

Impacts of General Data Protection Regulation on Obligations of Finnish Accounting Companies

Farigu Linh



Author(s) Farigu Linh	
Degree programme International Business	
Report/thesis title Impacts of General Data Protection Regulation on Obligations of Finnish Accounting Companies	Number of pages and appendix pages 44+6
<p>In May 2018, the General Data Protection Regulation repealed the Data Protection Directive 1995 and came into effect. The Regulation strengthens data subject rights, and reinforces the obligations of data controllers and data processors. Affecting both small and large firms, it forced every company to review its operation and make possible changes regarding the process of personal data to comply with the law because failing to conform to the Regulation can lead to severe fines.</p> <p>The thesis covers how the General Data Protection Regulation has impacted the obligations of Finnish accounting companies. The purpose of the study is to find out how the new law has impacted on their particular responsibilities on personal data processing. The aim of the study is to figure out how they manage the new law alongside routine work: how accounting firms have prepared, what actions they have taken and what changes they have made.</p> <p>The study consists of a theoretical part and an empirical part. The theory section explains the need for the new law. Then, the main differences between the General Data Protection Regulation and the Data Protection Directive are shown. Moreover, the theoretical part deals with personal data processing, and personal data law in Finland. An overview of the field of accounting and the obligations of accountants in Finland is also included. At the end of the theory section, the theoretical framework is outlined. The empirical section is based on interviews with business owners and experts in the field.</p> <p>The study was conducted through a qualitative approach in the form of interviews. The questions for the interviews were designed based on an internal control framework. Semi-structured interviews were then implemented. Five accounting companies and two associations were interviewed. All of the interviews were recorded and transcribed.</p> <p>The findings show that all of the interviewed companies are well aware of the Regulation. They have made careful preparations and adopted some changes in their companies to conform to the law. A significant amount of working time has been spent on training and learning the Regulation. The whole data processing has been critically reviewed. To handle possible risks, they have prepared some solutions in advance. Contracts, layout of payslips and encrypted messages are major changes in accounting companies.</p> <p>To balance serving the customers and complying with the law, it is necessary to have mutual agreements and to sign contracts with customers beforehand. It is also important to check that the software suppliers of accounting firms comply with the law.</p>	
Keywords General Data Protection Regulation, Data Protection Directive, personal data, Finnish personal data law, Finnish accounting companies, semi-structured interviews	

Table of contents

1	Introduction	1
1.1	Background.....	1
1.2	Research problems and investigative questions.....	3
1.3	Demarcation	4
1.4	International aspect.....	6
1.5	Benefits.....	6
1.6	Key concepts	7
2	Theoretical framework.....	9
2.1	A need for the General Data Protection Regulation.....	9
2.2	Data Protection Directive and General Data Protection Regulation	12
2.3	Personal Data Processing.....	14
2.3.1	Data controller and processor	14
2.3.2	Data subject rights	15
2.3.3	Data disclosure and data storage.....	16
2.4	Personal data law in Finland	17
2.5	Accounting firms and the Regulation.....	18
3	Methodology	22
3.1	Research approaches and ethics	22
3.2	Research design	24
4	Results.....	27
4.1	Reactions of accounting firms towards the new law	28
4.2	Data processes of accounting companies	29
4.2.1	Access of accounting companies to personal data	30
4.2.2	Data storage and data disclosure.....	30
4.3	Actions of accounting firms	32
4.4	Changes in accounting firms	33
4.5	Suggestions	34
5	Discussion.....	36
5.1	Reliability and validity.....	36
5.2	Main results and recommendations.....	36
5.3	Self-reflection on learning	37
	References	38
	Appendix	45
	Appendix 1. Overlay Matrix	45
	Appendix 2. Main Activities Checklist	46
	Appendix 3. A Framework for Interviews: themes, topics and categories	47
	Appendix 4. Justification for Interview Questions.....	48

Appendix 5. Questions for respondents, sent in advance before interview days.....50

1 Introduction

The first chapter explains how the thesis writer chose the topic. After that, the research question and investigative questions are shown. Following that is the demarcation part, which points out what to focus on. International aspect, benefits and key concepts are also specified in this chapter.

1.1 Background

Criteria for a Bachelor Thesis should be researchable within the scope of 15 credits. Moreover, the research should be accessible to collect necessary data. “Ethical, well-grounded, usable, beneficial, topical & timely, innovative, specific, logical & systematic, well – formulated” are other important characteristics of a good research (San Miguel 2015, 19). Based on those evaluating criteria, the author came up with the topic about impacts of General Data Protection Regulation (GDPR) on accounting companies in Finland. The idea came from discussions with teachers from a virtual course: Consolidated and IFRS financial statement.

The meaning of privacy has developed over time. Friedewald and Pohoryles 2013 call it “tension between an individual and the community”. Data protection on the other hand, goes further in meaning because it not only secures personal data but also strengthens the rights of individuals. It is believed that the protection of personal data is a fundamental human right. However, fast-growing technology has violated these rights by collecting, storing and processing data for political reasons, commercial uses, and in the worst case, harmful purposes. (Friedewald & Pohoryles 2013.)

In a Bermuda TEDxTalk, Stuart Lacey emphasized that personal data is an asset that should belong to the individual only. Nonetheless, some large companies exploit the free resource from consumers and build their business empires. Behind their business models are data and advertising. They do it by connecting people with resource to other people who want the resource. Uber, Airbnb, Facebook are no exception. Uber does not own any vehicles, but it exists because it connects people with vehicles to those who do not have ones. Airbnb does not own any accommodation properties but it connects people who have them to those who need ones. Working the same way, Facebook tends not to have content, but it connects people with information to those who want it. In the Internet of things, the data exhaust you leave behind does not disappear. However, big companies can access the data, then sell it for revenue. (Lacey 2015.)

Although some applications appear free, they do really cost something. Users just have to pay by other means of payment for searching Google and contacting friends via Facebook. The price of free applications for customers is economical benefit and revenue stream to other cooperations by selling your data to advertisers. For each advertiser, data subjects are worth some amount of money to Google and Facebook as an old saying goes: if you are not paying for it, you are not the customer; you are the product. (Lacey 2015.)

When the Internet was in its early age of development, the EU had already taken privacy into account and adopted the 1995 Data Protection Directive. However, technology always develops with a speed beyond our imagination, it has transformed our lives immensely. Due to the speed of change, there is a need for privacy law review. (Europa 2018.) Enforced in 1995, the Data Protection Directive aimed to harmonise data processing activities. Despite its good intentions, legal differences among Member States led to legal uncertainty. Processing activities that were permitted in one country could be illegal in other States. Failing to serve its initial goals, there was a need to update the law. (Voigt 2017, 1-2.) Companies are forced to reconsider their data processings to comply with the new Regulation.

Severe consequences will be imposed on companies who fail to comply with the law. For example, an Austrian privacy campaign group has filed complaints against some entertainment streaming giants for insufficiently complying with the law. The privacy campaign group claimed that these companies failed to disclose third parties that receive users' data. The group filed complaints to the Austrian Data Protection Authority. If breaking the law, they have to face the maximum fine of 20 million euros or 4% of their global turnover. (Financial times 2019b.)

At the same time, the Google Limited Liability Company (LLC) has been fined to the tune of 50 million euros by the French data regulator for breaching the General Data Protection Regulation. The company was blamed for suspicious use of personal data. (Financial Times 2019a & CNIL 2019.)

Because the law affects any business that deals with personal data, it raises concern how businesses should prepare themselves to comply with the General Data Protection Regulation. Hence, the next subchapter will answer the question: What to do with it now?

1.2 Research problems and investigative questions

The European Commission 2018c defines that personal data is any data that can identify an individual. Based on personal experiences gained from practical training, the author has learned that accountants work with personal data from clients; for example, names, home addresses, email addresses, social security numbers, bills, receipts, and bank transaction documents.

Since the new law came, it has given more details about data processing. It makes business owners consider the data they collect. Anyone who processes personal data should question themselves what data do they have to collect and for what purposes? How do they store the data? To whom can they share the data with? Moreover, the Regulation also mentions data portability and right to be forgotten. Thus, the company also should prepare to give customers what information they have in their system. In addition, they should prepare for the situation when a client asks to transfer their data to another company or delete their data in the company system. (Regulation on Personal Data 2016/679.)

Based on above concerns, the research question (RQ) is formulated as: How has the General Data Protection Regulation impacted the obligations of Finnish accounting companies? The purpose of the research is to learn how the new law has influenced on accounting companies. The research shows possible differences in companies after the new law and if nothing changes, then why? At the end, the thesis writer suggests recommendations to those who want to become accountants so that they have some ideas about an accountant's working life. For those who are working as accountants, they will have more fresh insights into the topic and the working field. To achieve the goal, the research question is divided into the following investigative questions (IQ):

Table 1. Research question and investigative questions

RQ. How has the General Data Protection Regulation impacted the obligations of Finnish accounting companies?
IQ 1. How have Finnish accounting companies reacted to the new law?
IQ 2. How have Finnish accounting companies prepared to comply with the new law?
IQ 3. What changes have been made in Finnish accounting companies due to the new law?
IQ 4. What recommendations do accountants have for other accountants in Finland to comply with the GDPR?

1.3 Demarcation

The purpose of demarcation is to mark the areas that the thesis covers.

In both bad and good times, every business needs accountants and accounting is a source of many jobs. To develop a career in accounting, it is an important step in the career planning process to know the industry and working life. For those new to accounting, it is worth knowing what a working day of an accountant is like and what to expect of the workload. The more you are aware of the responsibilities, and what needs to be done, the more productive your working day will be. The more you get to know the industry environment, the easier you adapt to the new environment and set yourself up for success.

Finland is the focus of the thesis because it is where the author resides and has working experiences in accounting companies. Based on interviews with established companies in Finland, this thesis looks at accounting from a GDPR perspective. In light of the GDPR, the thesis goal is to find out how the new law has generally impacted the working days of accountants and their particular responsibilities on personal data processing. In short, the purpose is to figure out how Finnish accounting companies manage the new law alongside the routine work.

The connection between the law and accounting is that accountants work with personal data from customers while the GDPR is about personal data. Due to the Brussels effect of the new Regulation, accounting companies need to comply with the law based on the accountability principle of the law. When handling personal data, accounting companies comply with the law by: following instructions of data processing from data controllers, updating contracts with data controllers, paying attention to purpose limitation of data processing, data disclosure, storage limitation, integrity and confidentiality.

According to European Commission 2018d, the new rule applies to all companies that process personal data in their business activities. No matter how large the company is, if it uses personal data in its process, it should follow the new Regulation. Through discussion with a financial assistant from a Finnish organisation, the thesis writer noticed influences of the GDPR to a certain extent. The organisation deals with a large amount of data from clients. In the first interview, the financial assistant shared her opinion about the GDPR. She thought that there would not be much changes because the organisation had its own rules related to privacy matters of clients. Failing to follow the rules, one can lose one's job. A few days after the first discussion, she contacted the thesis writer again. She told

the thesis writer that her organisation offered GDPR training to their staff in order to pass a test that they required. From the short interview with her, the thesis writer learned that the GDPR affected a large firm, which led to concern for other smaller companies. If a large organization which deals with a lot of data from clients has been affected, what about other accounting companies?

According to Eurostat 2018, micro companies are those who have less than 10 people. Sharing the same standard, Tilastokeskus and Taloushallintoliitto also define micro companies as businesses where there are less than 10 employees. Additionally, the final value of the balance sheet can reach 350 000 euros and revenue up to 700 000 euros (Accounting Act 1620/2015 & Taloushallintoliitto 2018a). Moreover, until March 2018, 93,3% of companies in Finland had less than 10 members of staff (Yrittäjät 2018).

When it comes to the number of accounting companies, there are more than four thousand firms in Finland (Taloushallintoliitto 2018b). For those companies who belong to Taloushallintoliitto, 37% of companies had 1 to 9 members of staff (Taloushallintoliitto 2018). Based on statistics related to the size of companies and accounting companies, the author prioritised micro companies. An interview with another bigger company was conducted after completing interviews with micro firms.

Furthermore, those companies who are outside Finland, but still in the EU and offering accounting services to EU customers are not the main target of the study. Moreover, companies that are located outside the EU and serving customers outside the EU are not affected by the GDPR (European Commission 2018d). As a result, the study does not cover that either. The table below will point out the main area that the thesis writer targets to study.

Table 2. The scope of the thesis

Within the scope	Out of the scope
<ul style="list-style-type: none"> - Finnish companies that are located in Finland and offering accounting services to customers in Finland. 	<ul style="list-style-type: none"> - Companies that are in Finland and offering services to customers in other EU countries. - Companies that are in Finland and offering services to customers outside the EU. - Companies that are in other EU countries and offering services to EU customers. - Companies that are in other EU countries and offering services to customers outside the EU. - Companies that are outside the EU and offering services to customers outside the EU.

1.4 International aspect

The law affects every company residing in the EU and serving EU citizens. Even companies who are outside the EU selling products or services to the EU are also affected. All companies who want to provide products or services to the EU must comply with the new Regulation. (European Commission 2018a.) If failing to comply with the new law, companies must pay a fine of up to 20 million euros or 4 % of annual revenue (European Commission 2018b).

Since the law came to effect until the beginning of 2019, there have been altogether 206 326 national cases from 31 European Economic Area (EEA) countries. Among those national cases, there have been up to 94 622 complaints and 64 684 data breach notifications. Out of national cases from 23 EEA countries, 52% of the cases has been closed while 47% ongoing and 1% appealed. The imposed fine from Supervisory Authorities of 11 EEA countries reached the value of € 55 955 871 in total. (European Data Protection Board 2019.)

Due to the global impacts of the GDPR, international aspect in GLOBBA theses is met.

When it comes to Finland, the Office of the Data Protection Ombudsman has participated in 22 cross-border cases with other supervisory authorities. It is estimated that there might be over 11 000 cases in total during the year. 3 100 cases have been reported to the Data Protection Office in Finland until April 2019. Out of those cases, there have been 1 050 personal data breach notifications. Most of those personal data breach cases relate to Office 365 and phishing messages. (Tietosuoja 2019.)

1.5 Benefits

In theory, complying with the law secures trust. Thus, companies can keep business contracts. Moreover, companies can receive good branding and reputation. Following the rules prevents fines and legal fees. (Kolah 2018, 87.) With new legal framework, citizens have reinforced rights. It is a win-win situation because if it benefits citizens, then in return, it benefits businesses. Companies can save time and resources. For one continent, there is now only one law. Companies can work with One-Stop-Shop rule: one supervisory authority instead of dealing with every single Member State law. It is estimated that €2.3 billion will be saved each year. (European Commission 2018.)

In addition, Lambert (2018, 26 - 27) says that the new law offers opportunities for companies to stand out in the market. Moreover, in a benchmarking survey of Deloitte, many respondents saw possible benefits as a result of the law. Some view it as an advantage for reputation and competition. (Deloitte 2018, 2-4.) Sharing the same belief, KPMG also mentions opportunities behind the law. If it is appropriately applied to the company strategy, the company can get a competitive edge. (KPMG 2017, 3.)

When it comes to the thesis, the benefits of the study are the results that answers the investigative questions. Furthermore, it is important because complying with the new law and regulation is one of the ethical principles and standards required for accountants (Braun & Tietz 2013, 13-15). Because the law is current, the topic itself is interesting to the author. Thus, there was motivation to complete the thesis from the beginning to the end. Moreover, it benefits those who want to become accountants and who are now accountants.

Those students who choose accounting as their careers will get more profound knowledge about the field and the topic. Given limited materials written in English about accounting in Finland, let alone the Regulation in accounting, the thesis is mainly written in English. The result partly contributes to the career planning process in Finland and broadens knowledge about the Regulation. The thesis is an attempt to fill the gap of available resources in English about the working life of accountants in Finland.

Those who have been working as accountants can have more fresh insights into the industry, as following the law always go along with doing accounting. Therefore, the topic is beneficial to working life and professional competencies' development.

The study is also important for the thesis writer because she can learn and get more experiences. The thesis writer will share the results to some accountants that she knows and all the interviewed respondents.

1.6 Key concepts

GDPR is the updated law developed from Directive 95/46/EC. GDPR stands for General Data Protection Regulation. Adopted in 2016, the new Regulation came into force in May, 2018. The purpose of the new Regulation is to harmonise and protect European citizens' personal data. As a result, it affects the operation management of any companies regarding data management, for example consent, right to access, right to be forgotten, data portability, and data breach notification. (Regulation on Personal Data 2016/679.) Because the GDPR is a regulation, the Regulation is used to refer to the GDPR in this thesis.

Directive 95/46/EC was adopted to protect privacy as well as personal data processing and movement for European citizens (Directive 95/46/EC). It was repealed by the General Data Protection Regulation (Regulation on Personal Data 2016/679).

Data Controller is the party that has personal data. The data controller has a right to choose how and why data should be processed (European Commission 2018f).

Data Processor is a third party that takes care of activities for data controller companies. The data processor processes data on behalf of the data controller (European Commission 2018f).

Personal data is the data that can identify an individual (European Commission 2018c). It is any information that can be traced to a natural person (data subject), for example name, identification number, and location data (Regulation on Personal Data 2016/679).

Accounting firms are companies that offer accounting services to other customers. According to common agreements with customers, accounting firms are responsible for bookkeeping, financial statement preparation, tax reports and payroll. Accounting companies can offer also managerial accounting services. (Talouhallintoliitto 2018c.)

2 Theoretical framework

The second chapter presents the literature review. It starts with the data protection law in the past, which is Data Protection Directive, then the General Data Protection Regulation. Comparison between the two laws is made to see development from the former to the latter law. The principles of both the Directive and the Regulation are demonstrated. Then, the next subchapter expands on lawful personal data processing. The obligations of data controllers and data processors are explained. Data subject rights are identified. Moreover, it also covers how to disclose and store personal data. Updates of the Finnish personal data law, from Personal Data Act 523/1999 to Data Protection Act (1050/2018) are shown in the following subchapter. The last subchapter gives an overview of the field of accounting and the obligations of accountants in Finland. Then, the theoretical framework is outlined at the end of the chapter.

2.1 A need for the General Data Protection Regulation

The foundation of the current privacy law dates back to the 20th century when the Organisation for Economic Co-operation and Development (OECD) had a program on transborder data flows. After many years of activities, the OECD Council proposed Guidelines, also known as a Recommendation. Developed by a group of government experts with the intention of supporting basic human rights, it was adopted on 23 September 1980. (OECD 2013.)

Then, in 1995, Directive 95/46/EC was adopted to harmonise basic privacy legislation. As stated in Article 1 of the Directive, its purpose is to secure fundamental privacy rights and related data process. The Directive had six principles as stated in Article 6. (Directive 95/46/EC.)

First of all, the data process had to be processed pursuant to the law and consents of the data subjects. Secondly, only legitimate purposes were allowed to collect personal data. Thirdly, data collection had to be sufficient and relevant. Fourthly, every citizen had a right to access to edit or delete the data. For storing purposes, data had to be kept for a period of time of lawful purposes. When the time expired, it had to be deleted. Otherwise, it had to be securely kept for historical, statistical and scientific purposes. Finally, the controller had to measure its compliance. Moreover, Article 12 of the Directive 95/46/EC stated that all data subjects were allowed to know whom their data is disclosed to. (Directive 95/46/EC.) Those basic and essential principles still remain in the General Data Protection Regulation.

However, Voigt (2017, 2) states that the 1995 Directive did not match up with current business environment. In the past, supervisory authorities worked independently in cross-border cases. Under Directive 95/46/ EC, the Directive was differently interpreted because of legal differences in EU countries. As a result, companies that operated in several countries could face conflicting decisions from local authorities. (Voigt 2017, 2.) Back to the time before the GDPR, this problem arose, for example, when the Court of Justice handled the Weltimmo case.

Weltimmo was a company that was registered in Slovakia. However, it operated in Hungary. The company offered a property advertising website in Hungary, thus, it was responsible for processing data of the advertisers. According to the company, it was free to post advertisements in a one-month-period, but it was chargeable for a fee after that. The advertisers informed the company by email to delete their advertisements and their personal data from that period. Nevertheless, the company did not take actions that the customers would have liked. Instead, the company charged the advertisers and forwarded the data of those advertisers, who did not pay, to debt collection agencies. The advertisers filed complaints against Weltimmo to the Hungarian data protection authority. The company was imposed a fine of 10 million Hungarian forint, which equalled about 32 000 euros for breaching the country's law. (Court of Justice of the European Union 2019.) In accordance with Directive 95/46, Article 4 (1) (a) stated:

“Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;”

On the one hand, Weltimmo appealed and argued that the Hungarian data protection authority was not competent in this case. To Weltimmo, the company was established in another Member State. Weltimmo reasoned that the Hungarian data protection authority could not apply their law on their case. Based on Article 28, Weltimmo argued that the Hungarian authority should have contacted the Slovakian authority. (Court of Justice of the European Union 2015.) Article 28 (6) of Directive 95/46 stated:

“Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the

powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.”

On the other hand, to the Hungarian data protection authority, Weltimmo had a Hungarian representative in Hungary, also known as one of the owners of the company. Although its Internet servers were installed in another Member State, the owner lived in Hungary. It had a bank account in Hungary and a letter box in the country for daily business affairs. Their website was written in Hungarian and subject to advertisers that had properties located in the country. Thus, Weltimmo had a “real and effective activity” in Hungary. Following the same Article 28, the Hungarian authority was of the opinion that it had jurisdiction and competence to act. (Court of Justice of the European Union 2015.)

Prior to doubts regarding applicable law and power extent of Hungarian data protection authority under Article 4 (1) and Article 28 of Directive 95/46, the Hungarian Supreme Court referred the matter to the Court of Justice. It was questions of interpretation and establishment that brought the case further to the Court of Justice. The case continued after that and ended in 2015. (Court of Justice of the European Union 2015.)

The above example of the Weltimmo case showed that there was a lack of mutual understanding and interpretation of the Directive. It was a problem because the same legal text led to divergent understandings. Thus, instead of fragmentation across each Member State, there was a need for a new law, that could offer more legal certainties (Voigt 2017, 2).

In light of the GDPR, data controllers and processors who operate in more than one Member State choose one lead supervisory, where the main establishment of the business is located. The responsibility of the lead supervisory is to lead the procedure and work with other supervisory authorities to reach general agreement. The new regulation gives opportunities to supervisory authorities from different Member States to have joint investigations. The new mechanism can help companies to save time due to consistency in decision making from authorities. (European Data Protection Board, 2018.)

2.2 Data Protection Directive and General Data Protection Regulation

In comparison between the two laws, the former is a directive while the latter is a regulation. A directive is a legal goal that all EU countries aim at. It leaves some room for each EU country to transpose it into its national law first, then to decide on how to apply the law to reach the goal. However, a regulation is more legal binding. When a regulation is made, it must be simultaneously applied in every EU country. (Europa 2019.)

Developed from Directive (in total 34 Articles) to Regulation (in total 99 Articles), the new law works on seven principles as stated in Article 5 of the General Data Protection Regulation: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; accountability; integrity and confidentiality. Integrity and confidentiality is the new part in the principle of GDPR. Back then, it was mentioned that data should be kept with appropriate safeguards, but now data should be processed with technical and organisation measure to ensure security. Compared to the former law, transparency was not mentioned in Article 6 about personal data process principles of the Directive 95/46/EC. However, there are now seven principles and transparency has its place in the first principle.

As a matter of fact, transparency is a crucial principle. It is important as it is one of the reasons why CNIL imposed a fine of 50 million euros on Google LLC. The example of Google LLC with CNIL shows that lacking transparency can cost a fortune. Right after the law came to effect, on 25 and 28 May 2018, the French National Data Protection Commission (CNIL) received complaints from two associations, consisting of None Of Your Business (NOYB) and La Quadrature du Net (LQDN). After investigating the case, the French authority imposed a fine on Google LLC for lacking transparency and legal basis for processing personalized advertisements. It was blamed for lacking transparency because users had been insufficiently informed how their data was collected for personalized advertising. Purpose of data processing, storage period, and data categories for advertisements were given in a vague manner and spread through many documents.(CNIL 2019.)

When it comes to the rights of the data subject, their rights were limited in the Directive 1995. Nonetheless, there is now a whole chapter about data subject rights, including 12 Articles. (Directive 95/46/EC & Regulation on Personal Data 2016/679.) There was no such position as Data Protection Officer in the past. Now the position is needed for any company which has more than 250 employees.

Moreover, in the past, there was no clear instruction on the breach of data. With the new law, if an incident happens, it should be reported within 72 hours. Directive 1995 had Article 24 about sanctions, but showed no specific penalty. However, in case of infringement, as stated in Article 83 of the GDPR, a fine of 10 000 000 euros or 2% of the company's annual turnover and up to 20 000 000 euros or 4% of the company's annual turnover will be imposed. (Directive 95/46/EC & Regulation on Personal Data 2016/679.)

To summarize the distinguishments between the two laws, the table below shows the main differences between the Data Protection Directive and the General Data Protection Regulation.

Table 3. The summary of the main differences between the two laws

Areas of comparison	Data Protection Directive	General Data Protection Regulation
Type of legal document	Directive	Regulation
Number of Articles	34	99
Principles for processing of personal data	There used to be 6 principles.	There are 7 principles and transparency has its place in the first principle.
Personal data process	Data should be processed with appropriate safeguards.	Data should be processed with technical and organisation measure to ensure security.
Data subject rights	Rights for data subjects were limited.	Rights for data subjects are enhanced.
Data breach	The instruction was vague.	Reports should be made within 72 hours.
Data Protection Officer	It was unnecessary to have the position.	The position is needed in some cases.
Penalty	Sanctions were mentioned in Article 24 but no specific amount of penalty was shown.	A fine of 10 000 000 euros or 2% of the company's annual turnover and up to 20 000 000 euros or 4% of the company's annual turnover will be imposed for breaching the law.

2.3 Personal Data Processing

The subchapter expands on the obligations of data controllers and data processors. Moreover, data subject rights are also explained.

2.3.1 Data controller and processor

In light of the Regulation on Personal Data 2016/679, the new rule concerns different parties, such as data controllers and data processors (Lambert 2018, 62-63).

According to the Regulation on Personal Data 2016/679, Article 4 (7) defines that the data controller is a legal entity that has power on deciding how data should be processed. On the other hand, the data processor is a separate entity that processes personal data on behalf of the data controller as mentioned in Article 4 (8). For example, if a retail company outsources accounting tasks to an accounting company, then the retail company is the data controller and the accounting company is the data processor.

Pursuant to Article 24 of the Regulation on Personal Data 2016/679, the data controller is responsible for purposes of processing. When outsourcing services to other parties, companies should keep in mind clear contractual documents (Lambert 2018, 241). Article 28 of the Regulation on Personal Data 2016/679 states that the processor should assist the controller to process data according to the Regulation. To govern the processing, there should be a contract between the processor and the controller. The contract will give the instructions to both sides about the purpose, nature and duration of the processing. Explanations on why, when, how data is collected, processed and stored are also important (Lambert 2018, 65). It also means that consent is a key word to keep in mind before collecting any data (Tieto 2016, 7).

Article 4 (11) of the Regulation on Personal Data 2016/679 states that consent is “any freely given, specific, informed and unambiguous indication of the data subjects’ wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to processing of personal data relating to him or her”. It means that before any processing, there must be permission to process personal data from data subject for specific purposes as stated in Article 6, (1a) of the Regulation on Personal Data 2016/679. As the data subject has a right to give consent, so does he or she have a right to withdraw according to Article 7 (3) of the Regulation on Personal Data 2016/679. In short, the data processor operates according to instructions given by the data controller and permission from the data subject. In case the processing is involved with other processors, the same law is applied to other processors pursuant to Article 28 of the Regulation on Personal Data 2016/679.

Records of processing activities are suggested (Lambert 2018, 239–240 & Tieto 2016, 6). It means that both controller and processor should keep a record related to data processing. According to Article 30 (1) of the Regulation on Personal Data 2016/679, a record of the data controller should have contact details of the controller's representative, and reasons for the processing. The record also answers the following questions: how long the data is stored for, who is the data is disclosed to, and what measures are to be taken to ensure security. Like the data controller, the data processor also keeps a record of activities as stated in Article 30 (2) of the Regulation on Personal Data 2016/679. The record of the data processor covers contact details of both data controller and data processor. It answers questions of what activities the data processor carries out for the data controller, who has access to the data and what security measures have been done.

2.3.2 Data subject rights

The Regulation on Personal Data 2016/679 is the law about personal data, so it is important to know what the law affects. According to Chapter 1, Article 4 of the Regulation, personal data is defined as any data that can be traced to a natural person, for example, name, social security number, and location data. (Regulation on Personal Data 2016/679.) It means that company information is not personal data. In other words, company information is not affected by the law. Instead, the Regulation applies to data concerning a person, for instance, name, address and phone number. (Hanninen, Laine, Rantala, Rusi, & Varhela 2017.)

Personal data should be processed according to the seven principles in Article 5 on the Regulation on Personal Data 2016/679. As the first principle mentions, there are three things to remember: lawfulness, fairness and transparency. Before any data collection, data subjects should be aware of the data process.

Pursuant to the Regulation on Personal Data 2016/679, Article 13 (1) lists the rights of data subjects. The data subject should know why the data is processed and to whom the data is disclosed. As stated in Article 5 (c) of the Regulation on Personal Data 2016/679, the collected data should be relevant to the purpose of the processing. In other words, data collection should be sufficient for the purposes, nothing more and nothing less.

With a higher standard of transparency, the data subject should be able to perceive the data processing. Article 12 of the Regulation on Personal Data 2016/679 further explains that clear and plain language should be used to communicate with the data subject. In

other words, the data subject should understand what activities are happening regarding the data and how they affect the data subject (Voigt 2017, 88).

Moreover, the data subject has a right to access the process. If the data subject makes a request, he or she can receive in-depth information concerning him or her as stated in Article 15 of the Regulation on Personal Data 2016/679. It means that the data subject can know what is going on with his or her data. The data subject has a right to rectify, erase and restrict the processing pursuant to Article 16, 17 and 18 of the Regulation on Personal Data 2016/679. Additionally, according to Article 20, the data subject has a right to transmit the personal data to other controllers. This provides the data subject with more flexibility to change the data controllers and processors (Voigt, 168). In addition, the data subject has a right to have a copy of the data processing. It should be free of charge. However, if the data subject continually asks, the data controller can charge a fee in accordance with Article 12 (5) of the Regulation on Personal Data 2016/679.

2.3.3 Data disclosure and data storage

During data processing, only authorised disclosures are accepted. Data controllers, data processors, and public authorities are allowed to access the data. Public authorities include tax and customs authorities as stated in Recital 31. Like data controllers and processors, public authorities also need to follow the Regulation when processing the data (Regulation on Personal Data 2016/679).

As mentioned earlier, accountability is one of the data processing principles. It requires the controller to prove that their operation follows the Regulation. Certain measures are needed and a new position is suggested to audit compliance measures. Under Article 37, 38 and 39 of the Regulation on Personal Data 2016/679, Data Protection Officers are responsible for training employees, monitoring performance and communicating with data subjects or other supervisory authorities.

Integrity and confidentiality are data processing principles that ensure security and lawful access. Article 32 of the Regulation on Personal Data 2016/679 suggests technical and organisational measures. A good IT security system is recommended, such as encrypted data or pseudonymous data. Lambert (2018, 301–303) states that regular testing is needed to ensure ongoing confidentiality and minimize the risk of breach the law as stated in Recital 29 and 83 of the Regulation on Personal Data 2016/679. Another good rule to keep in mind is purpose limitation. If the data is no longer needed, then it should be deleted, except for historical or statistical research as mentioned in Article 5. (Regulation on Personal Data 2016/679.)

In case there is a high risk of data breach or in the worst case, if data breach happens, the data subject has a right to know according to Article 34. Clear and plain language should be used to ensure that the data subject can fully understand the situation (Regulation on Personal Data 2016/679).

2.4 Personal data law in Finland

Personal Data Act 523/1999 shared some similarities with the Directive 95/46/EC. It covered fundamental rights of data subjects: data processing, data transfer and secure data storage (Finlex 1999).

According to the Personal Data Act 523/ 1999, Chapter 1, Section 3, personal data was defined as any kind of information that could lead to a person or anyone else in their household.

Chapter 2 of the Personal Data Act 523/ 1999 listed how personal data should be processed. Before any collection, the data subject had to give consent. The data subject was allowed to access a description of the data process. It included information on the controller, purpose of the process and the destination of data disclosure. The data subject had a right to know if the data was treated with security. Moreover, they had a right to access and update the data according to Chapter 6, Section 26 and 29 of Personal Data Act 523/1999.

Data was only allowed to be transferred to other territories if there was adequate level of data protection as stated in Chapter 5 of the Personal Data Act 523/ 1999. The data type, purpose and process had to be evaluated. It includes data destination, legal provision, code of conduct and security measure as stated in Section 22 of Chapter 5 of the Personal Data Act 523/ 1999.

In case the data was used for marketing purposes, the data subject could reject the data process. During the data process, security was a priority. Organisational and technical measures had to be carried out as stated in Chapter 7, Section 32 of the Personal Data Act 523/ 1999. The data had to be deleted when it was unnecessary as stated in Section 34 of Chapter 7 of the Personal Data Act 523/ 1999. For the purpose of inspection, Chapter 9 of the Personal Data Act 523/ 1999 stated that data protection authorities in Finland were allowed to access personal data. (Finlex 1999.)

Due to the Regulation on Personal Data 2016/679, the Personal Data Act was updated. The proposal HE 9/2018 vp was sent to the Parliament in March 2018 and confirmed in December 2018 (Eduskunta 2018a). As a result, the Data Protection Act (1050/2018) came into force on 1 January, 2019 and repealed Finnish Personal Data Act (523/1999). It is applied in parallel with the Regulation on Personal Data 2016/679. Some significant changes were made to the guidelines on processing personal identity number, health data and sanctions. An age limit for information on children was also introduced. Article 8 of the Regulation on Personal Data 2016/679 forbids processing data of children under the age of 16. However, it has been proposed that the minimum age be dropped to 13. Like the Regulation on Personal Data 2016/679, the Finnish law also shares similarities on data subject consent and access of official authorities. Personal identification numbers can be processed by insurance, payment services, debt collection agencies and in the financial sector. (Regulation on Personal Data 2016/679, Oikeusministerio 2018 & Eduskunta 2018b.)

2.5 Accounting firms and the Regulation

In theory, accounting offers various job opportunities. There are many skills required from those who study accounting. They are expected to manage data programs, payroll rules, common collective labor agreements and tax issues. Working as accountants, they are supposed to do daily bookkeeping and prepare financial statements. They are expected to have the ability to make different reports, and send them to the tax authorities. Accountants have to examine those reports, then explain to the customers. Those who work for accounting companies are required to understand their customers' businesses, so that they can offer consulting services such as solutions for customers. In some cases companies have to assess and change their systems because traditional working methods do not match up with present challenges. (Jormakka, Koivusalo, Lappalainen, Niskanen 2016, 14; Koivumäki & Lindfors 2012, 11.) Furthermore, accounting has countless rules and regulations to work with. During busy periods, accountants are expected to double check every number. (WetFeet 2003, 2.)

For a long time, bookkeeping and payroll have been common services offered by accounting companies to other firms (Koivumäki & Lindfors 2012, 26). According to Taloushallintoliitto, accounting companies can offer full accounting service or parts of it (Taloushallintoliitto 2018c).

In some cases customers can handle their papers by themselves, then the information goes automatically to the accounting companies via e-financial cloud service so that they

can do the rest. (Koivumäki & Lindfors 2012, 11.) For example, when an association outsources to an accounting company, the responsibilities are divided. It is a process that requires work on both sides. On the one hand, an accounting manager prepares materials for payroll, collects working hours and employees' tax cards, then forwards them to an accounting company. On the other hand, the accounting company is responsible for payroll, bookkeeping, accounts receivable, sales invoices and purchase ledgers. When the accounting company complete the payroll, then they just need to send to the customer and attach the payments. (Finne 27 February 2019.)

Personal data is mainly used for payroll and tax purposes, for example, tax cards and bank account numbers (Lahti and Salminen 2014, 143). In some exceptional cases, identity number is used for legal issues to identify an individual. (Mattinen, Parnila & Orlando 2017, 299 - 301.) The legal issue can be related to the Act on Detecting and Preventing Money Laundering and Terrorist Financing. According to Act 406/2018, Chapter 3, Section 1 and 3, customers should be identified. All documents about the customers should be kept for five years. Information about customers includes name, date of birth, social security number, and address as well as information about registration and beneficial owners. (Finlex 2018.)

Some documents or reports have to be stored from 6 to 10 years. Any attachment that relates to business activities can be saved 6 years from the ending of the financial year. Financial statement, and charts of account can be stored up to 10 years. (Talloushallinto-liitto 2018d.) A tax card is valid within the tax year while tax notifications and other related attachments can be stored for 6 years. Moreover, there should be different places for health-related documents and accounting materials. (Mattinen, Parnila, and Orlando 2017, 304-306.)

In large accounting companies, many accountants can work together at the same time. One accountant may have to work with value added tax rates and record the same purchasing account repeatedly. Although the job is monotonous, it can be diverse. Working as an accountant does not mean isolation, but interaction with others. Accountants are responsible for preparing financial statements, calculating salaries, making reports, following the customer companies' results and revenues. In addition, accountants have to communicate with customers to interpret and explain their financial situations to them. (Simonen 8 February 2019.)

In a medium sized company, there can be some financial representatives who support customers' operations. They suggest solutions to customers' business problems. There

can be also another specialist leader who is responsible for commissions, arrangements and internal issues. For example, since the Regulation on Personal Data 2016/679 came to effect, the specialist leader has been responsible for training employees. (Paasi 25 February 2019.)

In large and medium sized companies, accounting tasks can be assigned to many people. However, for a sole proprietorship, the accountant is an entrepreneur who takes care of everything. When the law came, the entrepreneurial accountant had to read and learn the new rules. (Sirkiä 4 March 2019; Niemelä 15 February 2019 & Niemelä 20 February 2019.)

When personal data is processed, it is important to know the roles of data controllers and data processors as well as their responsibilities regarding data subjects. There should be clear instructions among parties. (Mattinen, Parnila, & Orlando 2017, 304-306.)

In reaction to the Regulation on Personal Data 2016/679, accounting offices and customers should prepare written agreements together. Some updates should be added, including reasons for the updates, nature and purpose of data processing. It is important that the data controllers and processors act according to agreed contracts. It causes more work to do and it might seem burdensome, especially to micro, small, medium-sized companies. However, there are no other choices but taking actions to comply with the law (Fredman 2018.)

Based on the above theory about the Regulation, the following framework shows relevant obligations that apply to the accounting companies in this thesis.

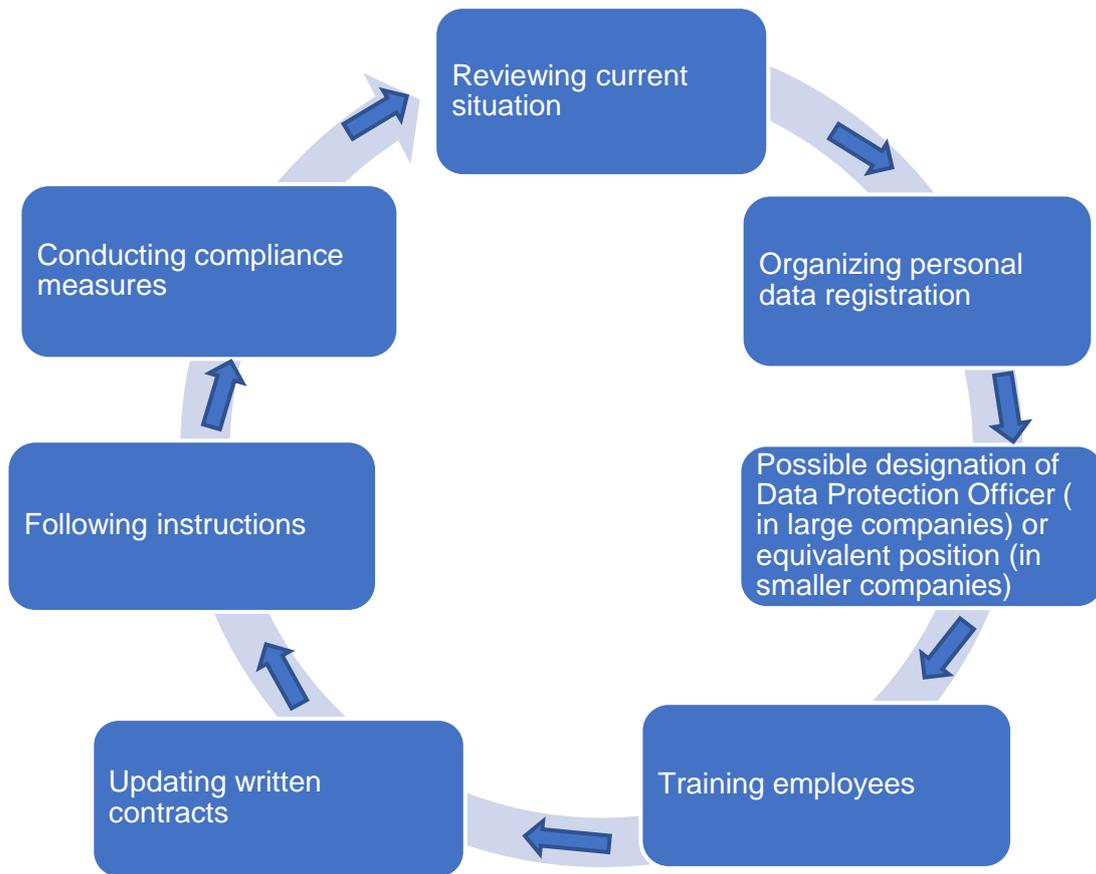


Figure 2. Framework of the GDPR and the accounting companies' relevant obligations on personal data processing (applied from Andreasson, Riikonen and Ylipartanen 2019, 91)

3 Methodology

The third chapter presents how to approach the research question from different perspectives. Research approaches and research ethics are explained. The research design is presented at the end of the chapter. The interviews' framework and justification for interview questions are attached in the appendix.

3.1 Research approaches and ethics

As a matter of fact, the research method is determined by the nature of the research. It means that the research objectives define how it should be done. Implementing a research can be looked from different perspectives, including research philosophies, approaches, purposes and strategies (Saunders & Lewis 2012, 129).

In accordance with Saunders & Lewis 2012, there are four common research philosophies. Positivism focuses on the study of cause and effect to make predictions so that companies can have better control over variables. Interpretivism concentrates on social phenomena, which helps researchers understand what is going on in a company. Realism investigates more profound structures and relations to find out what is beneath the tip of the iceberg in social reality. Pragmatism supports mixed methods, for example in one study, it is possible to have two different methods, qualitative and quantitative. (Saunders & Lewis 2012, 104–107.) The objective of the thesis is to study how the new law has affected accounting firms and to understand their obligations which explain organizational behaviour of companies to comply with the new law. Therefore, the objective matches with interpretivism.

Two common research approaches can be named as deduction and induction. While deduction tends to test existing theories, induction develops new theories. On one hand, in deductive studies, researchers explain relevant and connected relations of variables. On the other hand, induction has an emphasis on closer understanding of the research area. (Saunders & Lewis 2012, 108-109.) Because the thesis provides deeper knowledge and fresher insights into the accounting field, the purpose of the thesis matches the inductive approach.

Saunders & Lewis 2012 explain different types of studies, including exploratory studies. Its aims match the aims of the thesis. Saunders & Lewis 2012 mention that this type is suitable for new phenomena. It is appropriate for this study because the Regulation is the new law. An exploratory seeks fuller understanding of an issue, which matches this thesis objective: to gain a better understanding of the Regulation from viewpoints of accounting

firms. Moreover, an exploratory study is carried out using qualitative methods or interviews. (Saunders & Lewis 2012, 110.)

In addition, qualitative and quantitative methods are common among researchers. Quantitative methods give answer to the questions: where, who, how much, and how often. In contrast, qualitative methods answer to questions: why, what, and how. While quantitative methods give result in numeric format, qualitative methods highlight on phenomena exploration. It is used when there is limited knowledge of the subject. (Kananen 2011, 37-42.) Based on the purposes of quantitative and qualitative methods, a qualitative method was chosen because its purposes were suitable for the thesis objectives. The table below summarises chosen approaches of the thesis.

Table 3. The research approaches of the study

Perspectives	Factors
Research philosophy	Interpretivism
Research approach	Induction approach
Research purpose	Exploratory study
Research strategy	Qualitative

When implementing the research, the writer paid attention to research ethics. She contacted the companies that were affected by the Regulation and appropriate respondents that were able to answer the investigavtive questions.

When contacting companies, the writer tried to be as clear as possible about the topic and required time. The author sent emails to the accounting companies. In some cases, phone calls were made. When contacting companies, she mentioned the purpose of the study and that the research results could offer other students and accountants more knowledge on the influences of the Regulation and possible changes in accounting companies. Research is time consuming for companies' employees (Eriksson & Kovalainen 2016, 33). Thus, it was understandable that participation from companies was voluntary.

A list of questions was sent to the interviewees before the interview day so that the interviews could go smoother. Respecting other researchers' work was crucial, thus all the references were done according to the school guidelines. (Eriksson & Kovalainen 2016, 55 - 77.)

3.2 Research design

The research design was created based on research approaches and investigative questions. In the first phase, the thesis writer searched for reliable materials, prioritised and learned about relevant theory.

Secondary research was done by learning the Data Protection Directive 1995 and the Regulation on Personal Data 2016/67. The purpose was to learn the foundation of the personal data law. The author learned the similarities of those laws and the development from the former to the latter law: problems the Directive 1995 caused and why there was a need for the new Regulation. Finnish Personal Data Act 523/1999 and Data Protection Act (1050/2018) were mentioned. The author noticed how the personal data law affected accounting companies. She read books and articles about what kind of services accounting companies offered, what personal data they needed, what purposes they needed it for, to whom they shared the data and how they stored the data. Evaluation, comparison and linkage of theory were made to create the theoretical framework.

To understand the impacts of the Regulation on obligations of accounting companies, the answers from respondents covered:

- The proof of being experts in the field that had knowledge about the subject: years of experience, positions and responsibilities and sources of information about the Regulation.
- Impacts on current financial situation: what benefits and challenges the law bring.
- Impacts on preparations to conform to the law: accounting companies' access to personal data, accounting companies' responsibilities: data storage, data disclosure, data transfer, data breach, data probability, and data subject rights.
- Impacts on operations: what needs to be updated, changes on data processes, contracts, layouts, and IT systems.
- Impacts on monitoring: measurements of law compliance.

Then, interview questions were created to support the ultimate purpose of answering the investigative questions, thus the research question could be answered. Along with the theory from the literature review, a framework was used for designing interview questions.

COSO is a framework designed for internal control. COSO stands for the Committee of Sponsoring Organization. It helps companies to reach their goals, comply with the law and prevents mistakes. (Ikäheimo, Laitinen, Laitinen, & Puttonen 2014.) The framework was chosen because it was suitable for the topic and the purpose of the thesis. To get answers for the investigative questions, there was a need for a framework that could support the interview questions. COSO served its purpose by structuring interview questions through five themes. The thesis was about the Regulation. Its aim was to learn how accounting

companies prepared to conform to the law: what obligations they were under and what changes needed to be done. In addition, the framework's objective is to ensure effective operations, reliable reports and compliant activities (Ratsula 2016, 14-16). The themes of the five components covered the investigative questions to see how efficiently the interviewees comply with the law.

Ratsula (2016, 17) lists five components in the COSO framework:

- Environment control: commitment to certain standards and processes of internal control in companies.
- Risk assessment: identifying and managing possible risks.
- Activity control: risk mitigation and technology support.
- Information and communication: sharing knowledge and awareness of everyone's roles in the processes.
- Monitoring: continuous control on companies' operation.

A table about its themes, topics and categories related to the study is attached in the appendix.

In the second stage, potential respondents were searched for and contacted. Two of the interviewed companies were the author's internship places. Another accounting company was recommended to the interviewer after completing an interview. By attending workshops and via a personal contact, the author accessed another respondent. For the rest of the interviewed respondents, the author read articles written by them about the Regulation from their websites, then contacted them for interviews.

Interviews were conducted in the final phase. Semi-structured interviews were used because they allowed flexibility of the respondents. How the respondents understood and assessed the topic was important. (Bryman & Bell 2007, 474-475.) Moreover, semi-structured interviews gave respondents more space to share their experiences. During the interviews, some questions for further clarity could be asked. (Galetta 2013, 46-52.) Depending on different participants, questions could be modified (Saunders & Lewis 2012, 151).

The figure below presents the design of this research.

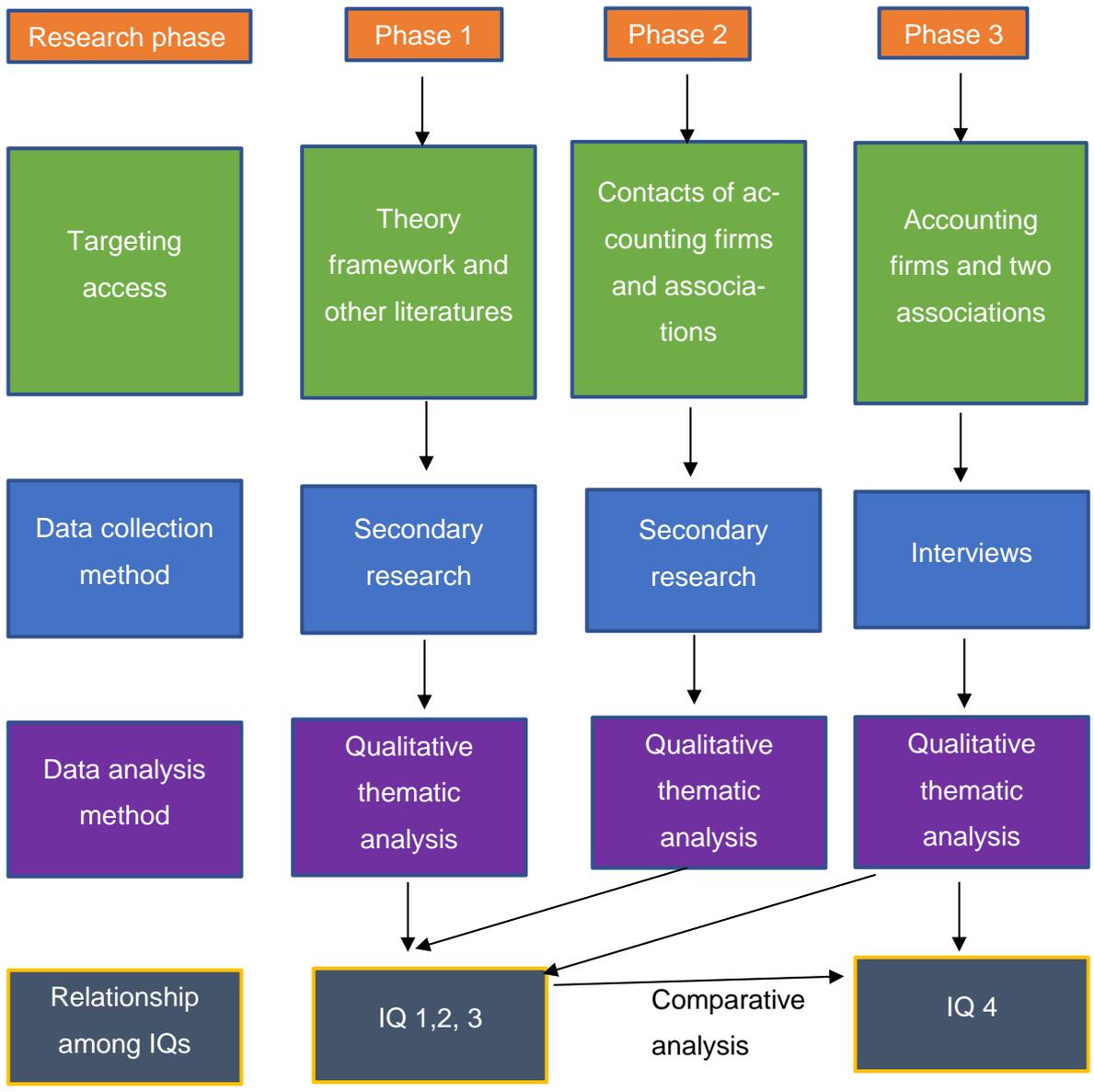


Figure 2. Research design

4 Results

This chapter presents answers to the investigative questions. After the primary data from the respondents was collected, the results were analysed by structuring the data according to the topics of the investigative questions. The data was interpreted by finding meanings and relationships among answers of the respondents. Similarities and frequencies were identified. (Galletta 2013, 151; Saunders & Lewis 2012, 194-199.)

Before discussion of the findings, this table below shows background information of the interviewed respondents.

Table 4. Summary of the respondents' background

Background information	Short introduction	Responsibilities in brief
Respondent		
Respondent 1: -38 years in the accounting field -Micro-sized accounting company	The respondent is a sole trader. Founded in 1996, the company has been an established accounting firm. At the same time, the respondent is working as an accountant in another accounting company.	The respondent is responsible for bookkeeping, VAT payments, financial statement preparations and tax notifications. In addition, she has to manage her own company.
Respondent 2: -More than 10 years in the accounting field -Micro-sized accounting company	The respondent is a manager, an entrepreneur and an accountant.	The company offers services of bookkeeping, accounts receivable, accounts payable, payroll, VAT payments, tax notifications.
Respondent 3: -30 years in the accounting field -Micro-sized accounting company	The company was founded in 1992. The respondent is a chairman of the Board.	The firm offers services of bookkeeping, payroll, digital archive, purchase and sale invoices.
Respondent 4 : -5 years in the accounting field	The respondent is a specialist leader who works for a medium-sized accounting firm.	The respondent is responsible for commis-

		sions, tax issues, different financial calculations, and internal management, for example training the company's employees.
Respondent 5: -10 years in the accounting field -Micro-sized accounting company	The respondent is an accountant and a business advisor.	Because this is a one-person-company, the business owner is responsible for almost everything: getting new customers, answering interviews, consulting customers, preparing financial statements and tax notifications.
Respondent 6: -29 years in the accounting field	The respondent is an accounting manager who has worked for an association for 2,5 years. The association outsources partly accounting tasks to an accounting company in Finland.	The respondent is responsible for preparing payroll material. The respondent collects employees' working hours and works with their personal data.
Respondent 7 : -20 years in the accounting field	The respondent is a financial management specialist who has worked for 2 years at an association that represents Finnish accounting firms. The number of their members is more than 800.	The respondent is responsible for writing articles, consulting and preparing trainings for members that belong to the association.

4.1 Reactions of accounting firms towards the new law

All of the interviewed companies were well aware of the Regulation. They accessed the law via reliable and trustworthy sources of information, for example, professional publications or courses organized by public authorities. In one accounting company where the first respondent works, its intranet platform also showed news for employees to follow up.

To three micro-sized companies which do not have employees, the law can be good when personal data is processed more securely and implementing better storage methods. Looking on the bright side, the Regulation makes accountants think more carefully before processing personal data. It has good intentions to control giant companies, such as Google and Facebook.

However, the Regulation can be considered as another bureaucracy that the companies have to manage. To an entrepreneurial accountant, it does not bring any benefits to a micro-sized company.

In a medium-sized company that has limited resources, the new law required a considerable amount of work. Nonetheless, hard work paid off. It was beneficial because it brought revenue to the company. For example, the expert in the medium-sized company helped some customers prepare documents about the General Data Protection Regulation.

Moreover, when it came to effect, it affected every company, even small ones. The problem is that there was no clear instructions. There might have been some guidances, but they were vague. It was difficult to know, for example step by step, what small companies were required to do. Another challenge was the writing techniques used in the GDPR. For an accountant who is used to reading Finnish legislation, it might be difficult to understand the Regulation. Therefore, learning the law is time consuming for a sole trader that has to take care of various tasks.

Due to these challenges, when it came to effect last year, many accounting firms in Finland had to work with the accounting association to receive more advice and guidance according to a financial management specialist.

Regardless of some inconveniences, no one is against it. Every accountant has to learn and follow the law according to all of the interviewed respondents.

4.2 Data processes of accounting companies

This subchapter explains how accounting companies manage personal data. It covers what personal data is needed, what purpose the accountants need the data for, whom the data is shared with and how to store the data.

4.2.1 Access of accounting companies to personal data

When the data is saved in digital accounting software, accounting companies can see the customers' suppliers, customers and employees according to a specialist leader at a medium-sized company.

In the working day of an accountant, the main purpose of personal data collection is payroll and tax. To carry out the tasks, accountants need addresses and social security numbers. Work contracts are also needed to know working hours and collective labour agreements. In a medium-sized company, personal data is needed to pay the dividends to the shareholders.

Occupational healthcare and debt collection agencies need customers' social security numbers. In addition, accounting companies can access sensitive information, such as distraint information, labour union payment, and sick leave information. Because some data is sensitive, it is important to explain the purpose of data collection. For example, one association outsources partly accounting services to an accounting company. When they organized a summer camp for children, then the accountant needed the dates of birth of people who paid for the summer camp's participants. In one case, a parent phoned and asked the purpose of it. It was explained that if payments were not paid, it would be forwarded to the debt collection agency.

In some cases, personal data is used when accounting companies assist customers in establishing their own businesses and making loan reports. According to a one-person accounting firm and another micro-sized accounting firm, when accounting companies offer consulting services, for example, helping customers to start up their own businesses, personal data is needed for the purpose of registration. It includes name and social security number. If he or she does not have Finnish social security number, then the accounting company needs dates and place of birth, citizenship, name of the company, its registration number, address, phone number, position and share of ownership. When accounting companies follow the Anti-Money Laundering Act, the accountant makes observations on the customers and takes note. If the law demands collection of certain data, then the accountant must collect and store the data safely.

4.2.2 Data storage and data disclosure

A few interviewed respondents continue storing most of the data in binders, while others save the data to digital accounting software and other electronic folders. When using digital accounting software, the customers can have their own account and manage the data

themselves. The data is stored as long as the law requires according to all of the interviewed respondents.

To all the interviewed companies, data is shared to tax authorities, banks, insurance companies and auditors. In case customers do not pay the bills, the debt collection agency is contacted. It is necessary to distinguish personal data and company data. For example, in some cases, a one-person-company has the name of the owner. A one-person-accounting company explains that when the name of the customer appears on the invoice of the debt collection agency: the sole trader X has not paid the required amount which means that name is not personal data, but company data.

If the customers give consent, the data is also shared to occupational health services and other suppliers of the accounting companies to carry out their tasks. For example, when a medium-sized accounting company makes an offer to a new customer, it needs personal data of potential customers in order to send marketing messages or newsletters.

It is known that when accountants use the Finnish accounting softwares, the data stays within Finland. However, it is possible that some data might go abroad when the suppliers are from outside the EU. For example, a USA company supplies an accounting company with contact forms so that new and potential customers can contact them. Although the data of the customers' employee does not go outside of the EU, the data of those who use the contact form might go abroad according to a medium-sized company. Another example is the email system. It is unclear who can access the data according to an association that uses Outlook email system. To both a medium-sized firm and a one-person company, accountants have to pay attention to working culture and working method. Therefore, it is important for accounting companies to check whether or not the supplier has US Datashield and complies with the Regulation.

All the interviewed respondents agreed that accountants have to try all possible methods to improve the situation if data breach happens. First of all, it is important to know what happened and why. The reasons can be from two sides. On the one hand, someone might have done something wrong. On the other hand, it can be the system, for instance, the technical devices might be inappropriate. Data breach can happen by accident when unencrypted emails are sent. In that case, accounting companies and customers should have common agreements on how to deal with the situation in accordance with a medium-sized firm and a one-person company.

If the data breach is serious, the specialist leader advises that a notification should be composed and sent to data protection authorities. According to the second respondent, there are some instructions on the website tietosuoja.fi.

Following instructions given by the customer, their data can be transferred to another accounting firm if they want to change company according to a medium-sized firm and a one-person company. One of the benefits of the digital accounting software is that the customers' data remains in the software. With consent of the customer, the data transfer happens easily, especially if both accounting companies use the same software. Although contracts end, data still needs to be stored as long as the law requires. For example, job certificates and accounting materials are meant to be stored for 10 years.

Most of the interviewed respondents share the same principle that if customers would like to know what information the companies have about them, it is free of charge. However, a fee can be charged in some cases. To make sure the data is given to the right people, the representative of the customer should contact the accounting company in order to protect the customer's identity. One interviewed accounting company decided that it is free of charge if one department asks what information the company has about them. If one of the customers' employees continuously asks and it significantly affects the accounting company's workload, then it is chargeable.

4.3 Actions of accounting firms

Before implementing any plans, some companies have reviewed their registrations in the companies to make sure that the processing goes smoothly. In a medium-sized company, they also did risk analysis and decided some solutions in advance. Before the law came to effect, one of the interviewed accounting companies had to check its operation to make sure that everything works pursuant to the law.

One of the noticeable actions from the accounting companies is that one accounting company where the first respondent works asked an IT company to design a system of encrypted messages. In addition, all of the interviewed respondents have to update their contracts with customers. As data controllers, the customers should give instructions on how to process the data. However, in some cases, customers are busy with other businesses, so the fifth respondent has to prepare instructions on behalf of the customers.

All of the interviewed respondents are committed to complying with the law. They know that their companies' operations conform to the law because all of them have spent a tremendous amount of working time learning and implementing it. They attended some courses, or even organized some trainings at their working places.

Another good sign to know whether or not the company conforms to the law is that no one calls or no customer complains according to an entrepreneur and an accounting manager. Under certain circumstances, some actions might not exactly be law abiding. To both a medium-sized firm and a one-person company, because the Regulation has so many requirements, it is challenging to follow them meticulously. Only the inspector authority can answer if their operations are compliant. The accounting companies have tried their best to do their jobs. Thus, in case some customers are not satisfied, then only the Court of Law is able to decide who is right.

4.4 Changes in accounting firms

According to a one-person accounting company, Finland had a good law on this subject, so the data was processed safely and confidentially in the past. There would not have been revised if everything had been done in a correct manner before.

However, there have been certain changes in accounting firms due to the Regulation. Accountants are expected to pay more attention to the personal data they process, for example, to the information that can lead to an individual and makes a connection between the individual and their tasks. Thus, in accordance with the first respondent, it is important that the connection should be put in confidentiality.

Due to the Regulation, there is a need to update some parts of the contracts between the customers and all the interviewed companies. For example, some attachments about data protection were added. In a medium sized company, terms, layouts and attachments have been changed, for example, description of different registrations: the source of the data, how to process the data and when to delete it. After written contracts were signed, the homepages of the interviewed companies were updated.

One of the major changes is encrypted messages in both a micro sized firm and an association that receives services from an accounting company. To communicate with accounting companies, the customers need a code to open and read the messages. In a one-person accounting company, the layout of payslips has been changed. Letter Xs are

used to hide parts of personal data. The new payslip partly shows personal data. For example, bank numbers are not fully shown. There can be four numbers in the beginning and at the end, but there are a series of letters Xs in between.

When it comes to accounting software, all of the interviewed companies did not have to take care of technical changes because the accounting software's suppliers handled it already. In a medium-sized company, firewall might have been used to ensure security before, but now the security is strengthened with the technical updates.

4.5 Suggestions

The result of the research suggests that accountants should spend significant time on reading, learning the Regulation and following the news. Some reliable sources can be the website of Office of the Data Protection Ombudsman or professional publications, for example Yrittäjä, Verotieto, and Tilisanomat. Attending courses organized by Tax Administration and insurance companies are recommended. Moreover, Kauppakamari also organizes some courses and trainings. Another option is to read legal literature. One book from Helsingin Kauppakamari was recommended: *Henkilötietojen käsittely. EU-tietosuojasetuksen vaatimukset (2017)*.

According to a financial management specialist, because payroll is the section that has most of the personal data, especially sensitive information, such as health-related information, it is important for accountants to review and record the data processing. Documentation of the process is good not only for complying with the law but also for the employees. If some members of the staff change employer, the new employees can familiarize themselves with the new working environment easier. Accountants are advised to critically and thoroughly review the data processing: how to receive and save the data from customers, who the data is disclosed to and how to store it. In case any risks arise during the process, accountants should be prepared and come up with solutions in advance.

Moreover, there should be common agreements on how to process data. For example, a one-person-accounting firm recommends that whether payslips are sent by post or by email is decided by the customers' employees. Normal post might be safer than email from certain viewpoints. Nevertheless, someone can steal and see people's personal data. When the letters are opened, someone else at the workplace can accidentally see it as well. According to an accountant, emails are better, but officially normal post is safer. Therefore, it is better to have mutual agreements with customers in advance. The accountant should always ask the customers, which method they prefer: post or email.

In one case, encrypted messages were challenging for a customer. In the company where the first respondent works, prior to technical changes, it requires certain steps, thus, the customer can have a challenging experience to open and read the messages. It can lead to customer dissatisfaction with the service of the accounting company. As a result, the company had to use normal emails again to communicate with the customer.

The Regulation does not state that normal emails are forbidden. However, encrypted messages are highly recommended. Customers can decide, but accounting companies should have a secure system according to a financial management specialist. The law has many requirements and it is challenging to meticulously conform to the law. Therefore, a specialist leader advises that accountants need to find a way to balance serving the customers and complying with the law.

Moreover, good organizational skills are essential according to the second respondent. It is necessary that all materials are in the correct places, for example, accounting materials and data related to health such as medical certificates should be kept in different places. It is good to keep in mind that everything has its own places and there is a place for everything.

According to one accounting company, Dos Palka is recommended due to its security. Moreover, Procountor is also a good piece of software. Its supplier is responsible for all the technical updates. It has a feature that if someone asks what information the company has about them, then the software has a function to collect all the data according to a one-person accounting firm.

5 Discussion

The final chapter explains why the thesis reached its reliability and validity. Reflection on self-learning is presented. Key results are shown. Suggestions are also made for further researches in the future.

5.1 Reliability and validity

The thesis plan was well-designed before conducting any interviews. Reliability and validity were taken into consideration at the planning stage. A significant amount of time was spent on learning the Regulation, researching methods and contacting accounting companies. All of the interviewed respondents have strong backgrounds from at 5 to 38 years in the accounting field. All of the interviews were documented.

A thesis demonstrates reliability when a researcher implements the research again and receives the same result (Kananen 2011, 66). Moreover, Kananen (2011, 66) states that a thesis achieves validity when the research answers the questions it aimed to. During interviews with accounting companies, respondents answered the questions about their reaction towards the Regulation, actions and changes in the companies to comply with the law. In addition, the respondents shared valuable working experiences. Accounting companies gave insight on what personal data they needed in practice and why. An interview with an association added the customer viewpoint to the study and an interview with an accounting association provided some solutions for current situations of accounting companies. The most important thing is that the replies from the respondents answer the investigative questions, thus answer the research question.

Furthermore, the reliability and validity of a research increases when saturation point is reached. It means that the answers start to be repeated. (Kananen 2011, 66.) All of the interviewed accounting companies had common answers regarding compliance of the law, for example, contract updates, and customers' consents. In this thesis, the replies of one respondent shared similarities with other respondents' answers. The answers were also repeated in the interviews with two associations, that encrypted messages are the best solutions for security against unlawful accesses.

5.2 Main results and recommendations

The findings show that all of the interviewed companies are well aware of the Regulation. A significant amount of working time has been spent on training and learning the Regulation.

In short, the whole data processing has been reviewed. The interviewed respondents have made careful preparations. They have also prepared some solutions in advance and signed mutual agreements with customers. All of the interviewed respondents have adopted some changes in their companies to conform to the law. Contracts, layout of payslips and encrypted messages are major changes in their companies as discussed in Chapter 4. As accounting companies use softwares from other suppliers, it is important to check that the suppliers also comply with the law, especially those suppliers from outside the EU.

This result of the thesis represents only the interviewed respondents. Further interviews with other accounting firms can be done in the future to get a broader picture of the Regulation and the accounting companies in Finland. Along with organisational measures, technical measures are required by the Regulation. To make sure that IT suppliers from outside the EU comply with the law, an audit on the suppliers' softwares and systems is recommended. This could be a topic of research to IT students or experts for example.

5.3 Self-reflection on learning

This study helped the author understand more about the working life of accountants in Finland and what obligations can be expected in the working environment of accountants in Finland. It is valuable not only for the thesis writer but also for those students who have limited working experiences in Finland. The thesis was an effort to narrow down the gap between those students, including the author and accounting companies in Finland.

Moreover, working on the thesis supported the author to develop herself at her own pace. The author has learned to improve research and communication skills during the thesis writing process. She learned how to evaluate the sources, apply and analyse the information. Communication skills were improved when she started contacting accounting companies. The thesis writer learned how to present the ideas and ask the respondents for interviews. It was a long process and hard work was required. However, the author had opportunities to develop her knowledge and competence about the Regulation and accountants' obligations. She is thankful for all the participants that spent time on participating in the interviews.

References

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava Tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tietosanoma Oy. Helsinki.

Braun, K. & Tietz, W. 2013. Managerial Accounting. 3rd edition. Pearson Education. Upper Saddle River.

Bryman, A. & Bell, E. 2007. Business Research Methods. 2nd edition. Oxford University Press. Oxford.

CNIL 2019. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. URL: <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. Accessed: 31 March 2019.

Court of Justice of the European Union 2015. Judgement of the Court. URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=704475>. Accessed: 31 March 2019.

Deloitte 2018. GDPR benchmark survey. URL: <https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/risk/ch-en-deloitte-GDPR-benchmark-Survey-Report.pdf>. Accessed 3: October 2018.

Directive 95/46/EC. Directive 95/46/EC of the European Parliament and of 24 October 1995 on the protection of personal data. Official Journal L 281, 23/11/1995 P.0031 – 0050.

Eduskunta 2018a. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. URL: https://www.eduskunta.fi/FI/vaski/Kasittelytiedot-Valtiopaivaasia/Sivut/HE_9+2018.aspx. Accessed: 3 April 2019.

Eduskunta 2018b. Hallituksen esitys HE 9/2018 vp. URL: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx. Accessed: 3 April 2019.

Europa 2018. 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: 15 January 2019.

Europa 2019. Regulations, Directives and other acts. URL: https://europa.eu/european-union/eu-law/legal-acts_en. Accessed: 3 May 2019

European Commission 2018a. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en. Accessed: 3 September 2018.

European Commission 2018b. What if my company/ organization fails to comply with the data protection rules? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en. Accessed: 3 September 2018.

European Commission 2018c. What is personal data? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. Accessed: 3 September 2018.

European Commission 2018d. Who does the data protection law apply to? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en . Accessed: 9 September 2018.

European Commission 2018e. How can I access my personal data held by a company/organisation? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/how-can-i-access-my-personal-data-held-company-organisation_en. Accessed: 11 September 2018.

European Commission 2018f. What is a data controller or a data processor? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en. Accessed: 11 September 2018.

European Data Protection Board 2018. Cross-border cooperation and consistency procedures- State of play. URL: https://edpb.europa.eu/news/news/2018/cross-border-cooperation-and-consistency-procedures-state-play_en. Accessed: 30 March 2019.

European Data Protection Board 2019. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf. Accessed: 30 March 2019.

European Union 2018. Data protection and online privacy. URL: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm. Accessed: 3 September 2018.

EU GDPR 2018. URL: <https://eugdpr.org/the-regulation/>. Accessed: 11 September 2018.

Eurostat 2018. URL: <https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme>. Accessed: 13 October 2018.

Eriksson, P. & Kovalainen, A. 2016. Qualitative Methods in Business Research. 2nd edition. SAGE Publication. London.

Financial Times 2019a. France fines Google €50m in test for EU's new data laws. URL: <https://www.ft.com/content/e341f482-1d92-11e9-b126-46fc3ad87c65>. Accessed: 23 January 2019.

Financial Times 2019b. Netflix, Youtube, Amazon and Apple accused of GDPR breach. URL: <https://www.ft.com/content/4a977276-1b3e-11e9-b93e-f4351a53f1c3>. Accessed: 23 January 2019.

Finlex 1999. Henkilötietolaki 523/1999. URL: <http://finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523>. Accessed: 9 April 2019.

Finlex 2015. Laki kirjanpitolain muuttamisesta 1620/2015. URL: <https://www.finlex.fi/fi/laki/alkup/2015/20151620>. Accessed: 16 April 2019.

Finlex 2018. Laki rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain muuttamisesta. URL: <https://www.finlex.fi/fi/laki/alkup/2018/20180406>. Accessed: 9 April 2019.

- Finne, E. 27 February 2019. Accounting manager. Helsingin Nuorten Miesten Kristillinen Yhdistys. Interview. Helsinki.
- Fredman, J. 2018. Tietosuoja-asetusTAL2018-sopimusuudistuksessa. URL: <https://tilitoimistossa.taloushallintoliitto.fi/toimintamallit-ja-tyokalut/tietosuoja-asetus-tal2018-sopimusuudistuksessa>. Accessed: 22 January 2019.
- Friedewald, M. & Pohoryles, R. 2013. Technology and Privacy. *Innovation: The European Journal of Social Science Research*, 26, 1-2, 1-6.
- Galeletta, A. 2013. *Mastering the Semi-Structured Interview and beyond. From Research Design to Analysis and Publication*. New York University Press. New York.
- GDPR 2018. Article 32. URL: <https://gdpr-info.eu/>. Accessed: 15 January 2019.
- Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. *Henkilötietojen käsittely. EU-tietosuoja – asetuksen vaatimukset*. Helsingin Kamari Oy. Helsinki.
- Henkilötietolaki 22.4.1999/523. URL: <https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523>. Accessed: 19 February 2019.
- Ikäheimo, S., Laitinen, E., Laitinen, T., & Puttonen, V. 2014. *Yrityksen taloushallinto tänään*. Vaasan Yritysinformaatio Oy. Vaasa.
- Jormakka, R., Koivusala, K., Lappalainen, J. & Niskanen, M. 2016. *Laskentatoimi*. Edita Publishing Oy. Helsinki.
- Kananen, J. 2011. *Rafting through the thesis process step by step guide to thesis research*. JAMK University of Applied Sciences. Jyväskylä.
- Koivumäki, J. & Lindfors, H. 2012. *Pk-yrityksen taloushallinto käytännönläheisesti*. Helsingin seudun kauppakamari. Helsinki.
- KPMG 2017. *Ready for GDPR? Five steps to turn compliance into your advantage*. URL: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/kpmg-gprd-guide.pdf>. Accessed 3 October 2018.
- Lahti, S. & Salminen, T. 2014. *Digitaalinen taloushallinto*. Talentum Media. Helsinki.

Laki kirjanpitolain muuttamisesta (1620/2015). URL:
<https://www.finlex.fi/fi/laki/alkup/2015/20151620#Pidp446220352>. Accessed 19 October 2018.

Lambert, P. 2018. Understanding the New European Data Protection Rules. CRS Press. Boca Raton FL.

Lacey, S. 2015. TEDxTalks: The future of your personal data – privacy vs monetization. URL: <https://www.youtube.com/watch?v=Jlo-V0beaBw&t=182s>. Accessed: 15 January 2019.

OECD 2013. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofprivacyandtransborderflowsofpersonaldata.htm#oecd>. Accessed: 28 March 2019.

Oikeusministerio 2018. Uusi tietosuojalaki voimaan vuoden 2019 alusta. URL: https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta. Accessed: 22 January 2019.

Paasi, A. 25 February 2019. Specialist leader. Balanco Tilitoimisto. Interview. Helsinki.

Mattinen, K., Parnila, K. & Orlando, C. 2017. Palkanlaskenta käytännönläheisesti. Helsingin Kamari Oy. Helsinki.

Niemelä, A. 15 February 2019. Manager, Accountant and Entrepreneur. Tmi Niemelä Laskentatoimisto. Interview. Vantaa.

Niemelä, T. 20 February 2019. Chairman of the Board. Tilitoimisto Finndebet Oy. Interview. Vantaa.

San Miguel, E. 2012. Demarcation Principles and Tools. Haaga-Helia University Applied Sciences. Thesis planning course material. Helsinki.

San Miguel, E. 2015. Skill in Motion thesis tools. Haaga-Helia University Applied Sciences. Thesis planning course material. Helsinki.

Ratsula, N. 2016. Yrityksen sisäinen valvonta. Edita Publishing Oy. Helsinki.

Regulation on Personal Data 2016/679. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on personal data processing and movement. Official Journal of the European Union L 119/1.

Saunders, M. & Lewis, P. 2012. Doing research in business management. An essential guide to planning your project. 1st edition. Pearson Education Limited. England.

Simonen, M. 8 February. Sole trader and Accountant. Kirjanpitoimisto Simonen Maarit Tmi. Interview. Hyvinkää.

Sirkä, J. 4 March 2019. Accountant, Business Advisor and CEO. Accounting Office Relipe Oy. Interview. Vantaa.

Taloushallintoliitto 2018a. Kirjanpidon vaatimukset riippuvat yrityksen koosta. URL: <https://taloushallintoliitto.fi/kirjanpidon-abc-mita-jokaisen-tulisi-tietaa-kirjanpidosta/kirjanpitovelvollisuus/pieni> Accessed: 14 October 2018.

Taloushallintoliitto 2018b. Tilitoimistoala Suomessa. URL: <https://taloushallintoliitto.fi/tietoa-meista/tutkimuksia-ja-tietoa-alasta/tilitoimistoala-suomessa>. Accessed: 14 October 2018

Taloushallintoliitto 2018c. Tilitoimiston Palvelut. URL: <https://taloushallintoliitto.fi/tilitoimistoasiointi/tilitoimiston-palvelut>. Accessed: 18 February 2019.

Taloushallintoliitto 2018d. Miten kauan kirjanpitoja täytyy säilyttää? Arkistointi. URL: <https://taloushallintoliitto.fi/kirjanpidon-abc-mita-jokaisen-tulisi-tietaa-kirjanpidosta/miten-kauan-kirjanpitoja-taytyy-sailyttaa>. Accessed: 19 February 2019.

Tieto 2016. The ABC of GDPR. How General Data Protection Regulation will affect your organisation. Tieto. Helsinki. URL: <http://pages.tieto.com/security-wp3.html>. Accessed: 25 April 2019.

Tietosuoja 2019. Tietosuojavaltuutetulle ilmoitettujen asioiden määrä edelleen kasvussa. Tietosuojavaltuutetun Toimisto. Helsinki. URL: https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetulle-ilmoitettujen-asioiden-maara-edelleen-kavussa. Accessed: 5 May 2019.

Tilastokeskus 2018. Microyritys. URL: <https://www.stat.fi/meta/kas/mikroyritys.html>. Accessed: 13 October 2018.

Voigt, P. 2017. The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer. Switzerland.

WetFeet 2003. Insider Guide to Careers in Accounting. WetFeet Incorporated. San Francisco. URL: <https://ebookcentral.proquest.com/lib/haaga/reader.action?docID=4388457>. Accessed: 9 April 2019.

Yrittäjät 2018. Yrittäjyys Suomessa. URL: <https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363>. Accessed: 14 October 2018.

Appendix

Appendix 1. Overlay Matrix

Investigative questions	Theoretical framework	Research methods	Results
IQ 1. How have Finnish accounting companies reacted to the new law?	GDPR, business opportunities, and challenges.	Secondary and primary research.	Current situation of accounting firms in Finland due to the new law.
IQ 2. How have Finnish accounting companies prepared to comply with the new law?	Consent, right to access, right to be forgotten, data portability, and data breach.	Secondary and primary research.	Actions that accounting firms have taken.
IQ 3. What changes have been made in Finnish accounting companies due to the new law?	contractual, organizational, processing and technological changes.	Secondary and primary research.	Actions that accounting firms have taken.
IQ 4. What recommendations do accountants have for other accountants in Finland to comply with the GDPR?	Accounting skills, and law compliance.	Secondary and primary research.	Recommendations are suggested to improve efficiency of accounting works.

Appendix 2. Main Activities Checklist

To-do list	Done	✓
Thesis planning	August - October	
Map thesis ideas to find thesis topic	Week 33 (2018)	✓
Create research question, investigative questions and demarcation	Week 34 - 35 (2018)	✓
Define theoretical framework	Week 36 - 37 (2018)	✓
Map research method and research design	Week 38 - 39 (2018)	✓
Thesis implementation	October- March	
Phase 1: Theoretical framework and other literature		
Search relevant materials	Week 41 - 43 (2018)	✓
Read, evaluate and connect existing knowledge with thesis objectives		
Create interview questions based on theoretical framework	Week 47 - 49 (2018)	✓
Phase 2: Accounting firms & associations' websites	Week 44 - 46 (2018)	✓
Search unfamiliar companies that are interested in GDPR	Week 50 - 52 (2018)	✓
Phase 3: Accounting companies and other associations		
Contact those companies (from phase 2) to ask for interviews	Week 1 - 5 (2019)	✓
Contact existing contacts for interviews	Week 2 (2019)	✓
Conduct interviews and collect data	Week 6 -11 (2019)	✓
Thesis finalisation	March - April	
Interview transcription	Week 12 (2019)	✓
Analyse data	Week 13 (2019)	✓
Finish writing thesis	Week 14 (2019)	✓
Review and proofread thesis	Week 15 -17 (2019)	✓
Submit thesis	Week 17 -19 (2019)	✓

Appendix 3. A Framework for Interviews: themes, topics and categories

Themes	Topics	Categories	Codes (key words or key phrases for analysis)
Environment control (Investigative question 1)	Current situation of interviewed accounting companies.	Regulation awareness, benefits and challenges.	Source of information, and viewpoints.
Risk assessment (Investigative question 2)	Preparation for the law: data processes.	Purpose limitation, data disclosure, storage limitation.	-Personal data and its purposes in accounting companies. -Authorized access. -Data transfer, data probability, data breach, data subject rights.
Activity control (Investigative question 3)	Impacts on data processes, contracts and technical systems.	Principle of the GDPR on data processing: lawfulness, fairness and transparency Integrity and confidentiality .	-Changes on working methods, data processes, contracts and accounting systems.
Monitoring (Investigative question 3)	Assessment of the law compliance.	Principle of the GDPR on measurement of law compliance: accountability.	-Law-abiding.
Informationa and communication (Investigative question 4)	Suggestions for other accountants to prepare to comply with the Regulation.	Sharing and improving awareness of the Regulation.	-Training and recommendations.

Appendix 4. Justification for Interview Questions

Purposes	Questions	Connection to theory
General questions	<ul style="list-style-type: none"> - Please could you briefly introduce the company? - Please could you tell me about your position and responsibilities? - What kind of everyday tasks do you have? - How many years of experience have you had in the field? 	Background questions and beginning of semi-structured interviews.
Personal Data Processing: data subject rights and obligations of data controllers and processors	<ul style="list-style-type: none"> - what personal data do you collect and for what purpose? - Who do you share data with? - How do you store personal data? <ul style="list-style-type: none"> • Do you transfer data to other EU States or outside the EU? • What would you do if data breach happens? • What would you do if a customer wants to use other accounting service? Will you transfer their data to another company? When the contract ends, will you delete their data? • Does the customer or employees of customer have to pay if they would like to know what information your company has about them? 	<ul style="list-style-type: none"> -Subchapter 2.3 and 2.4. -A component of COSO framework (Risk assessment).
Reaction towards the law and impacts on financial situation	<ul style="list-style-type: none"> - what do you think about the new law? - What benefit can this new law bring to the company in your opinion? - What challenges have you faced due to the law? 	<ul style="list-style-type: none"> -Subchapter 2.5. -A component of COSO framework (Environment control).
Preparation to conform to the law	<ul style="list-style-type: none"> - How did you find out about this law? - What action did you take to prepare company activities to comply with the new law? - How do you know that what you do complies with the new law? 	<ul style="list-style-type: none"> -Components of COSO framework (Activity control and monitoring). -Subchapter 2.3 and 2.4.

Changes in accounting companies	<ul style="list-style-type: none"> - What are the possible changes in the company data processing activities? - How does the law affect contracts between your company and clients? - How does the law affect the technical system, for example accounting system? 	<ul style="list-style-type: none"> -A component of COSO framework (Activity control) -Subchapter 2.3 and 2.4
Recommendations	<ul style="list-style-type: none"> - What would you say or recommend to other accountants to make sure that their work complies with the GDPR? 	<ul style="list-style-type: none"> -A component of COSO framework (Information and communication)

Appendix 5. Questions for respondents, sent in advance before interview days

EU:ssa General Data Protection Regulation (Yleinen tietosuoja-asetus) astui voimaan vuonna 2018. Uusi laki vaikuttaa kaikkiin yrityksiin. On tärkeää, että asiakkaiden henkilötiedot ovat turvassa, eli niitä käsitellään luottamuksellisesti, eivätkä ne mene ulkopuolisille ja muuhun tarkoitukseen. Haluaisin tutkia nykytilaa: miten uusi laki vaikuttaa tilitoimistoon Suomessa. Tästä löytyy haastattelun kysymykset:

1. Voisitko kertoa lyhyesti sinun tilitoimistostasi?
2. Voisitko kertoa sinun asemastasi ja vastuustasi yrityksessäsi?
3. Millainen on sinun työpäiväsi ja mitä tehtäviä siihen kuuluu?
4. Kuinka monta vuotta sinä olet ollut tällä alalla?
5. Mistä sinä saat tietoja laista?
6. Mitä sinä ajattelet tästä uudesta laista?
7. Mitä hyötyä tämä laki voi tuoda sinun työpaikallesi?
8. Minkälaisia haasteita sinun yrityksesi voi kohdata lain muutoksen takia?
9. Mitä henkilötietoja sinä tarvitset ja mihin tarkoitukseen niitä käytetään?
10. Kenelle muille sinun yrityksesi jakaa asiakkaiden henkilötietoja?
11. Miten säilytetään henkilötietoja yrityksessäsi?
 - Siirretäänkö tietoja Euroopan Unionin tai Euroopan talousalueen ulkopuolelle?
 - Mitä tekisit jos tietovuoto tapahtuu?
 - Mitä tekisit jos asiakas haluaisi käyttää toista kirjanpidon palvelua? Siirrätkö heidän tietojan toiselle yritykselle?
 - Kun sopimus loppuu, poistatko heidän tietojan?
 - Maksaako asiakas tai asiakkaiden työntekijä, jos hän haluaisi tietää, mitä tietoja yrityksellä on hänestä?
12. Mitä toimenpiteitä olet tehnyt noudattaksesi lakia?
13. Mitkä ovat mahdollisia tietojen käsittelymuutoksia tilitoimistossasi?
14. Miten yleinen tietosuoja asetus 2018 tulee vaikuttamaan sinun yrityksesi ja asiakkaiden välisiin sopimuskäytäntöihin?
15. Miten yleinen tietosuoja-asetus 2018 vaikuttaa sinun tekniikan järjestelmään, esim kirjanpidon systeemiin?
16. Mistä tiedät että sinun toimenpiteesi ovat lain mukaisia?
17. Mitä suosittelet muille kirjanpitäjille?