3= Moderately concerned; 4= Extremely concerned)

This result links to the question “How significant were the changes in the preparation for GDPR compliance compared to the previous activities?”. In general, most of the answers shared that the companies either updated, replaced to a latest version or combined the old technology systems with the new one which enable them better control of data processing and handling to facilitate compliance. Some answers also shared that they already made a so-called GDPR compliance plan and introduced it to their employees. More checks and updates were added into the procedure of handling personal data as well. These results mean that all of the SMEs in this research understands the importance of GDPR compliance and urges themselves to make changes in order to comply with GDPR.

4.4.2 Opportunities on Business and Marketing-related Activities

Even though there are numerous compliance challenges that the GDPR has brought not only to the authorities, the EU organizations, but also to those which are outside the EU, the presence of the GDPR has two utmost goals: to protect the rights, privacy and freedoms of EU citizen, and to reduce the hindrance of data flow to facilitate business development across the EU (IT Governance Privacy Team 2017, 2). More than a year after its enforcement, the GDPR has been seen as bringing many positive changes for the development in nowadays’ digital environment, which is likely to assume that it is going in the right direction.

One big step forward with the development of the personal data privacy regime is the GDPR raises the voice of the civil society into the digital world. Thanks to the Regulation, more and more people knows or even understands and studies about GDPR. According to a recent statistic provided by The European Data Protection Board (2019), until March 2019 there are 67 percent of Europeans have heard of the GDPR, an increasing number of queries and complaints is reported, compared to 2017 with over 144 thousands queries and complaints to data protection authorities.

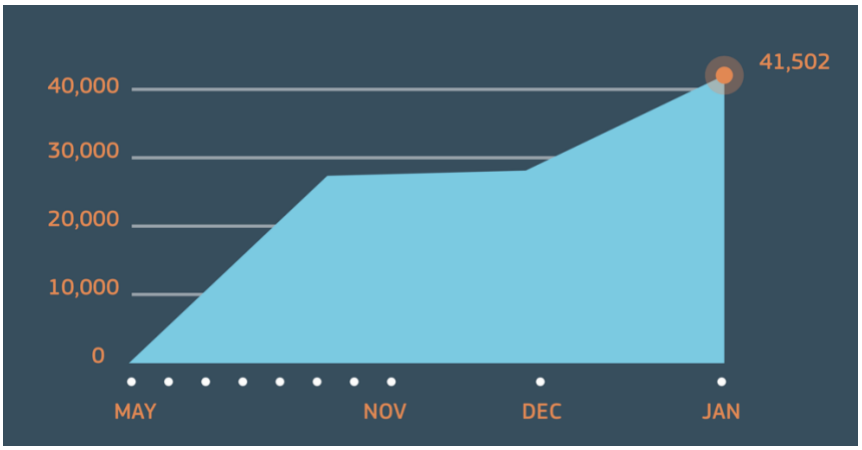

Figure 8. Accumulated numbers of data breach notifications over time, from May 2018 to January 2019 (The European Data Protection Board, 2019)

The diagram above shows the fast-rising accumulated number of data breach notifications over a short time, only 9 months from May 2018 until January 2019. While the number was only 41 502 data breach notifications on January 2019, it considerably accelerates to over 89 thousands of data breach notifications across the EU just two month later. Undoubtedly, it is inevitable to stay away from data breach in the age of today digital technological advancement, when data is still easily misused by human errors and the majority of attacks originated from malicious outsider (Statista 2019). However, the increase number of responses to breach reflects the rising awareness of the Europeans towards data privacy and their data protection rights. Those numbers also reflect the enhanced commitment of organization to comply with the GDPR's requirement of breach notification in particular as well as the GDPR in general.

The level of commitment to comply can also be interpreted by the organizations' stage of readiness for GDPR compliance which is showed in Figure 9 below. The result revealed that in the total of 9 companies, there was no company has not acted in accordance with the law. Precisely, four out of nine companies assumed that they fully complied with the GDPR and the same number of companies were in the stage of implementing the plans and procedures for compliance. Only one company was still planning steps to meet the requirements.

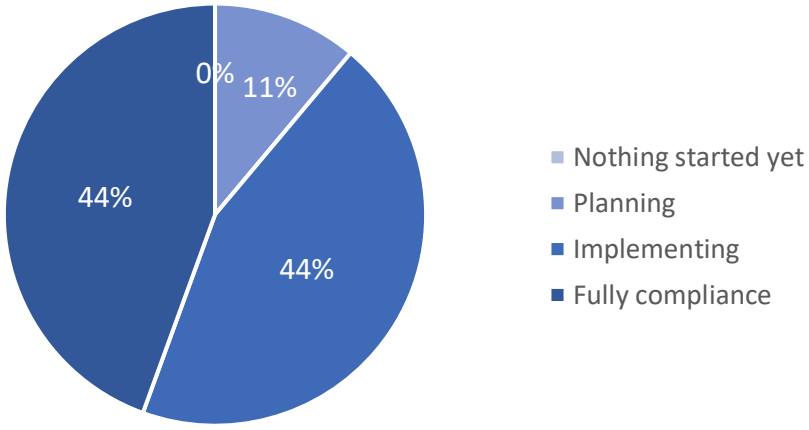

Figure 9. Organizations' stages of readiness for GDPR compliance.

The more people are aware of their data privacy rights, the more concerns are raised regarding how and when their information is collected, processed or stored, and for which purposes. Due to the lack of trust in digital environments, people are now more vulnerable for the security of their personal data than ever (European Commission 2018, 3). This is the point for organization to prove the respect towards the data protection of its clients, customers, prospects as well as all other stakeholders by showing them transparently that their data is processed totally in accordance with the law and providing transparent tracking of personal data. Transparency is now not only a merely key theme throughout the GDPR, but it also plays an important role for organization to embrace a big opportunity to win the customer's hearts and minds as well as the business. (Mathur 2018.) In some perspective, the complexity of the regulation is likely to result in the lack of the GDPR understanding and confusion of customer. In terms of CRM, business can also take advantage of this by using "Privacy by Design" concept in designing user experience in which data privacy is set as first priority. A clear communication with customers on the data privacy policies may make the brand trustworthy and differentiate services that understand the concerns of customer and always put customer first. (Reuter 2018.) Furthermore, the compliance framework (figure 4) introduced earlier can also be useful to obtain certifications by using national or international standards in order to enhance credibility with customers and stakeholders (IT Governance Privacy Team 2017, 18).

All of the SMEs participating in the questionnaire not only recognized the GDPR's challenges that they possibly face by understanding their weakness on complying with the legislation, but they also see the opportunities that the regulation brings in the long run. The respondents shared the same views on the opportunity to earn trust and enhance reputation of the firm with highest transparency and being serious about personal data

privacy. However, almost all of the respondents see the challenges outweigh the opportunities that the GDPR has brought, since changes are not easy to accept.

As being clarified in section 3.1.3, the Right to Data Portability is first introduced by the GDPR, which strengthens the control of the data subject while giving it the greater accessibility of data as well as the chance to transfer data from one service provider to another. For some organization, this might be burdensome, yet they are still able to turn that compliance difficulty to their business opportunity. As users can transfer their own data across different systems without further pain, business especially SMEs are able to seize the competitive advantage to attract customers from competitors. (IT Governance Privacy Team 2017, 199.) In addtion, the Right to be Forgotten has been explained as one of the biggest concerns for organization. However, the advatage from it can only be seen in the long run. Individual who raises their request to the company to implement the Right to Erasure will not care about neither the products, services as well as benefits that they are offered, nor other necessities of, for example, being in the email list of the company. Hence, for email marketing, the less those kinds of emails and information of individual who is no longer interested in the company, the email list has, the more opportunity the company has to deliver more and better value to the right potential customers and prospects by, for instance, providing personalized email content. Once redundant, obsolete and trivial data is eliminated, there is more room to achieve better customer engagement, Return On Investment (ROI) and better decision making. (Fagerström 2018.)

After one year of implementing, the GDPR has been observed as going towards its original and ultimate goals since its harmonization impact is recognized across the EU. The GDPR presents as a single set of rules which make the legal compliance simpler and cheaper for organizations to do business (European Commission 2018, 3). Data flow between the EU countries are fostered, which facilitates business development of the single market by allowing organization to contact one data protection officer instead of 28 like before, and only have to deal with one Data Protection Authority (DPA) in most case. The new and strict legislation might be daunting for most of organization at first; however, once the organization implements steps and those standardized requirements to ensure the GDPR compliance, it will be able to make a shift in the process improvements which the impact of necessary changes are minimized to enable bigger opportunities to thrive in the evolving regulatory environment (IT Governance Privacy Team 2017, 5).

4.5 Effect of the GDPR on the Case Company

The case study interview was conducted with a marketing and sales coordinator working in an international SMEs which providing services of trade media such as news, stories and publication on a variety of industry's trusted trade press. The company is operating as an intermediate between the company clients who desire to attract more target audiences, and many industrial press editors who receive specified industrial news and articles of the INS's clients from INS. They are operating in B2B market. That is the reason the target audiences that the clients of INS are looking for are not easy to segment and reach. INS works closely with both its clients and its editorial contacts as well as tries to obtain more clients through marketing and sales effort.

Compared to the results, the case company shared mostly the same view with other B2B SMEs on the changes that the new Regulation – the GDPR has brought recently. Answering the interview, he shared about how his organization know about the GDPR. While most of other SMEs obtain information solely from the European Data Protection Supervisor (EDPS) website, the company had more preparation on legal aspects by consulting with a legal representative. Based on the consultancy from the legal representative, the company could step forward to know how to renew the company's policy to comply with GDPR.

The company is as both the controller and processor of its data. The no involvement from third parties make the firm easier to fully control of the personal data in several stage of collecting, processing and storing. Thus, the risk of processors or third parties' non-compliance can be eliminated. However, the enforcement of the GDPR has imposed burdensome on the business operation. More stringent checks and updates are done frequently in the company handling to cater correctly for people that unsubscribe from communications. The investment on the new software was made to enable better quality of data handling. It also helps as a better mean for individuals requesting their right to access and control the data we store. (Thompson 16 October 2019.)

Based on the company business model that the interviewee shared, the GDPR has significant impacts on their business. As a service provider for their clients, the company has a huge number of contacts. These contacts are clients' contacts and editorial contacts that "INS provides them with articles for their publication based on the principle of their contact data being publicly available with implied purpose of being used for such communications" (Thompson 16 October 2019). This is a risk for the company as there is barely any argument for implied consent for personal data collecting and storing. Any

communications later to that contact might raise questions about consent to them. According to the theorical framework, a valid consent has to be freely given, specific, informed and unambiguous. This is a huge issue within the firm. As being shared by Thompson (16 October 2019) “our ability to achieve complete and explicit consent falls into a slight grey area in terms of using individuals’ data for the means it is intended to be used. We rely on an amount of “good faith” in our communication chain”. In the other hand, this is not a dead end to the company, those contact information is available publicly and the company did not obtain it directly from the individuals. In order to minimize the risk from obtaining invalid consent and being subject to the severe penalties, the company as a data controller must explain the affected editorial persons as the data subject that their personal data was collected from open sources and any information related to the handling of that personal data.

Nevertheless, in order to lower the risk of invalid consent, the company has been focusing on the ability to communicate information with interested parties through its database as well as it updated website. During the meeting, the interviewer and interviewee not only asked and answered the questions, but also expanded the issue to further discussion. Regarding the company’s website, it has been changed and updated a lot to ensure the GDPR compliance. However, in order to obtain explicit and valid consent, the consent pop-up is an effective tool to collect the consent yet handling withdraw consent has to be also considered. The IT Governance Privacy Team (2017, 215) states that “data subject must be able to withdraw consent as easy as they provide it”. From figure 10, although the main page of INS’s website already updated a pop-up asking about using cookies, it is also required to have a set of internet tools to add privacy controls feature to the pop-up dashboard. This will allow the data subject to easily see an overview of relevant processing or just a link to privacy policy of the company attached to the dashboard, as well as enable and disable cookies on the fly.

Figure 10. Main page of INS's website

Obtaining valid consent is one of the most vital steps to offer transparency to the individuals. It is also one of the most onerous requirements from the new legislation according to the results of the research. On the other hand, if the company can show a better transparency on its company's website as the face of the company, there are certainly opportunities to earn trust and enhance the firm's reputation over the others.

6 Conclusion

In conclusion, the enforcement of GDPR changes substantially the way most of the organization handle data. As it imposes many detailed requirements of consent rights and data portability, governance responsibilities and additional liabilities, mandatory breach notification, privacy by design and by default, along with heavy fines for non-compliance on everyone processing the personal data of data subjects residing in the EU, regardless of the company's location or even where the data is handled, the changes might be difficult and challenging, especially for small and medium sized companies mostly due to lack of qualified staff, low budget for preparation of changes and the complexity of law text.

Nevertheless, with some organizations where the awareness and readiness for the GDPR are at the highest from top down across the organization, the GDPR is no longer a difficulty. They grasp it with responsibility and commitment to turn it into potential opportunities of gaining trust and reputation from all stakeholders as well as improving better customer engagement while attracting customers from other firms.

There are possibilities for further research on the same topic but with wider range of respondents instead of only SMEs to have better view of the GDPR impacts. Moreover, the research with the focus on how companies successfully adapted to comply with the GDPR is also a potential suggestion for further research in the future. A detailed guideline can be produced based on that with adequate information, checklists and frameworks in order to ensure the GDPR compliance from initial steps.

It is hard to say that the case company can avoid the risk of obtaining implicit consent since it takes time to deal with the way company sending articles to the editorial contacts for publication. However, the new technology systems that the company has currently operated is a significant improvement of data processing and handling. The systems enable automated tools and manual checks to ensure any request of the rights of individuals is handle correctly, which contributes to achieve the GDPR compliance.

The GDPR cannot be defined as a threat or opportunity, it a current global gold standard for organization to fit in. Indeed, the benefits taken from the successful application of the GDPR requirements in a user-friendly way will be highlighted to overcome the challenges. Its impacts are significant; hence, while the authorities are putting efforts to improve the GDPR more comprehensively and justify some controversy provisions, there is time for

organizations to change their process and technical solutions quickly and accordingly with the Regulation.

References

Barclay, C. 2019. The Road to GDPR Compliance. ISACA Journal: Competing Interests of Privacy and Security, 1(1). URL: http://www.isacajournal-digital.org/isacajournal/2019_volume_1/MobilePagedArticle.action?articleId=1453152#articleId1453152. Accessed: 30 September 2019.

Barclays Corporate Banking. 2019. GDPR: From compliance headache to business opportunity. Reuter. URL: https://www.reuters.com/sponsored/article/From-Compliance-Headache-to-Business-Opportunity. Accessed: 23 October 2019.

Bennett, CJ. 2018. The European General Data Protection Regulation: An instrument for the globalization of privacy standards?. Information Polity. 23. 1-8. 10.3233/IP-180002. URL: https://pdfs.semanticscholar.org/3813/041fc44467933d64c54c3e39a467c2be63c3.pdf. Accessed: 20 January 2019.

Beaumont, S. 18 January 2018. The Data Protection Directive versus the GDPR: Understanding key changes. Software Integrity Blog. URL: https://www.synopsys.com/blogs/software-security/dpd-vs-gdpr-key-changes/. Accessed: 28 September 2019.

Birer, N. 2019. First anniversary of the GDPR: an overview of the changes. EULogos Athena. URL: https://www.eu-logos.org/2019/07/17/first-anniversary-of-the-gdpr-an-overview-of-the-changes/. Accessed: 20 September 2019.

Buttarelli, G. 2015. The General Data Protection Regulation: Making the world a better place?. EU Data Protection 2015 Regulation Meets Innovation Event. Keynote Speech. San Francisco. URL: https://edps.europa.eu/sites/edp/files/publication/15-12-08_truste_speech_en.pdf . Accessed: 9 June 2019.

Commission Recommendation 2003/361/EC. Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises. Official Journal of the European Union, L124, 6 May 2003, pp. 36-41.

Data Protection Directive 95/46/EC. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data

and on the free movement of such data. Official Journal of the European Union, L218, 24 October 1995, pp. 31-50.

General Data Protection Regulation 2016/679/EC. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal of the European Union, L119/1, 27 April 2016.

European Commission. 2018. The GDPR: new opportunities, new obligations. Luxembourg: Publications Office of the European Union. URL: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf. Accessed: 20 September 2019.

European Data Protection Supervisor. 2017. Annual Report 2017. URL: https://edps.europa.eu/sites/edp/files/publication/18-03-15_annual_report_2017_en.pdf. Accessed: 10 June 2019.

European Data Protection Supervisor. The History of the General Data Protection Regulation. URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Accessed: 11 February 2019.

Fagerström, A. 2018. GDPR – from adversity to opportunity. The Startup. URL: https://medium.com/swlh/gdpr-from-adversity-to-opportunity-bbc956911e8a. Accessed: 23 October 2019.

Gantz, D. 2014. The Basics of IT Audit. Syngress.

Hall, S. 2017. Innovative B2B Marketing: New Models, Processes and Theory. 1st ed. Kogan Page Limited. New York.

Identity Theft Resource Center, CyberScout. ITRC Data Breach Report H1 2018, pp. 3-5. URL:https://www.idtheftcenter.org/wp-content/uploads/2018/07/DataBreachReport_2018.pdf. Accessed: 20 January 2019.

Information Commissioner 's Office. 2019. GDPR One year on. URL: https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf. Accessed: 25 September 2019.

IT Governance Privacy Team, 2017. EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide. 2nd Edition. Cambridgeshire. IT Governance Publishing.

Kolah, A. 2018. The GDPR Handbook - A Guide to Implementing the EU General Data Protection Regulation. Kogan Page Limited. London, New York.

Lingard, S. 2017. HR data and GDPR: what you need to know about consent (and why not to rely on it). URL: https://www.hrzone.com/perform/business/hr-data-and- gdpr-what-you-need-to-know-about-consent-and-why-not-to-rely-on-it. Accessed: 18 March 2019.

Lynskey, O. 2015. The foundations of EU data protection law. 1st edition. Oxford University Press. London.

Mathur, N. 26 February 2018. GDPR Compliance: The Challenges and Problems with Personal Data. Neo4j Blog. URL: https://neo4j.com/blog/gdpr-compliance-challenges-personal-data/. Accessed: 20 October 2019.

McKinsey Global Institute. 2016. Digital Globalization: The new era of global flows. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx. Accessed: January 20th, 2019.

Office of Data Protection Ombudsman. 2018. Annual Report 2018. URL: https://tietosuoja.fi/documents/6927448/10717840/Annual+Report+2018.pdf/2cd8a0d3-2241-5c43-a68e-f35f74a40a1b/Annual+Report+2018.pdf. Accessed: 29 June 2019.

OECD. 2013. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed: 28 February 2019.

Ponemon Institute LLC. 2019. The cost of cybercrime. URL: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf. Accessed: 27 October 2019.

Saunders, M. Lewis, P. & Thornhill, A. 2012. Research Methods for Business Students. 6th edition. Pearson Education Ltd. London.

Seshagiri, A. 2013. Claims That Google Violates Gmail User Privacy. The New York Times. URL: https://archive.nytimes.com/www.nytimes.com/interactive/2013/10/02/technology/google-email-case.html. Accessed: 11 February 2019.

Statista. 2019. URL: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/. Accessed: 14 January 2019.

Statista. 2019. URL: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/. Accessed: 14 January 2019.

Statista. 2019. URL: https://www.statista.com/statistics/996456/data-breaches-reported-in-europe-by-country/. Accessed: 20 October 2019.

Sturdy, G. R. 2012. Customer Relationship Management using Business Intelligence. Cambridge Scholars Publishing. Newcastle upon Tyne.

The European Data Protection Board. 2019. GDPR in numbers. Infographics. URL: https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf?utm_medium=social&utm_source=linkedin&utm_campaign=postfity&utm_content=postfity05e1e. Accessed: 20 October 2019.

The European Data Protection Board. 2019. GDPR in numbers. Infographics. URL: https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf. Accessed: 20 October 2019.

The European Parliament and the Council. General Data Protection Regulation. REGULATION (EU) 2016/679. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed: 23 May 2019.

Thompson, C. 16 October 2019. Marketing and Sales Coordinator. Industrial News Services (INS). Interview. Helsinki.

Voigt, P. & Bussche, A. 2017. The EU General Data Protection Regulation (GDPR) A Practical Guide. Springer International Publishing. Berlin.

APPENDIX

Appendix 1. Interview Questions

1. Size of organization (by number of employees)

2. Position in the organization

3. How has your organization obtained information about GDPR?
   Attending seminars or other training
   - By consulting a lawyer
   - On the EDPS website
   - Other, how:

4. When did your organization start preparing for the GDPR?

5. The organization is controller/processor? Does the company have any processor? If yes, as a controller who undertakes more responsibility than the processor, how do you ensure their compliance?

6. What concrete changes have the preparation made for the Regulation compared to previous activities? (technological changes, organizational changes…)

7. Does your company have enough technology tools to ensure a streamlined personal data management lifecycle that will facilitate the maintenance, anonymization, blocking and deletion of the personal data? How do you know those tools will work efficiently when data subject raises their request (to access, to rectification, to object…)?

8. As a marketing coordinator, how much do you think the GDPR changes that way you used to collect, process and store data for marketing purposes?

9. Which of the requirements of the Privacy Regulation do you think will affect your organization the most? Why?

10. Do you generally see regulation as a threat or an opportunity and why?

Appendix 2. Qualitative Questionnaire

Questionnaire on the impacts of the GDPR on businesses

1. Size of organization (by number of employees)

2. Position in the organization

3. How has your organization obtained information about GDPR?

- [ ] Attending seminars or other training
- [ ] By consulting a lawyer
- [ ] On the European Data Protection Supervisor (EDPS) website
- [ ] Other, please specify:

4. When did your organization start preparing for the GDPR?

Questionnaire on the impacts of the GDPR on businesses

5. How do you evaluate the stage of readiness of your organization for the GDPR compliance?

- ◯ Nothing started yet
- ◯ Planning
- ◯ Implementing
- ◯ Fully compliance

6. How significant were the changes in the preparation for the Regulation compared to previous activities? (Please give specific answers for Technology changes; Organizational changes (structure, employees, etc.), Budget, etc.

7. From scale 1 to 4 can you rate these possible challenges for your organization to GDPR compliance?

	Not at all concerned (1)	Somewhat concerned (2)	Moderately concerned (3)	Extremely concerned (4)
Complexity of law	◯	◯	◯	◯
Too little time	◯	◯	◯	◯
Lack of well-qualified employee	◯	◯	◯	◯
Insufficiency of budget	◯	◯	◯	◯
Technology shortage	◯	◯	◯	◯

8. How much do you think the GDPR changes that way you used to collect, process and store data for marketing purposes?

Questionnaire on the impacts of the GDPR on businesses

9. Which of the requirements of the new data privacy Regulation do you think affects your organization the most? Why?

10. Do you generally see the GDPR as a threat or an opportunity and why?