TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Aleks Koha 153398IVCM

IMPACT ASSESSMENT OF AN EU GDPR SELF-ASSESSMENT QUESTIONNAIRE ON ENTREPRENEURS

Master's Thesis

Supervisors: Sten Mäses
MSc
Anu Baum
MBA

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Aleks Koha IVCM153398

ANALÜÜS EUROOPA ANDMEKAITSESEADUSE ENESEANALÜÜSI KÜSIMUSTIKU MÕJUST ETTEVÕTJATELE

Magistritöö

Juhendajad: Sten Mäses
MSc
Anu Baum
MBA

Tallinn 2018

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Aleks Koha

21.04.2018

Abstract

Compliance with the European Union's General Data Protection Regulation (EU GDPR) is becoming an increasingly important topic, as the deadline for compliance is only a month away. Consultants and specialists have developed multiple self-assessment questionnaires which should help entrepreneurs get started on compliance. The problem this thesis tackles is to assess what kind of an impact does a self-assessment questionnaire have on entrepreneurs, two hypothesises will be raised. For the purpose of this research a self-assessment questionnaire will be developed, taking into account different components of a business. Completing the questionnaire will present the participating entrepreneur with a list of EU GDPR articles that they need to be compliant with. The impact this questionnaire will have on the entrepreneur's level of compliance confidence and awareness will be assessed before and after the questionnaire. The results of the survey will be brought out in the end of the thesis and the answers to the two hypothesises given.

This thesis is written in English and is 91 pages long, including 8 chapters, 2 figures and 16 charts.

Annotatsioon

Euroopa Andmekaitseseadusega (EU GDPR) kooskõlas olamine muutub järjest aktuaalsemaks, tähtaeg selleks on vaid ühe kuu kaugusel. Konsultandid ja spetsialistid on loonud mitmeid GDPRi eneseanalüüsi küsimustike, mis peaks ettevõtjaid uue seadusega kohanemisel aitama. Antud lõputöö uurib millist mõju GDPRi eneseanalüüsi küsimustik võib ettevõtjatele avaldada, püstitatakse kaks hüpoteesi. Püstitatud eesmärgi saavutamiseks luuakse antud lõputöö raames samuti eneseanalüüsi küsimustik, võttes arvesse erinevaid ettevõtte komponente. Küsimustiku tulemiks on nimekiri EU GDPRi artiklitest millega ettevõtja veel oma organisatsioonis tegelema peaks. Antud küsimustiku mõju ettevõtja andmekaitseseaduse teadlikkuse tasemele ning GDPRiga kooskõlas olemise enesekindlusele hinnatakse enne ja pärast uuringut. Uuringu tulemused ja vastused hüpoteesidele tuuakse välja lõputöö lõpus.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 91 leheküljel, 8 peatükki, 2 joonist, 16 graafikut.

List of abbreviations and terms

EU GDPR	European Union General Data Protection Regulation
DPO	Data Protection Officer
SaaS	Software-as-a-service
SME	Small-medium enterprise
ICO	Information Commissioner's Office

Table of contents

List of figures

List of charts

1 Introduction

The number one key thing in business is people and to understand people you need information. Data has become an underlying tool in business, we gather it, we process it, we analyse it, we make decisions based on it and we sell it. The amount of data is growing rapidly, a study by the IDC's Digital Universe predicts that the world's data will amount to 44 zettabytes by 2020. Within that substantial number is also a lot of personal information about individuals and this information has to be protected. [1]

In order to better protect personal information, the European Union, after four years of preparation and debate, has finally approved the General Data Protection Regulation (GDPR or EU GDPR) on the 14th of April in 2016. This regulation will enter force on the 25th of May in 2018, by then all organizations that the GDPR applies to have to be compliant. [2]

However, it's not easy to wrap your head around the regulation due to its size and complexity but enterprises have to do it nevertheless. As a result, multiple self-assessment questionnaires have been developed to help entrepreneurs on this journey. This thesis will assess if and what kind of impact such a tool might have on the awareness level and compliance confidence of entrepreneurs regarding EU GDPR.

1.1 Research purpose and goals

The main goal of the given research is to understand if a self-assessment questionnaire helps entrepreneurs understand the EU GDPR better, to what extent and if there is an overconfidence among entrepreneurs regarding compliance and to what extent.

It's important to assess this impact because people who don't have experience in the field or haven't researched the topic don't know what they have to take into account when founding a business or running an existing one during the transition to be compliant with the new changes, therefor they will turn to self-assessment questionnaires, as it is the easiest first option that emerges from a Google search, because professional legal help is often expensive. The result will help understand if the self-assessment questionnaires

have the intended effect on entrepreneurs. Thus, the first hypothesis is defined as follows: “Completing an EU GDPR self-assessment questionnaire will raise awareness about which articles the entrepreneur’s organization needs to be compliant with and understanding about the general implications of GDPR.” If true, alongside this hypothesis, the result of the thesis will also show to what extent such questionnaires raise awareness.

Furthermore, the researcher believes that entrepreneurs underestimate the requirements and depth of EU GDPR and as a result they are overconfident about the level of compliance in their organization, which can be negated by completing a self-assessment questionnaire. This can be dangerous because ignorance doesn’t solve data protection problems and when issues arise, the financial effect can be a lot more damaging than properly preparing for compliance. Thus, the second hypothesis is defined as follows: “Upon completing a self-assessment questionnaire, the compliance confidence of an entrepreneur will drop.” If true, alongside this hypothesis, the result of the thesis will also show to what extent confidence drops.

The summary of the hypothesises and the research questions:

1. Hypothesis 1: “Completing an EU GDPR self-assessment questionnaire will raise awareness about which articles the entrepreneur’s organization needs to be compliant with and understanding about the general implications of GDPR.”

2. Hypothesis 2: “Upon completing a self-assessment questionnaire, self-confidence regarding EU GDPR compliance will drop in entrepreneurs.”

3. Research questions:

    a. When does EU GDPR apply to an organization? Goal: Understand the survey target group.

    b. In creating the self-assessment questionnaire, which articles need to be included to cover all aspects relevant to entrepreneurs? Goal: Understand what level of depth is required in order to be equally significant compared to other self-assessment questionnaires.

c. Which components of a business do the requirements of the EU GDPR influence? Goal: Understand which components of an entrepreneur's organization are affected and use them to group the questionnaire's questions to give context to the scope of GDPR in the output of the self-assessment questionnaire.

Also, it will be determined how much awareness raises and how much confidence drops.

The researcher predicts that existing GDPR self-assessment questionnaires cannot be used for the purpose of this study, for they are either not in the required format or they are segmented into sub-categories and as a result the intended survey would be difficult to conduct. As a result, a self-assessment questionnaire that covers all aspects relevant to an entrepreneur has to be created in this thesis, in order to conduct the survey and prove the hypothesises. Since all self-assessment questionnaires are based on the EU GDPR itself, such as the once created in this thesis, the generalized trend of the research will logically apply to other questionnaires as well. Of course, there would be substantial differences in results if the same experiment were to be conducted with different frameworks, as the quality and design determine self-assessment questionnaire effectiveness, but the general trend can be shown nevertheless.

This research is structured to first review what kind of GDPR studies have been done in the past and what self-assessment frameworks have been developed and why none of them could be used for the purposes of this research. The next step will be understanding when the EU GDPR applies to a business, where research question a) will be answered. The same chapter will also, based on the sanctions, map out the articles that need to be included in the self-assessment questionnaire, as a result research question b) will be answered. Once the articles are defined, a business model template must be developed to understand which parts of an organization specific points in the EU GDPR influence. The next step then would be to create the questions for the self-assessment questionnaire that will be developed for the survey to assess the hypothesises, as the GDPR is quite a massive document, this will be extensive work. Once the business model template and the questions are ready, it must be organized into the self-assessment application, which will be a front-end web application, when the questions are combined with the business

model template, research question c) will be answered. The final part of the thesis will be conducting the survey to analyse the impact and get answers to the proposed hypothesises.

2 Related Literature

In the related literature chapter, an overview of related EU GDPR research will be presented.

There are multiple overviews of EU GDPR, one such paper is titled “EU General Data Protection Regulation: Changes and implications for personal data collecting companies.” The purpose of that study was to compare the current Data Protection Directive 95/46/EC with the GDPR by analysing their differences to identify the practical implications of the EU GDPR. That study brings out a number of aspects of those implications and the corresponding guidance on how to prepare the new requirements, the implications are: specifying data needs and usage, considering conditions for data processing in international context, building privacy through data protection by design and default, demonstrating compliance with GDPR requirements, developing processes to deal with data breaches, reckoning with sanctions for non-compliance, designating a DPO, providing information to data subjects, obtaining consent on personal data usage, ensuring individuals’ right to be forgotten, ensuring individuals’ right to data portability and maintaining documentation. That paper proposes business strategies and practices, as well as organisational and technical measures but no automatic questionnaire to assess the situation, so the affected individuals still have to research it in great detail themselves. [3] Since this framework helps enrich manual research on GDPR, it is not usable to do a self-assessment survey for the purpose of proving the hypothesises in this thesis.

That paper also gives a good overview of the history of data protection. Getting acquainted with the history of data protection helps put the EU GDPR changes into context. [3]

There are also short overviews such as “The EU General Data Protection Regulation (GDPR): European regulation that has a global impact.” This overview focuses on the core privacy principles and the wide jurisdictional scope. The article highlights six

general data protection principles: fairness and lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality [4]. The Estonian data protection inspectorate has published an article titled “Don’t panic! How to be compliant with the new GDPR in 5 steps.” The article suggests to not panic, conduct an integrated assessment of data processing in the case of processing of personal data at large-scale, to check data portability, to find a specialist to assist you with the process. [56] These short overviews are definitely not usable for self-assessment, as they are too broad and don’t cover all aspects for entrepreneurs, they do however help put different articles into perspective when creating the questionnaire.

A good article to shed light on EU GDPR in the context of small businesses in the US is: “What about small businesses? The GDPR and its consequences for small U.S-Based companies.” This paper explores the legal landscape of data privacy and explains why the current methods for small, U.S.-based businesses attempting to comply with the GDPR are not operationally feasible. [5] As any other GDPR article it gives an overview of the changes and their implications. The article also brings out a good point that companies can avoid data transfer clauses by simply keeping their data within the European Economic Area. The paper also brings out the fact that business leaders are currently unaware of the requirements that the new regulation will impose on their organizations, there was also a study by Amárach Research that revealed that 63% of financial decision makers working in organizations with an average of 800 employees were unaware of the requirements or penalties associated with the EU GDPR. [5] Such statistics implies that, if the self-assessment questionnaires have the benefit that is estimated, then promoting them can be a solution to increase awareness among entrepreneurs and high-level decision makers.

The paper also proposes a short-term and long-term solutions. The short term solution would be federal tax credit for US small businesses that will help level the playing field with large companies. The long-term solution would be to create a federal data privacy and protection legislation similar to the EU GDPR. [5] However, these suggestions are more high level and not immediately usable by companies.

There aren’t many general frameworks that have been developed but there are quite a few more detailed analyses of different more important parts of the EU GDPR, such as consent, data portability and automated decisions making. For example, Sandeep Mittal,

a cyber security and privacy researcher from New Del hi, India has done an analysis on models of consent. He has developed a high-level table that gives an overview of different aspects of consent, taking into account that consent is an instrument in the hands of data subjects to control their personal data. [6]

Another article proposes that data portability can be approximated under two different perspectives: the minimalist approach and the empowering approach, which, in the article, is considered more preferable. The first being when data is transferred from one service provider to another in a way where the customers data is removed from one location and moved to the other. The other, empowering approach, that was named the fusing scenario, promotes a more interconnected solution. Users can export their data across services, including their "quantified self" data (lifestyle data, nicknames, intellectual creations, virtual properties, user generated content etc.). This idea allows to fuse the fragmented multiplicity of digital services into interoperable segments of a user-centric internet of things. [7] Such research not only promotes compliance but suggests features on top of the compliance itself which is the best possible scenario in the adoption of a regulation.

A lot of systems in modern technology have automated decision making and this is another point that is regulated by the GDPR. An article in the European Journal of Law and Technology titled "Safe guards for the right not to be subject to a decision based solely on automated processing" seeks to provide an analysis on of the Article 22 that regulates this activity. The safeguards required are brought out, which are also examined in detail in this thesis. The article also highlights a new challenge of the right to obtain human intervention which will be hard to enforce, as it's difficult to contest an automatic decision without a clear explanation of what the decision was. In order to challenge such decisions a team of data analysists will have to detect false positives and discriminations, which of course, is an expensive measure to take. [8] Automated decision making will definitely be included in the self-assessment questionnaire developed in this thesis.

As it will be highlighted in the business template chapter, there is a team component in the business, which also needs to be compliant with EU GDPR. This brings us to an article published in Labour and Law Issues titled "GDPR and Personal Data Protection in the Employment Context." The given article explains that in the GDPR the right of employees to the protection of personal data is not particularly protected so as to prevail

over the interests of companies. Despite the importance of individual rights in the EU has failed to establish uniform rules for this issue. However, employees are still allowed to control their own data and personal identity but it is also highlighted that workers are in a weak position as the individual right is not absolute and doesn't always prevail over companies' interests to improve business through processing personal data. The article also takes a look at employment screening and monitoring at the workplace and out of it and data processing at work in the employment context. [9] In this thesis the team component will be assigned to the questions that may affect the employees in the context of EU GDPR, as a result the employer will know how to properly act in handling employee's data in the work environment.

The best self-assessment questionnaire that was found originates from the Information Commissioner's Office from the UK, which was the only possible candidate to use in this research. However, ICO's framework is split up into sub-categories, which makes it difficult to use in this research, as the choice of sub-category depends on what type of company the surveyed is from. The type of company is not known and hard to pre-define for directing the surveyed to all the correct sub-categories separately. Therefore, it cannot be used in this research, for all aspects of GDPR regarding entrepreneur's organizations need to be covered. [57]

Regarding strategic suggestions, the ICO framework has short tips as a result of their toolkit alongside some links to their own articles. The questionnaire that will be developed in this thesis provides direct references to GDPR articles and no strategic tips have been added, for the reason that the researcher doesn't possess a legal background and interpreting the GDPR articles for real world suggestions should be consulted with a legal professional. As mentioned before, the depth of different questionnaires will surely have different effects on entrepreneurs, but since they are all still based on the EU GDPR the general (hopefully positive) trend can be identified nevertheless. [57] This is especially true if the result is positive, that would imply that more detailed and professional self-assessment toolkits will produce even better results.

In conclusion there are multiple frameworks and overviews of the EU GDPR but most of them are more high level and introductory. Also, deeper analysis has been conducted on specific articles of the GDPR but their result is also not in a practical format to be consumed by entrepreneurs. One, almost suitable, questionnaire by ICO was identified

but due to sub-categorization it is not usable for the purpose of this research, as the complexity of the survey would become too much to be accommodated in the scope of a master's thesis. Therefore, the researcher has to create a self-assessment questionnaire for the purpose of confirming the hypothesises of this thesis.

3 Applicability of the European General Data Protection Regulation

As the official homepage of the EU GDPR says: "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years." [16]

The EU GDPR was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. [16]

According to EU GDPR personal data (or information) is defined as follows: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [16]

The EU GDPR lays down rules for protecting the natural persons regarding the processing of personal data and rules relating to the free movement of personal data. It protects the fundamental rights and freedoms of these people and in particular their right to the protection of personal data. Also, the free movement of personal data within the European Union will not be restricted. [17]

Every business that deals with personal data is going to have to get acquainted with this regulation. As the EU GDPR aims to ensure a consistent level of protection throughout the Union, it stresses the importance of legal certainty and transparency for economic

operators, including micro, small and medium-sized enterprises and to provide all natural persons in all the Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors. [18] In essence, that means that everyone processing European Union's citizens' personal data has to comply with the regulation, even if they are based outside of the Union.

It is also important to note how a business or an 'enterprise' is defined in the EU GDPR: 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity. [19] As it can be seen the size of the enterprise is not defined which means businesses of all sizes have to comply. There is an exception only in regard to keeping records which will be explored in this chapter briefly and in more detail later in the research.

Furthermore, the EU GDPR divides enterprises into controllers and processors. A controller is a natural or a legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member state law. A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [20]

As it can be seen by the above definition if your business determines the purposes and means of the processing of personal data then that business is considered a controller. A processor processes the personal data on behalf of the controller. There is however, no definition regarding organizational size.

The only mention of organizational size is where record keeping is defined: "Controllers and processors have to keep records of processing activities, the only exception to this is if a business is employing fewer than 250 people unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is occasional or the processing includes data relating to criminal convictions and offences or data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, genetic data, biometric data for the purpose of uniquely

identifying a natural person, data concerning the health or data concerning a natural person's sex life or sexual orientation." [21] As it can be seen, organizational size is only relevant in the case of record keeping.

This implies that businesses of all sizes have to comply with the EU GDPR if they process or control EU citizens' data, that means that the target group for this survey includes all entrepreneurs whose organizations process or control EU citizens' data. This includes organizations that are not based in the EU or if the data is processed or controlled outside of the Union. [22] The GDPR states that any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with the EU GDPR, regardless of whether the processing itself takes places within the Union. [23] Furthermore, monitoring of the behaviour of data subjects and the processing of their personal information also has to comply with the EU GDPR, so far as the behaviour of the data subjects take place within the Union. [24]

In conclusion, EU GDPR applicability is quite wide and covers all organizations who process or control EU citizens' personal information. This answers research question a) and defines the target group for the survey: all future and current entrepreneurs or other types of high level decision makers associated planning to deal with or dealing with EU citizen's personal information currently.

3.1 Defining the EU GDPR Articles to be covered in the self-assessment questionnaire

All data subjects have the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes EU GDPR. [25] Infringements of the GDPR lead to sanctions and the goal of compliance is to avoid sanctions. Therefore, sanctions define all the articles relevant to not be fined and that can be taken as the basis of the scope for the self-assessment questionnaire. If all articles mentioned in the sanctions, relevant to the entrepreneur's organization, are covered by the questionnaire developed, then that will give the questionnaire developed in this thesis equal weight to other solutions (such as ICO's questionnaires) because all self-assessment questionnaires are based on the EU GDPR and covering all articles regarding sanctions will ensure that every aspect is considered.

The GDPR has two levels to sanctions, the lighter one states: “Infringement of the obligations of the controller and the processor pursuant to EU GDPR articles 8, 11, 25-39, 42 and 43; the obligations of the certification body pursuant to articles 42 and 43; the obligations of the monitoring body pursuant to article 41(4) will result in administrative fines up to 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.” [26]

That means failing to comply with the following articles: child’s consent in relation to information society services (8), processing which doesn’t require identification (11), data protection by design and by default (25), joint controllers (26), representatives of controllers or processors not established in the Union (27), processor (28), processing under the authority of the controller or processor (29), records of processing activities (30), cooperation with the supervisory authority (31), security of processing (32), notification of a personal data breach to the supervisory authority (33), communication of a personal data breach to the data subject (34), data protection impact assessment (35), prior consultation (36), designation of the data protection officer (37), position of the data protection officer (38), tasks of the data protection officer (39), certification (42), certification bodies (43). [27]

The harsher sanction is defined as follows: “Infringements of the basic principles for processing, including conditions for consent, pursuant to EU GDPR articles 5, 6, 7 and 9; the data subjects’ rights pursuant to articles 12 to 22; the transfers of personal data to a recipient in a third country or an international organisation pursuant to articles 44 to 49 will result in an administrative fine up to 20 000 000 EUR or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.” [26]

That means failing to comply with the following articles: principles relating to processing of personal data (5), lawfulness of processing (6), conditions for consent (7), processing of special categories of personal data (9), articles concerning data subjects’ rights (12-22) and the articles covering the transfers of personal data to a recipient in a third country or an international organization (44-49). [28]

This sets the scope for which articles need to be considered in putting together the questionnaire for the purpose of proving the hypothesises. Comparing it to ICO’s sub-

categorized questionnaire, that also cover all aspects, which means that the questionnaire developed here based on those articles will be sufficient for measuring the effect regarding self-assessment questionnaires.

In conclusion, this chapter has defined the articles that need to be covered by the self-assessment questionnaire in order to cover all aspects of an entrepreneur's organization which is of sufficient depth to assess the hypothesises, answering research question b).

4 Template of a business

The goal of this chapter is to understand which components of an entrepreneur's organization are affected and use those to group the questionnaire's questions to give context to the scope of GDPR in the output of the self-assessment questionnaire. A template of a business will be defined along with the processes associated with such a business.

There are three major types of businesses: a service business, merchandising business and a manufacturing business. A service type of business provides products with no physical form such as professional skills, expertise, advice and other similar products. Merchandising businesses buy products at wholesale price and sell the same products at retail price, they sell the products without changing its form. Examples of merchandising businesses include grocery stores, distributors and other resellers. The third type, manufacturing business, is a type of business that buys products with the intention of using them as materials in making new products, thus transforming the products they purchased. [10] Since there are three major types of businesses, the business template has to cover all aspects.

It is important to firstly explore the core components of a business to understand the use of data in these systems. The business template will be created based on a business model, it will then be extended with the systems and processes required to operate the business model.

Firstly we need to understand what a business model is. A model can be described as a simplified description and representation of a complex entity or process. Business can be described as the activity of providing goods and services involving financial, commercial and industrial aspects. Combining the two a business model can be described as a conceptual tool containing a set of objects, concepts and their relationships with the objective to express the business logic of a specific firm. Therefor it must be considered which concepts and relationships allow a simplified description and representation of what value is provided to customers, how this is done and with which financial consequences. [11]

According to the journal of business research there are six questions that underlie a business model: [12]

1. How do we create value?
2. Who do we create value for?
3. What's our source of competence?
4. How do we competitively position ourselves?
5. How do we make money?
6. What are our time, scope and size ambitions?

Regarding the template that we're creating that translates to the following:

1. The product.
2. The customers.
3. The employees and management of the small business – the team.
4. Competitive advantage.
5. Revenue sources and respective interfaces.
6. Time, scope and size ambitions.

Points four and six are not relevant because if processes relevant to those points process or control personal information then they are already covered by the other points. Removing them, we finally get to the components of the template:

1. The product component
2. The customer component
3. The team component.
4. The financial component.

Each of these components have processes and systems associated with them that are interlinked with each other. Next, these components will be described for the purpose of assigning them to the compliance questions in order to give an understanding of which parts of the surveyed entrepreneur's organization are affected.

The product component - According to The Economic Times, a product is the item offered for sale, a product can be a service or an item, it can be physical or in virtual or cyber form. Every product is made at a cost and sold at a price. [13]

The product component covers all aspects of your solution or service, both technical and non-technical.

The customer component - A customer is a party that receives or consumes products (goods or services) and has the ability to choose between different products and suppliers. [14]

A business must acquire more customers to reach its ultimate goal which is financial gain. In order to do so a business must engage in sales and marketing. Both processes are data driven and often require the use of personal information and accumulation of it to create customer data bases.

In the case of some products customers may also require customer support which may process personal information or use it to verify customer identity.

Therefor the customer component consists of customer interaction, customer communication, customer support, marketing and sales.

The team component - Behind every business are people, the team who came up with the idea, created the product and takes the risk of the business. The team consists of employees and management.

The team component includes human resources activities and deals with personal information of the employees and management. Each team member is also a communication channel to the world external to the business.

The team component can also be considered as an input/output element to all other components of the business because people communicate and as such are able to communicate aspects of the business to the outside world and also take information from the outside world to the internal environment of the business.

The financial component - The financial component is essentially a finance department. It's the part of the organization that manages its money. The business functions of a finance department typically include planning, organizing, auditing, accounting for and controlling its company's finances. The finance department also usually produces the company's financial statements. [15]

While it's true that every company doesn't have a separate financial department, especially small businesses, all the duties of a financial department still always exist and responsibilities are distributed or outsourced, otherwise the business could not legally function.

The financial component is also connected to the payment systems of the business, whatever they use to receive funds (manual invoicing, credit card payments and so on).

In conclusion the financial component consists of the financial department (or the respective functions carried out by other means), payment systems and processes and accounting.

To bring an example of a use of the business template a hypothetical software-as-a-service (SaaS) company X will be used.

In the product component company X has a software platform that has been developed in house. The solution has a database and an interface that the customers can interact with. In order to use the platform customers have to register, providing some personal

information in the sign up process that is stored in the user's database. The personal information of the customers is processed and controlled by the software.

As it can already be seen the customer's component is very tightly linked with the product component as their personal information is used by the solution. The customers pay the company for the software, thus also interacting with the financial component. In order to acquire new users, the data of the existing users is used to draft better targeting plans for sales and marketing. Company X also has a customer support department that has access to the data.

The team consists of employees and the founders, they have a human resources department that holds personal information of the employees and the founders. Since certain team members communicate with customers they are also data interfaces.

In order to receive and process payments the company has set up a third party automated credit card payment system. The system processes the transactions and automatically covers the other aspects of the financial department through a data export interface.

As defined earlier in the research a business can be described as the activity of providing goods and services involving financial, commercial and industrial aspects and that there are three types of businesses (a service business, merchandising business and a manufacturing business). The business template created covers all aspects of businesses that interact with data: the goods or services offered (including industrial aspects of product creation), the customers who consume the goods or services, customer acquisition, the team who creates and organizes the business and the financial or commercial result of the business activity. It's also universal enough to cover all three types of businesses. As a result, it is possible to assign a component to each question regarding the business with the aim help the surveyed entrepreneurs understand which parts of their organizations are affected by the EU GDPR. It is also clear that multiple components can be connected to one question, as the processes and systems regarding these components are interlinked with each other.

In conclusion, the four components of a business defined in this chapter cover all aspects of the business and can be assigned to the questions developed in the research. Of course, the EU GDPR affects all aspects of an organization, but as organizations have a different level of compliance, the affected components may also be different in each case. After

the components are assigned to each question in the next chapter, research question c) will be answered.

5 Self-assessment questionnaire

To avoid getting fined because of non-compliance is something entrepreneurs want to avoid and that is why they seek out self-assessment questionnaires or frameworks. To assess the hypothesises proposed in this thesis, a self-assessment questionnaire has to be developed based on the research questions. The questionnaire will cover all aspects based on research question b). In creating the questionnaire, the researcher will focus on isolating points that ensure compliance in day-to-day operations alongside with pre-emptive action plans for likely inquiries, motivations and values proposed by the EU GDPR.

The questions will be developed based on the articles defined in sanctions. Each of the articles contain sub-points and a question (sometimes multiple) will be given for each of the relevant points, which will be a reversal of the point as a yes/no question. The question is something the surveyed have to ask themselves to understand if they are compliant and each question will direct the surveyed through the questionnaire and each of them will correspond to the article of where the question was raised. This means that if a compliance requirement is detected based on the logics system described in 5.1, then the framework will refer to the appropriate EU GDPR article for instructions and display the relevant business components that are affected to help the surveyed understand the scope of the impact. The full list of the EU GDPR article and question mapping for the questionnaire has been brought out in appendix 1.

The questions were designed to be yes/no questions for simplicity, with the answer “yes” implicating that everything is okay with the point under question or that the question has more detailed sub-questions that need to be addressed, in that case the self-assessment questionnaire goes a level deeper to understand the details. In the case the surveyed answers “no” it indicates noncompliance or if the question has sub-questions under it, it

means that the self-assessment questionnaire skips that segment as it is not relevant for the surveyed.

The questions are grouped under general topics and some questions may overlap as the logic involved to translate the context of the answers under different topics was too complex to be developed only for the sake of usability and those overlaps exist infrequently.

Business model components have also been assigned to the questions, which can be observed in the program code found from the link in appendix 2. As it is a front-end application, all the relevant code can be viewable within the browser. The arrays containing the questions, the business model components and the EU GDPR locations are all a one-to-one match in their indexing. This answers research question c) defining which components of a business the EU GDPR affects for each time someone completes the self-assessment.

As all the research questions have been answered and the questions for the self-assessment questionnaire have been mapped out, the next step is to prepare the front-end application in order to conduct the survey to test the hypothesises proposed.

5.1 The front-end application of the self-assessment questionnaire

The questions that were developed previously require to be organised in a structured way to be implemented into an active questionnaire. The self-assessment questionnaire will be called the Article Checker for short.

The structured format of the questions in the form of three one-to-one matched arrays with the corresponding components and GDPR articles with locations have been brought out in the link in appendix 2 containing the program code. Questions or statements marked with [General Topic], are types of questions that are not asked of the entrepreneur directly, they indicate the topic of the following questions.

The questions have been converted into a structured array (according to JavaScript syntax). Questions are grouped, groups are determined by arrays within arrays, called objects, if an object is detected after a question, then that indicates that the questions within the object are grouped under the preceding question.

The questionnaire iterates through the questions, each iteration is incremented upon answer, if the next increment is an object, the question goes one level deeper into that object and when it runs out of elements and the next element in the array is defined as 'undefined', it decreases the depth of the increments and goes a level up in the questions array.

If the answer is a "no" the answer is saved in the "no" array and if the answer is "yes" the answer is saved in a "yes" array. Questions have been assigned with logic operators, as some articles require all the points to be answered as "yes" and some articles only require one of the questions to be a "yes" to be compliant. Therefor questions are also tagged with *and* and *or* logic operators to calculate the answers in the end.

Answers are saved as locations in the questions array (increments of the position) and the components and GDPR locations arrays are a one to one match of the questions array.

The logic operation information, article name and article location in the EU GDPR (page number) are all defined in the string in the EU GDPR locations array, separated by a colon.

The flow of the application looks as follows:

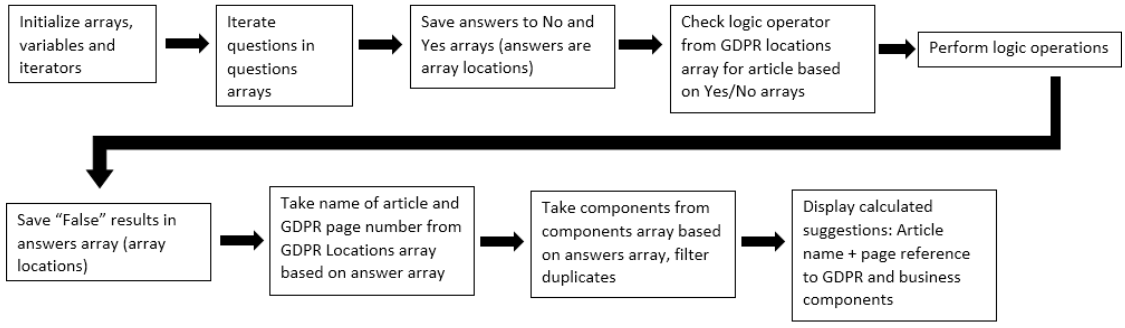

Figure 1. Article Checker program flow.

As mentioned before, the developed questionnaire is a front-end application written in HTML,CSS and JavaScript, the code is brought out in appendix 2. The Article Checker be used in the survey as the self-assessment questionnaire. In order to deploy the questionnaire and test it, index.html and code.js should be saved in the same folder.

After completing all of the questions, the surveyed will be presented with a list of EU GDPR articles that their organization still needs to deal with including the business model components associated with the articles. Here is an example based on my own company (screenshot does not contain business model components):

Figure 2. Example of the result of the framework based on my own company.

Now that the Article Checker in the role of the self-assessment questionnaire is complete, it is time to conduct the survey and test the hypothesises brought out in the beginning of the thesis.

6 Validation of the hypothesises and the survey

In this chapter the testing of the hypothesises will be described. The target group for the survey is based on research question a): individuals of different awareness levels, who are either owners of an organization, high-level decision makers, future entrepreneurs, compliance officers or with other related responsibility to the GDPR. There will be no geographic restrictions as the GDPR applies to all organizations dealing with EU citizen's

personal information. The survey will be released publicly on social media and it will be anonymous, collecting high level data on the size and industry of the enterprise and awareness levels of the surveyed.

The survey is structured as follows:

1. General information (current role/job, industry, size of organization, how acquainted the surveyed individual is to GDPR – not at all, a little bit, dedicated more than an hour or researched in detail)

2. Primary assessment questions:

    a. On a scale of 1 to 10 how ready do you think your organization is regarding the EU GDPR now? This question is to measure confidence prior to completing the Article Checker.

    b. On a scale of 1 to 10 how well do you know which specific Articles of the EU GDPR your organization has to deal with? This question is to measure the awareness level regarding required articles of the EU GDPR prior to completing the Article Checker.

    c. On a scale of 1 to 10 how well can you find the relevant information to your organization from the EU GDPR document? This question assesses the navigability of the EU GDPR in the eyes of the surveyed prior to completing the Article Checker. This helps to understand the perceived complexity of the EU GDPR from the perspective of the surveyed.

    d. On a scale of 1 to 10 rate your general understanding of the implications of the EU GDPR to your organization. This question helps to understand the general understanding of the implications of the EU GDPR in the eyes of the surveyed prior to completing the Article Checker.

3. The surveyed are presented with the Article Checker.

4. The surveyed will return to the survey and complete a reassessment that contains the same questions as point 2.

The expected outcome of the survey is that awareness levels will increase, perceived complexity drops (navigability increases) and that confidence regarding compliance drops. In that case both of the hypothesises will be proven true and the goal of the research will be achieved, which is to show that self-assessment questionnaires do indeed increase awareness and in addition they also drop the confidence of an entrepreneur regarding the current situation in their company regarding compliance.

6.1 Results of the survey

The survey was distributed through social media, specifically Facebook (various large groups), LinkedIn, Twitter and also directly via e-mail. The survey gathered 44 replies by entrepreneurs from 16 different countries. The raw results of the questionnaire are brought out in a table at appendix 3. The tables of the results of the numeric questions and text questions have been separated but they are a one to one match, so combining them will restore the original format. In the results of the survey different distributions will be brought out, then the general results and the results for each distribution. After each chart the findings are analysed.

Firstly, the distribution of participants based on previous experience with EU GDPR:

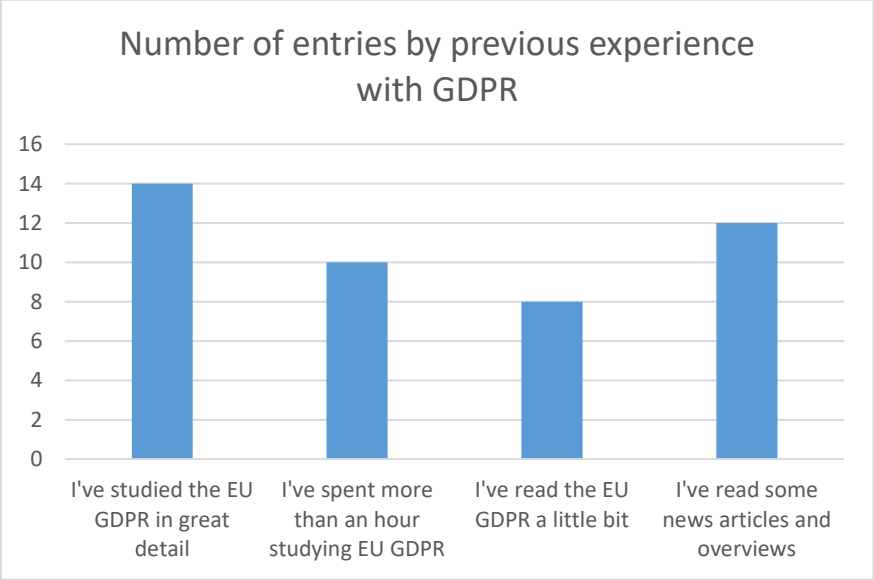

Chart 1. Distribution of participants based on previous experience with EU GDPR.

From this chart it can clearly be seen that the highest concentration of participants have either studied the EU GDPR in great detail (14 participants) or read only some news

articles and overviews (12 participants). This result is not surprising as the survey was distributed in numerous GDPR Facebook groups and also general entrepreneurial groups.

Luckily the distribution is relatively equal and the only awareness level that received zero entries was “Not at all.”

Next, the distribution of participants by will be shown by company size:

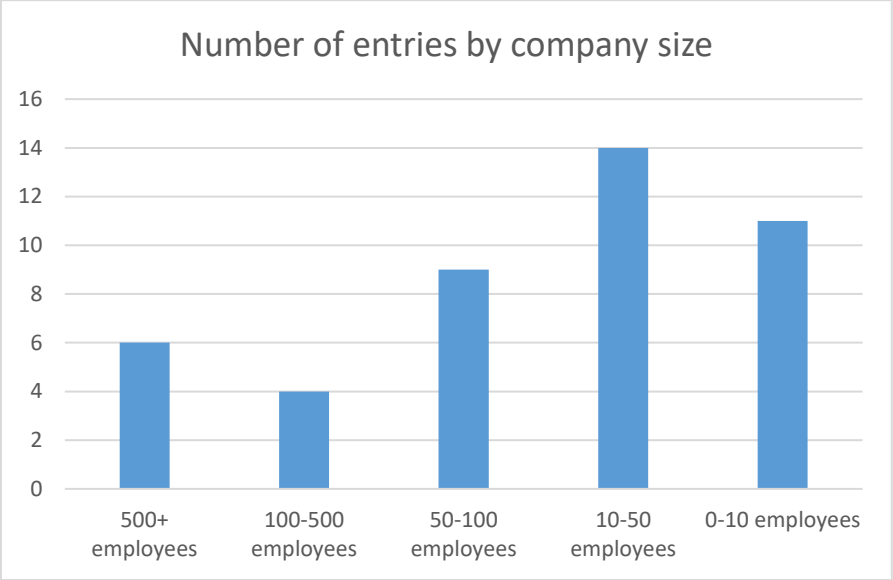

Chart 2. Distribution of participants based on company size.

Here it can be seen that majority of the participants were SME’s and a total of 10 large organizations were captured (100 employees and above).

The third and last distribution is by role in company:

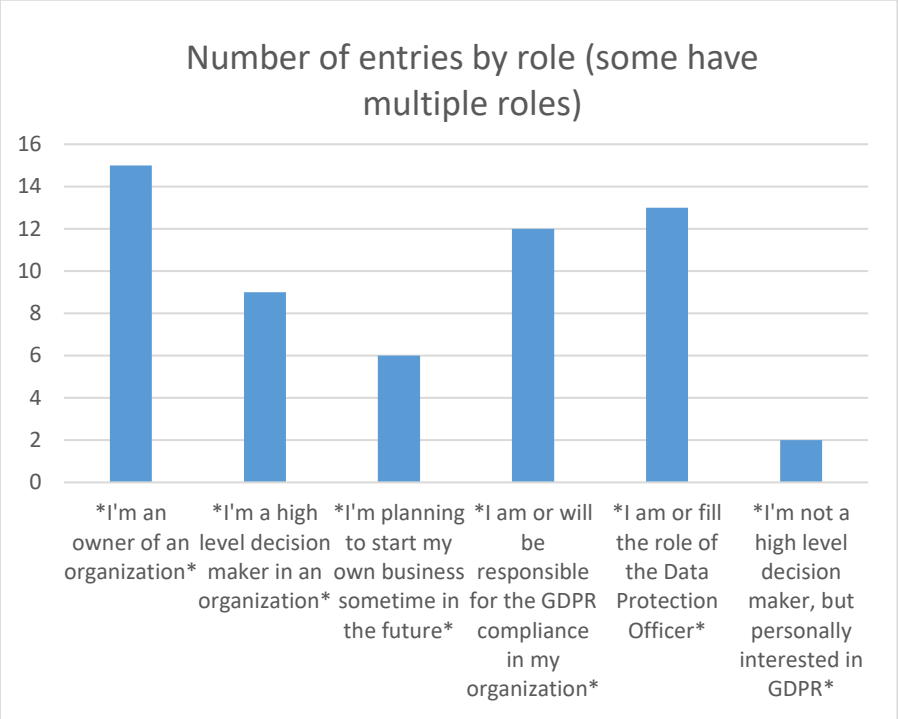

Chart 3. Distribution of participants based on role in company.

As it can be seen from the chart, the strong majority of the participants are closely associated with the GDPR. Since some people have multiple roles, some roles overlap and as a result this chart has seemingly more entries.

Now that the distributions have been presented, the results will be analysed.

Below, the general result of the survey has been brought out:

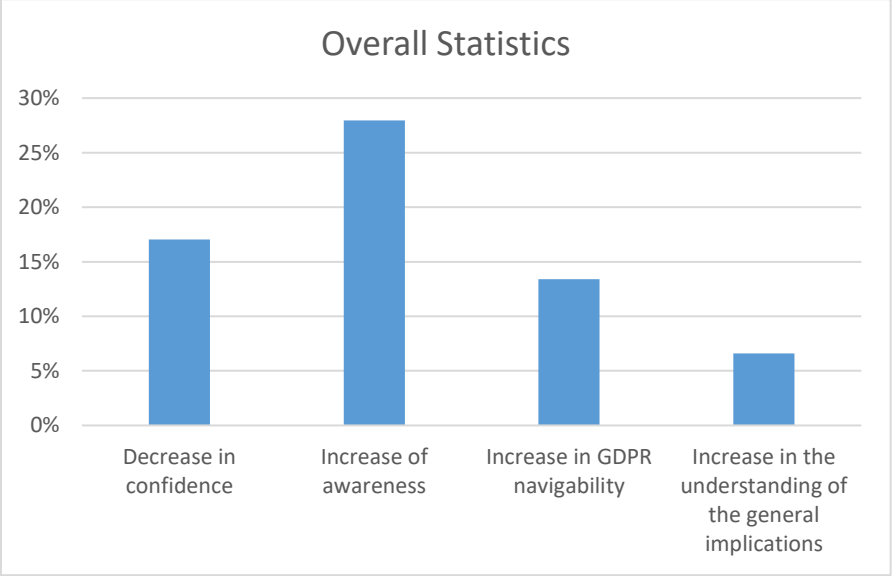

Chart 4. General result of the survey.

The general result clearly confirms the overconfidence hypothesis. In general, the level of confidence dropped by 17% in participants. The raise of awareness hypothesis is also confirmed. Generally, awareness about which articles an organization has to deal with increased 28% in participants. There was also an increase in the navigability of the GDPR, which means people perceived the GDPR less complex after completing the Article Checker, the general increase of GDPR navigability was 13%. The smallest increase was in understanding the general implications with a 7% increase.

This confirms both hypothesises that were raised in the beginning of the thesis. Not only does the research confirm that indeed self-assessment questionnaires do increase awareness, it sets a baseline for what the difference is before and after completing such an assessment, 28%. A baseline is also set for the confidence drop of using a self-

assessment questionnaire, 17%. This lays the groundwork for further research that will be described later in the thesis.

Next, the results that are based on previous experience will be analysed:

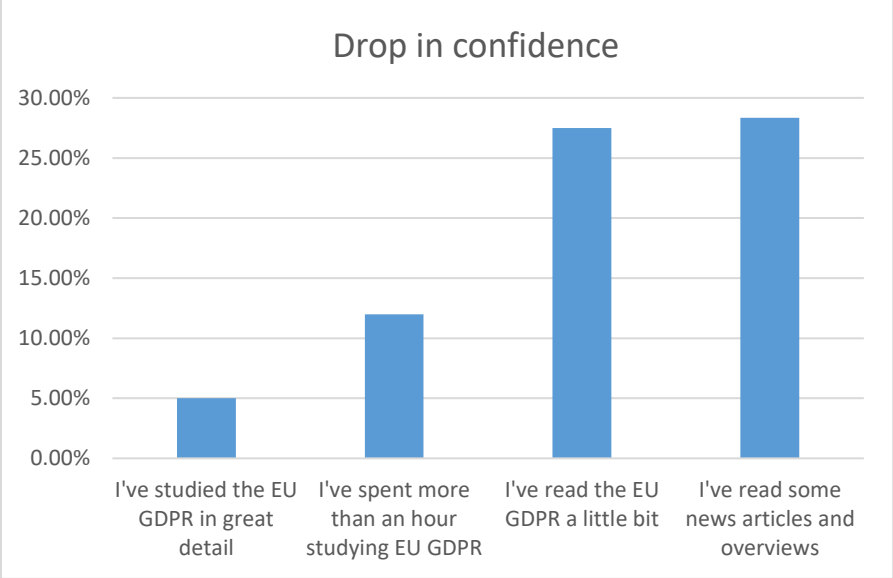

Chart 5. Drop in confidence based on previous experience with EU GDPR.

The drop in confidence was smaller in participants who are more informed about the EU GDPR. The most overconfident of compliance were people who have read the EU GDPR a little bit or just some articles and overviews. This result implies that the less informed participants did not expect that level of detail in the EU GDPR and as they were answering the questions about their own company, they realized how far they still are from compliance. This finding very strongly supports hypothesis 2.

There was also a drop in confidence, while smaller, among participants who have studied the GDPR in great detail. This can also emerge from the detailed questions that force you to analyse your business from all aspects and question your current situation.

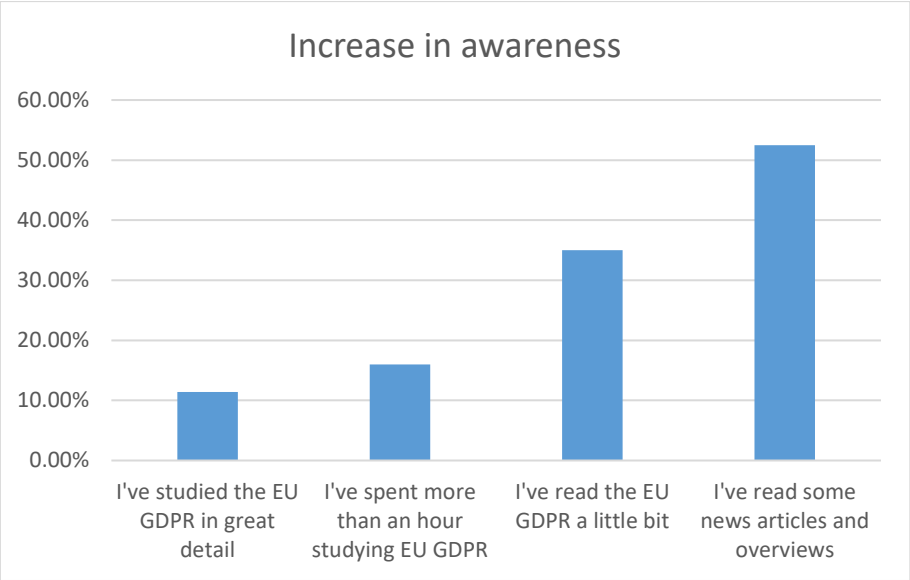

Chart 6. Increase in awareness based on previous experience with EU GDPR.

As it can be seen from this chart, the increase in awareness nicely correlates with the level of previous experience with EU GDPR. The ones who have least experience with the GDPR, gained the most out of completing the survey, in fact the participants who only read some news articles and overviews showed a significant average 52.50% increase in awareness. Also as previously predicted, the more informed induvial showed a smaller increase, as they already have a broader basis of knowledge regarding the GDPR. This adds more weight to hypothesis 1. 52.50% is a significant increase, so it not only helps raise awareness but it might make a vital difference in compliance.

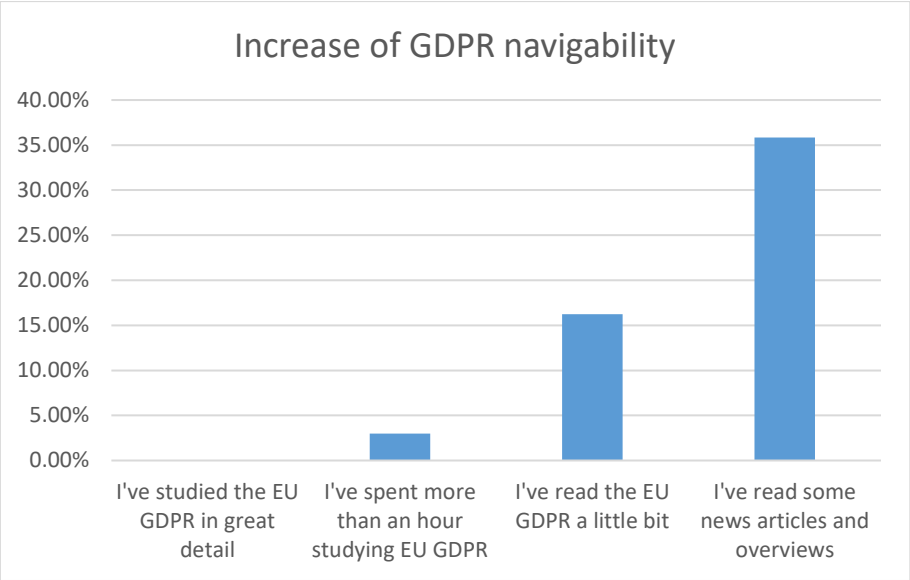

Chart 7. Increase of GDPR navigability based on previous experience with the EU GDPR.

On Chart 7 it can be seen that the ability to navigate GDPR effectively is sharply correlated with the level of previous experience, also indicating the perceived complexity of the EU GDPR through the eyes of the surveyed. The very experienced participants didn't show an increase in the ability to find information form the EU GDPR, while the participants that only read some articles and overviews showed a dramatic increase in the ability to find information. This indicates that perceived complexity was reduced the most among less informed individuals. Ability to find information from the GDPR also indicates a rise of awareness, which adds more weight to hypothesis 1.

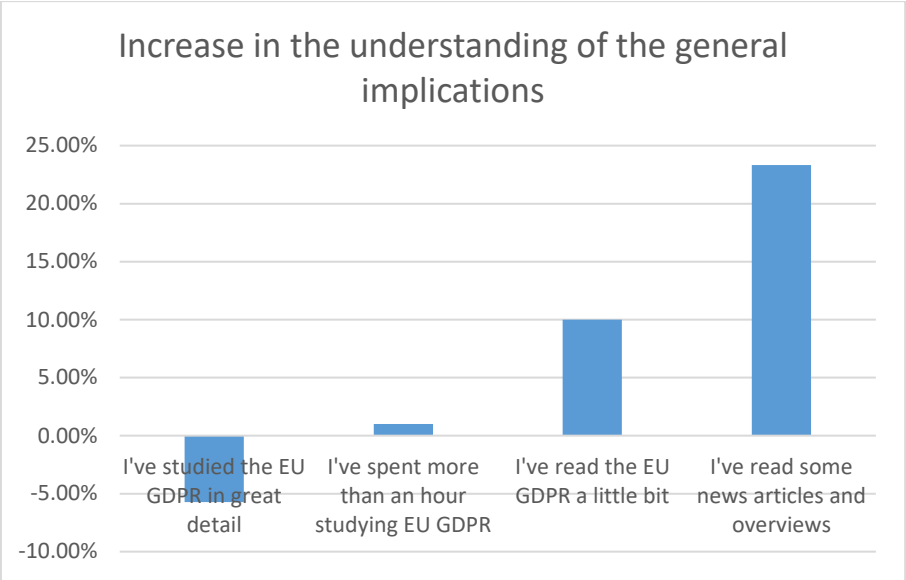

Chart 8. Increase in the understanding of the general implications based on previous experience.

As for the understanding of the general implications, the result was quite interesting. The participants who had studied the GDPR in great detail, actually showed a small drop in the understanding of the general implications, while on the other end the ones least informed about GDPR showed a significant increase. This could imply that the GDPR experts started to question their previous understanding of the GDPR after completing the very detailed Article Checker and as a result they didn't feel that confident about their knowledge afterwards, which was also predicted. Since some feedback was given to the Article Checker that some questions could be interpreted in multiple ways, the more experienced participants may have gotten slightly confused on that part and as such the negative result. This feedback can be used to improve the next iteration of the research described in future research in the end of the thesis.

This covers the analysis based on the distribution of GDPR awareness. The next distribution to be analysed is company size.

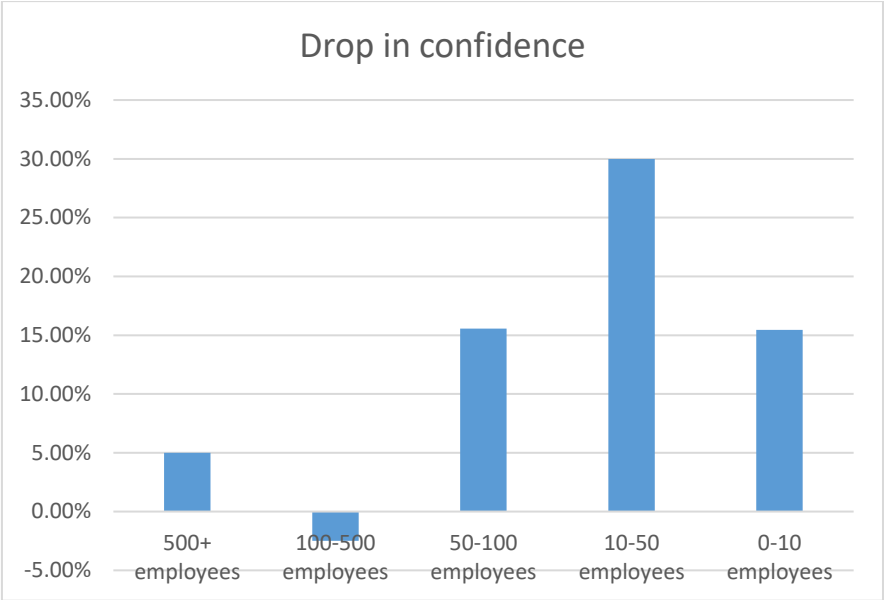

Chart. 9 Drop of confidence based on company size.

Starting with off with the first chart based on company size distribution which is drop in confidence. Here it can be seen that the 100-500 employee sized organizations showed a minor increase in confidence, this may indicate that 100-500 employee sized organizations are better prepared for GDPR. The smaller organizations were the most overconfident, this could imply that due to their size they don't have a lot of experience with different compliances in general and initially didn't worry a lot about GDPR, underestimating the requirements.

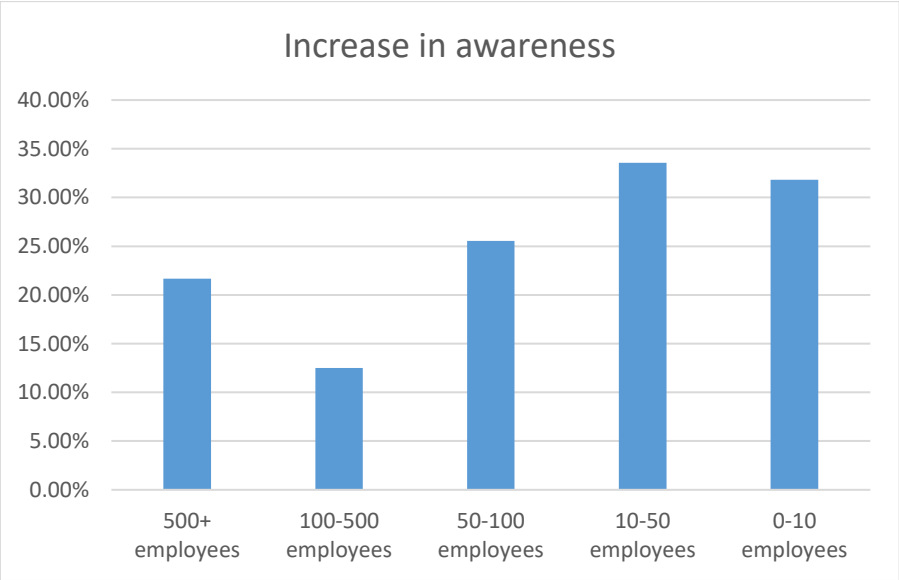

Chart 10. Increase in awareness based on company size.

As the previous chart showed, the 100-500 employee sized organizations showed the best level of confidence, it seems that they also increased in awareness the least, which may imply that they are already well informed so the effect was smaller. All-in-all the increase of awareness was significant in all sizes.

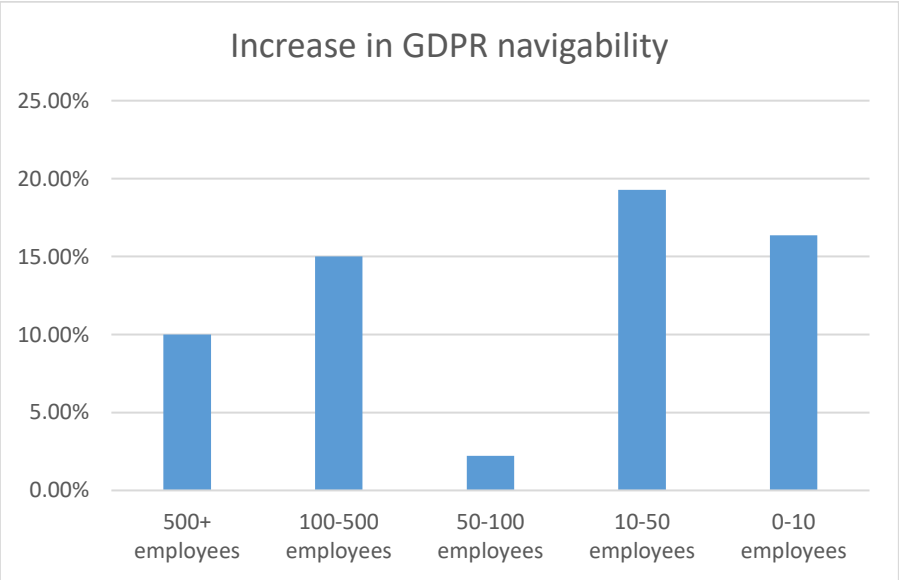

Chart 11. Increase in GDPR navigability based on company size.

Regarding navigability, in general, all sized organizations indicated an increase in the ability to find information from the GDPR, the only exception being 50-100 employee sized organizations. The result of the 50-100 employee navigability was impacted by one

individual who showed a 70% decrease in the ability to find information in the GDPR document, this could have been an error or the person simply overestimated their ability greatly and got confused afterward. As this was the only response of its kind in the research, it will be considered as an anomaly. Further research with larger target groups will most likely confirm this anomaly.

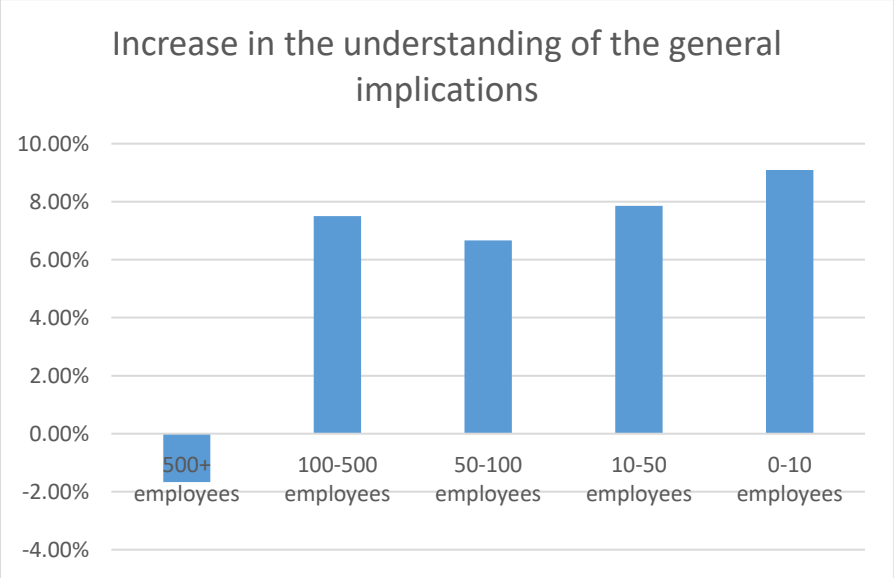

Chart 12. Increase in the understanding of the general implications based on company size.

In the case of distribution by awareness, the most informed individuals showed a decrease of understanding of the general implications and such is also the case with organizations above 500 employees. This correlation comes from the fact that most of the largest organizations also had the most informed participants. The negative result most likely has the same explanations as under the awareness distribution. All other sizes showed similar increases in the general understanding, which, once again, adds weight to the raise of awareness hypothesis.

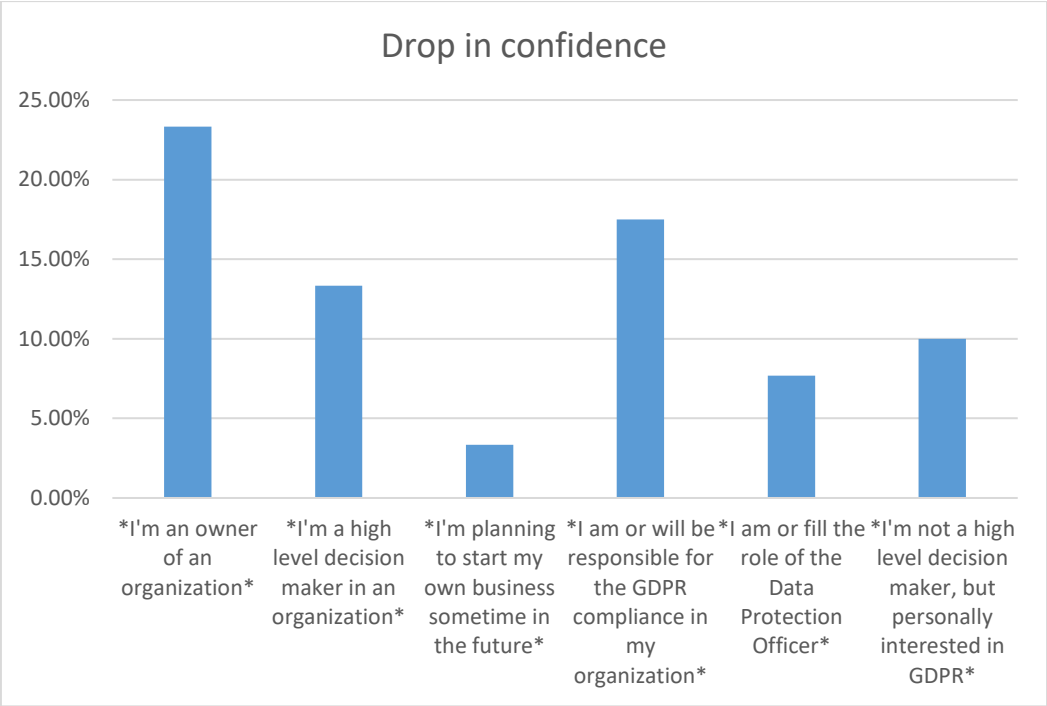

Chart 13. Drop of confidence based on the role in the organization.

This was one of the most interesting findings. It seems that owners of organizations showed the largest drop in confidence, implying that they are not completely informed about all aspects of their business and rated their company more compliant then it actually is. The second largest drop in confidence was in people who are or will be responsible for GDPR in their organization, this seems logical as they might just be getting into the topic, as they have been assigned to it and as a result had a higher confidence on the current situation in their organization. The smallest drop was observed in people planning to start their own business, which makes them the most sceptical group.

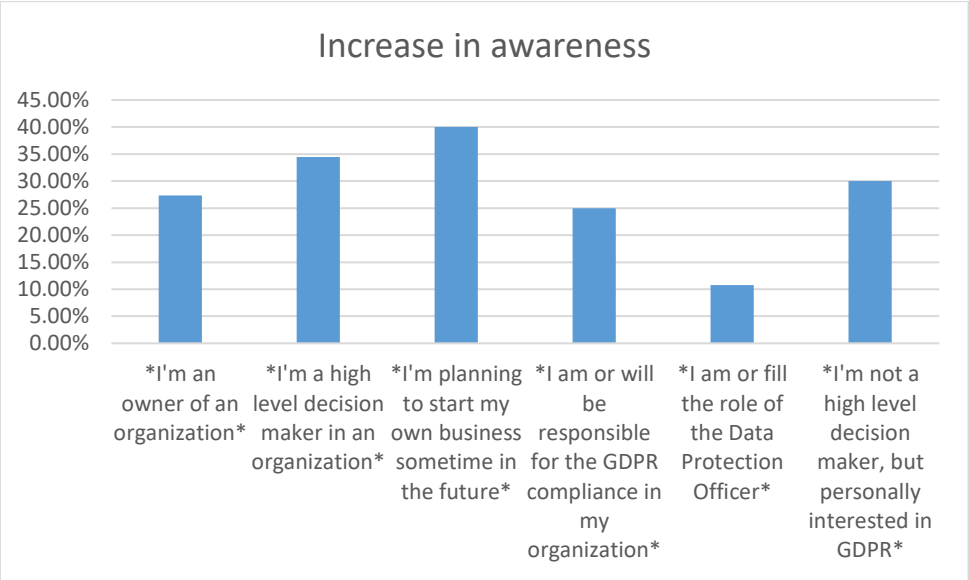

Chart 14. Increase in awareness based on the role in the organization.

As for the increase of awareness based on role, the smallest increase was among DPOs, which is logical because they are already very well informed on the topic. In general the raise of awareness of which articles need to be dealt with was quite significant in all roles. This also adds weight to the increase of awareness hypothesis.

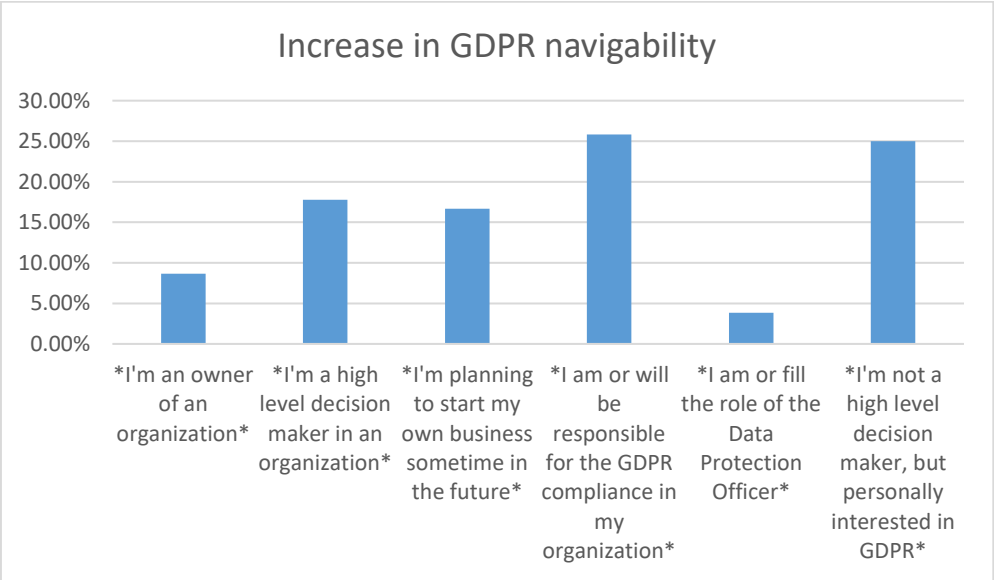

Chart 15. Increase of GDPR navigability based on the role in the organization.

Here it can be seen that the DPOs perceived the GDPR the least complex, this correlates with the previous chart on raise of awareness. It's most likely the case that DPOs have spent the most time in the EU GDPR and as a result can navigate it rather well. In general,

once again, the increase in the ability to find information from the GDPR increased quite a lot over all.

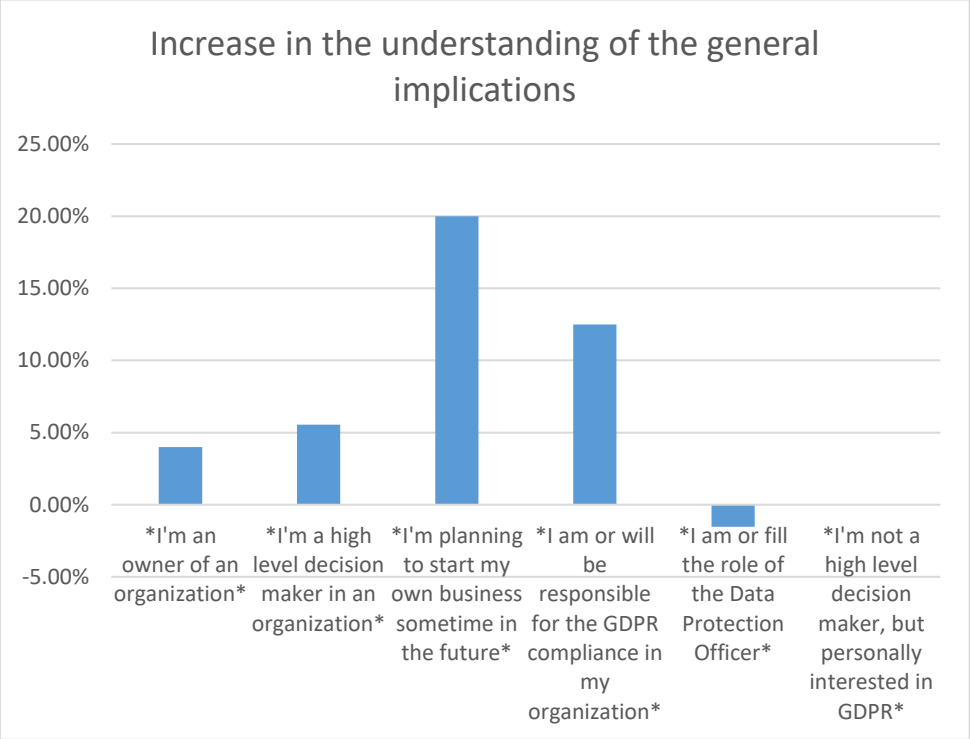

Chart 16. Increase in the understanding of the general implications based on the role in the organization.

Once again, the DPO, who is the most informed role type of the participants, shows a decrease in understanding of the general implications. As mentioned before, this could indicate that they were overwhelmed by the level of detail and as such became slightly confused or that they interpreted some of the questions in multiple ways. On the other hand, the people who are starting to plan their own business had a significant increase in understanding, which will help them take different aspects of the GDPR into account when founding their business. Adding more weight to hypothesis 1 that self-awareness questionnaires increase awareness and actually help quite a lot in preparing for compliance.

To conclude, the hypothesises brought out in research goals and purposes were validated and the results also showed direction for further research and improvement of the experiment. The less informed individuals from smaller organizations have the most benefit by completing self-assessments. Of course, a survey with 44 participants doesn't accurately portray the real situation but it does provide initial validation of the concept.

7 Summary

This thesis addressed two problems: if self-assessment questionnaires regarding GDPR really do serve their purpose and help people become compliant (and how much) and if an overconfidence exists among entrepreneurs regarding EU GDPR compliance (and how big is it).

Firstly, related works were examined and multiple alternative frameworks were considered for the experiment. None of the found solutions offered an all-in-on solution which was necessary for the confirmation of the proposed hypothesises and it was decided that in order to test these hypothesises a new questionnaire had to be created. Then EU GDPR applicability was explored and as a result research question a) was answered. After that, the articles that needed to be included in the new questionnaire were defined based on the sanctions, answering research question b). Once the articles were defined, a business model template was developed in order to understand which parts of an organization specific points in the EU GDPR influence, answering research question c). Then the self-assessment questionnaire questions were mapped out and developed into a front-end application called the Article Checker. Once all the research questions were answered, the survey was conducted and the two proposed hypothesises were confirmed as a result.

The result of the research is as follows:

1. Hypothesis 1: “Completing an EU GDPR self-assessment questionnaire will raise awareness about which articles the entrepreneur’s organization needs to be compliant with and understanding about the general implications of GDPR.” Hypothesis was confirmed and generally awareness is raised significantly, 28% and up to 52.50% in less informed entrepreneurs from smaller organizations.

2. Hypothesis 2: “Upon completing a self-assessment questionnaire, self-confidence regarding EU GDPR compliance will drop in entrepreneurs.” Hypothesis was confirmed and generally confidence drops 17% in participants and up to 30% in entrepreneurs who own smaller organizations.

3. Research questions:

a. When does EU GDPR apply to an organization? Answer: All organizations currently dealing with EU citizen's personal information.

b. In creating the self-assessment questionnaire, which articles need to be included to cover all aspects relevant to entrepreneurs? Answer: All articles defined in the EU GDPR sanctions.

c. Which components of a business do the requirements of the EU GDPR influence? The product component, the team component, the financial component and the customer component, covering all aspects of the business and different components are influenced based on different levels of compliance.

7.1 Future research

The findings set the stage for further research. From the feedback regarding the Article Checker, a "Not applicable" button was suggested and also some questions need to be reviewed that can be understood in multiple ways. As this research set the baseline of the usefulness of the self-assessment questionnaires and frameworks, future research should be done to compare different frameworks and their effect on levels of awareness and overconfidence. As a result of the future research, better self-assessment frameworks can be developed. Future research should include a larger target group and multiple, already existing, self-assessment questionnaires because an accurate global opinion can't be portrayed through a smaller study such as the one in this thesis. It is however, a positive starting point and proves that the hypothesises are true. Furthermore, as the results of this questionnaire were positive, another branch of future research would be to develop the given questionnaire into a practical solution for entrepreneurs taking into account the comparison of results from other frameworks to ensure maximum raise of awareness.

In conclusion, the proposed hypothesises were confirmed by the experiment designed in this thesis giving initial validation to the awareness raising effect of self-assessment questionnaires. It was also validated that an overconfidence exists among entrepreneurs regarding compliance and that self-assessment questionnaires can help with that. An assessment of the impact of self-assessment questionnaires was brought out for entrepreneurs in different company sizes, different awareness levels and different high-

level roles, contributing to further development of better EU GDPR self-assessment solutions.

References

[1] The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. (2014). Retrieved from https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm [Accessed: 12-Jan-2018]

[2] GDPR Portal. (2018). Retrieved from https://www.eugdpr.org/eugdpr.org.html [Accessed: 12-Jan-2018]

[3] Tikkinen-Piri, C., & Rohunen, A., & Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. (2018). Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364917301966 [Accessed: 23-Mar-2018]

[4] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59(6)*. Retrieved from https://www.bedicon.org/wp-content/uploads/2018/01/laws_topic3_source2.pdf [Accessed: 23-Mar-2018]

[5] McAllister C. (2017). WHAT ABOUT SMALL BUSINESSES? THE GDPR AND ITS CONSEQUENCES FOR SMALL U.S.-BASED COMPANIES. *Brooklyn Journal of Corporate, Financial & Commercial Law, 12(1), 12*. Retrieved from https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1263&context=bjcfcl [Accessed 23-Mar-2018]

[6] Mittal, S., & Sharma, P. (2017). THE ROLE OF CONSENT IN LEGITIMISING THE PROCESSING OF PERSONAL DATA UNDER THE CURRENT EU DATA PROTECTION FRAMEWORK. Retrieved from https://mittal.one/tag/models-of-consent/ [Accessed 23-Mar-2018]

[7] De Hert, P., & Papakonstantinou, V., & Malgieri, G., & Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Retrieved from https://ac.els-cdn.com/S0267364917303333/1-s2.0-

S0267364917303333-main.pdf?_tid=8fa33095-4daf-41d6-ac21-308c4cab5d75&acdnat=1521798899_a1486bc394dc25c21709f6d62825ffd3 [Accessed: 23-Mar-2018]

[8] Roig, A. (2017). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology, 8(3).* Retrieved from http://ejlt.org/article/view/570/771 [Accessed: 23-Mar-2018]

[9] Ogriseg, C. (2017). GDPR and Personal Data Protection in the Employment Context. *LaBoUR & Law Issues, 3(2).* Retrieved from https://labourlaw.unibo.it/article/viewFile/7573/7276 [Accessed: 23-Mar-2018]

[10] Types and Forms of Business. (2018). Retrieved from http://www.accountingverse.com/accounting-basics/types-of-businesses.html [Accessed: 12-Jan-2018]

[11] Osterwalder, A., & Pigneur, Y., & Tucci, C. L. (2005). CLARIFYING BUSINESS MODELS: ORIGINS, PRESENT, AND FUTURE OF THE CONCEPT. *Communications of AIS, 15.* Retrieved from https://www.researchgate.net/profile/Christopher_Tucci/publication/37426694_Clarifying_Business_Models_Origins_Present_and_Future_of_the_Concept/links/02e7e52d595e31e34e000000.pdf [Accessed: 12-Jan-2018]
[12] Morris, M., & Schindehutte, M., Allen, J. (2005). The entrepreneur's business model: toward a unified perspective. *Journal of Business Research, 58.* Retrieved from http://businessmodels.eu/images/banners/Articles/Morris_Schindehutte_Allen.pdf [Accessed: 12-Jan-2018]
[13] Definition of 'Product. (2018). Retrieved from https://economictimes.indiatimes.com/definition/product [Accessed: 12-Jan-2018]
[14] What is a customer?. (2018). Retrieved from http://www.businessdictionary.com/definition/customer.html [Accessed: 12-Jan-2018]
[15] What is a finance department?. (2018). Retrieved from http://www.businessdictionary.com/definition/finance-department.html [Accessed: 19-Jan-2018]
[16] GDPR Portal. (2018). Retrieved from https://www.eugdpr.org/ . [Accessed: 19-Jan-2018]
[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 1, pp 109.*
[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General

Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, pp 9.*
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 4, pp 118.*
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 4, pp 118.*
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 30&9, pp 160.*
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 3, pp 111.*
[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union,* pp *15.*
[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union,* pp *16.*
[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Chapter VIII, pp 239.*
[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 83, pp 247.*
[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 3, 11, 25-39, 42, 43.*

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 5, 6, 7, 9, 12-22, 44-49.*
[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 5, pp 118.*
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 6, pp 119.*
[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 7, pp 123.*
[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 8, pp 124.*
[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 9, pp 125.*
[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General

Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 11, pp 129.*

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 12, pp 130.*

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 13, pp 132.*

[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 14, pp 135.*

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 15, pp 139.*

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 16, pp 141.*

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 17, pp 141.*

[41] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 18, pp 143.*

[42] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 19, pp 144.*

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 20, pp 145.*

[44] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 21, pp 146.*

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 22, pp 147.*

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 25, pp 152.*

[47] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 26, pp 153.*

[48 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 27, pp 153.*

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 28, pp 155.*

[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 30, pp 159.*

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 32, pp 161.*

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 33, pp 163.*

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 34, pp 164.*

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General

Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 35, pp 165.*
[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119, Council of the European Union, Article 37, pp 171.*
[56] Don't panic! How to be compliant with the new GDPR in 5 steps. (2018). Retrieved from http://www.aki.ee/et/node/1471. [Accessed 18-Apr-2018]
[57] Data protection self assessment. (2018). Retrieved from https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/. [Accessed: 18-Apr-2018]

Appendix 1 – EU GDPR Article and question mapping for the self-assessment questionnaire

Article 5: Principles relating to processing of personal data

The main principles brought out in article 5 are as follows:

- Personal data has to be processed lawfully, fairly and transparently [29]. **Question**: Do we process data lawfully, fairly and transparently?

- Purpose limitation: only collect personal data for specified, explicit and legitimate purposes [29]. **Question**: Have we specified and displayed the purposes of collecting personal data?

- Data minimisation: only process adequate and relevant data what is necessary [29]. **Question:** Do we process more then we need to?

- Accuracy: personal data has to be accurate and kept up to date [29]. **Question:** Do we have measures to keep the data accurate and up to date?

- Storage limitation: only keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes of processing [29]. **Question:** Do we keep personal data only for the duration necessary for processing?

- Integrity and confidentiality: appropriate security for personal data processing including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage [29]. **Question:** Do we have appropriate security for personal data processing?

It's important to note that the controller is responsible for demonstrating compliance regarding previous points, so it is recommended to prepare for proof [29].

Article 6: Lawfulness of processing

Article 6 states that processing has to be lawful and it is lawful only if one of the following points apply:

- Data subject has given consent for processing their personal data for specific purposes [30]. **Question:** Do we collect consent for personal data specifically for each different purpose?

- Processing is necessary regarding a contract that the data subject is a party to or in order enter into a contract by the prior request of the data subject [30]. **Question:** Do we require personal information processing regarding a contract we are in or planning to enter into with the data subject? Does the data subject want to enter into a contract and we require processing for that reason?

- Personal data has to be processed regarding the controllers compliance with other legal obligations [30]. **Question:** Do we or does the controller whose data we process have other legal obligations that require the processing of personal data of data subjects?

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person [30]. **Question:** Do we need to process the data to protect the vital interests of the data subject?

- Processing is necessary for the performance of a task carried out in the public interest [30]. **Question:** Do we need processing for a task in the public interest?

- Processing is required for legitimate interests pursued by the controller or by a third party, these interests cannot conflict with fundamental rights and freedoms of a data subject which require protection of personal data [30]. **Question:** Do we provide easily understandable and accessible activity logs of processing? (Interests cannot conflict with fundamental rights and freedoms of the data subject)

Article 7: Conditions for consent

Certain conditions apply for consent that are the following:

- When the processing is based on consent the controller has to be able to demonstrate that the data subject has consented to the processing of their personal data [31]. **Question:** Can we prove that the data subject has given consent to processing of personal data?

- If the consent declaration is written which also concerns other matters then the request for consent has to be presented in a way that is clearly distinguishable from other matters and is easily understandable. If some points in that declaration infringes on the EU GDPR then those points are not binding [31]. **Question:** Are we asking for consent for multiple purposes? Are those purposes clearly distinguishable in the request for consent?

- Data subjects can withdraw consent at any time. Any processing done before that is lawful. It also has to be as easy to withdraw consent as to give it [31]. **Question:** Is it as easy to withdraw consent for each purpose as easily as it is given?

- Consent has to be freely given. Which means the data subject cannot be manipulated into giving consent through degrading performance of a contract that would otherwise not need that personal information [31]. **Question:** If the data subject doesn't give consent do we maintain access to areas of the contract (service, business relationship etc.) that do not require personal information?

Article 8: Conditions applicable to child's consent in relation to information society services

A good example of an information society service is a social media site and since children use them a lot, there are special conditions of consent regarding a child. These are as follows: [32]

- Consent is lawful if the child is at least 16 years old. If the child is below that age then consent has to be given by the holder of parental responsibility of that child [32]. **Question:** Do we have customers or users under the age of 16? Do we have means to gain consent from the holder of parental responsibility of that child?

- The controller has to make reasonable efforts to verify if the consent given or authorized by the holder of parental responsibility [32]. **Question:** Do we have methods to verify the consent given by the holder of parental responsibility?

Article 9: Processing of special categories of personal data

There are certain types of personal data that is treated differently, these include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union memberships, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. These types of data cannot be processed unless one of the following points apply: [33]

- Explicit consent is given for a specific purpose [33]. **Question:** Do we process special categories of personal data? Do we ask for explicit consent for each specific purpose we need the data for?

- Processing is necessary for the purposes of carrying out the obligations regarding employment and social security and social protection law, so far as it is authorized by Union or Member State law or a collective agreement according to the Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject [33]. **Question:** Is the processed data required for obligations regarding employment, social security or social protection law?

- Protect vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [33]. **Question:** Do we need the data in order to protect the vital interests of the data subject or of another natural person in the case the data subject is physical or legally incapable of giving consent?

- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing is related to solely to the members or to the former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without consent of the data subjects [33]. **Question:** Are we any of the following: foundation, association, not-for-profit body with a political, philosophical, religious or trade-union aim? Do we need the data for only the legitimate activity of our organization regarding solely to the members or to the former members or to people who have regular contact with our organization? Do we disclose the data outside of our organization without the consent of data subjects?

- Processing is related to personal data that is made public by the data subject in a clear and understandable way [33]. **Question:** Regarding the special category of data we process, is it related to personal data that has been made public by the data subject in a clear and understandable way?

- Processing is necessary for establishment, exercise or defence of legal claims or if a court is acting in their judicial capacity [33]. **Question:** Do we process data regarding legal claims we are dealing with?

- Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law. It has to be proportionate to the aim pursued [33]. **Question:** Is the processing necessary regarding substantial public interest (according to Union or Member State law)?

- If processing is necessary regarding medical reasons. Only a professional subject with the obligation of professional secrecy under Union or Member State law or rules may process this data [33]. **Question:** Is the processing required regarding medical reasons? Is the processor a professional subject with the obligation of professional secrecy?

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats or ensuring high standards of quality and safety of health care and of medicinal products or medical devices [33]. **Question:** Are we processing personal data for the reason of public interest in the area of public health (such as serious cross-border threats or medicinal products or medical devices)?

- Processing is necessary for archiving purposes in public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) which states what appropriate safeguards have to be used [33]. **Question:** Do we deal with archiving of personal data in public interest, scientific, historical or statistical research?

Article 11: Processing which does not require identification

If the controller no longer processes personal data or no longer requires the identification of a data subject then the controller is not obliged to maintain, acquire and process additional information in order to identify the data subject only for the reason of being compliant with EU GDPR. [34]

In the case where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In a case such as that articles 15 to 20 will not be applicable. There is also an exception in the case where the data subject for the purpose of exercising his or her rights under those articles provides additional information enabling his or her identification. [34]

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

The given article focuses on transparency and the ability for the data subject to exercise their rights. The following points need to be considered: [35]

- The controller has to take appropriate measures to provide any information either given by the data subject or obtained by other means and any communication under articles 15-22 and 34 relating to processing to the data subject in an easily understandable written form. Essentially this means easily understandable and accessible activity logs of processing activities [35]. **Question:** Do we provide easily understandable and accessible activity logs of processing activities to our customers?

- The controller has to make it easy for the data subject to exercise their rights under articles 15-22. The controller cannot refuse to act on the request of a data subject when they are exercising their rights under articles 15-22, unless the controller can demonstrate that it is not in position to identify the data subject [35]. **Question:** Have we made it easy for the data subject to exercise the following rights: right of access (Article 15), right to rectification (Article 16), right to erasure (Article 17), right to restriction of processing (Article 18), notification obligation regarding rectification or erasure (Article 19), right to data portability (Article 20), right to object (Article 21), automated individual decision-making and profiling (Article 22)? This question will be answered through questions in the named articles.

Article 13: Information to be provided where personal data are collected from the data subject

Article 13 focuses on personal data that the data subject gives to the controller, the controller then has to present the data subject with all of the information listed below, and at the time of collection (good example is a registration form): [36]

Question: Does the data subject provide the information to us?

- Identity and contact details of the controller or the controller's representative [36]. **Question:** At registration (or time of data collection) do we present identity and contact details of ourselves?

- Contact details of the data protection officer (if required) [36]. **Question:** Do we have a data protection officer? At registration (or time of data collection) do we provide the contact details of the data protection officer (if applicable)?

- Purposes for processing that personal data and the legal basis of it [36]. **Question:** At registration (or time of data collection) do we display the purposes of processing and the legal basis of it clearly?

- If processing is based on point f of article 6(1), the legitimate interests pursued by the controller or a third party [36]. **Question:** Is the processing based on legitimate interests pursued by the controller or a third party? At registration (or time of data collection) do we display legitimate interests of a controller or a third party clearly?

- Recipients or categories of recipients of the personal data [36]. **Question** At registration (or time of data collection) do we display recipients or categories of recipients of the personal data?

- If the controller intends to transfer personal data to a third country or an international organisation, then appropriate safeguards and means have to be presented alongside by methods which to obtain a copy of that data or where that data has been made available at [36]. **Question:** At registration (or time of data collection) do we present appropriate safeguards and means alongside methods to

obtain a copy of that data or where that data has been made available at (if applicable)?

- Period of how long the data is stored, if not possible to determine then presenting the criteria used to determine the period of data storage is also appropriate [36]. **Question:** At registration (or time of data collection) do we display the duration of data storage or the criteria that determines the period?

- The right to enforce the right-to-be-forgotten, meaning data rectification or erasure and also the right to data portability needs to be shown [36]. **Question:** At registration (or time of data collection) do we inform the data subject of the right to data portability, rectification and erasure?

- If processing is based on consent given by the data subject, the data subject has to be able to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal [36]. **Question:** Is the data subject able to withdraw consent at any time?

- It must also be presented that the data subject has the right to lodge a complaint with a supervisory authority [36]. **Question:** At registration (or time of data collection) do we display the right to lodge a complaint with a supervisory authority?

- It must be clear if personal data is necessary to enter into a contract, as well as whether the data subject has to provide the data and possible consequences of failure to do so [36]. **Question:** At registration (or time of data collection) is it clear that personal data is necessary to enter into a contract?

- If automated decision-making exists, including profiling, meaningful information about the logic involved has to be provided, as well as the significance and the envisaged consequences of such processing for the data subject [36]. **Question:** Do we do automated decision making or profiling? At registration (or time of data collection) if automated decision-making exists, including profiling, do we provide the data subject with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing?

- If the controller wants to process the personal data further for other purposes that were initially defined, then extra consent has to be acquired and explanations given [36]. **Question:** Do we process or want to process personal data further for other purposes that we initially defined?

- If the data subject already has all the above information, then they don't have to be displayed again on every cycle [36]. **Question:** Do we provide all of the information required in the case the data subject provides us with data at least once?

Article 14: Information to be provided where personal data have not been obtained from the data subject

This article handles the situation where data has been acquired from other sources either public or private, if the data has not been obtained from the data subject the controller has to do the following: [37]

Question: Is the data about the data subject collected automatically?

- Again, the identity and contact details of the controller and the data protection officer if applicable [37].

- Purposes of processing and legal basis [37].

- Categories of personal data obtained [37]. **Question:** Do we display categories of personal data obtained?

- The list of recipients or their categories of who receives personal data [37]. **Question:** Do we display the recipients or the categories of recipients of that data?

- Also again if the controller intends to transfer personal data to a recipient in a third country or international organization appropriate safeguards and means to obtain a copy of the data and where it has been published have to be presented [37].

- From which source the personal data has been obtained from and if it came from publicly accessible sources [37]. **Question:** Do we display where the personal data has been obtained from and if it came from public sources?

- All other points that overlap with article 13.

- The information above has to be provided to the data subject within reasonable time or at maximum within one month of collection [37]. **Question:** Do we inform people of automated data collection within one month of doing so?

- If the obtained personal data is used for communication with the data subject then that information has to be presented at first contact [37]. **Question:** Do we collect the personal data for communication intent? Do we present all the available information at first contact?

- If data disclosure to a third party is contemplated then the information has to be provided when the data is first disclosed [37]. **Question:** Do we disclose data to third parties or contemplate to do so? Do we provide the required information to the data subject when the data is first disclosed?

- An in the same way as Article 13 if the data subject already has all of this information, then it does not have to be presented again [37].

Article 15: Right of access by the data subject

Article 15 states that a data subject can ask a controller for confirmation to whether or not personal data concerning him or her are being processed, and if that is so, he or she can ask for access to the personal data and the following information: [38]

- Why is this data being processed [38]? **Question:** Can we tell the data subject clearly why we process the data within one month?

- Categories of personal data under question [38]. **Question:** Can we provide categories of personal data to the data subject under question within one month?

- List of recipients and categories of recipients who the personal data has been disclosed to, especially if recipients are in third countries or international organizations [38]. **Question:** Can we provide the list of recipients and categories of recipients who the personal data has been disclosed to the data subject within one month?

- Period of how long the data is intended to be kept or if not possible then the criteria to determine storage period [38]. **Question:** Can we provide the data subject with the information on how long the data is intended to be kept or the criteria determining the period within one month?

- To make a request to enforce the right-to-be-forgotten and the right to lodge a complaint [38]. **Question:** Can we execute the right-to-be-forgotten within one month upon request?

- If personal data has not been collected from the data subject, information to their source has to be disclosed [38]. **Question:** Can we disclose all data sources where the data has been found from within one month?

- Explanations of the automated decision-making if applicable [38]. **Question:** Can we provide explanations of automated-decision making in a clear way in one month?

- The controller has to provide a copy of personal data undergoing processing [38]. **Question:** Are we able to provide a copy of personal data undergoing processing?

Article 16: Right to rectification

The given article is short and concise: the data subject has the right to request the controller the correction of incorrect personal data concerning him or her. Depending on the purpose of the processing, the data subject has the right to have incomplete personal data completed through providing additional information. [39] **Question:** Are we capable of correcting incorrect personal data concerning the data subject within one month upon request?

Article 17: Right to erasure ('right to be forgotten')

Article 17 is one of the most spoken of in the EU GDPR, the famous right to be forgotten. It states that the data subject has the right to have his or her personal information erased with undue delay and the controller has the obligation to proceed with that request if one of the conditions in Article 17 point 1 apply. [40]

If the request comes in to a controller and the data is made public, then the controller has to make reasonable efforts to inform other controllers which are processing that personal data to remove any links to, copy or replication of that personal data. [40] However, reasonable effort is vaguely described. A controller has to take into account available technology, cost of implementation and technical measures. [40] **Question:** Regarding public data, are capable of forwarding the right-to-be-forgotten request to all other controllers that link to, have a copy or have replicated that personal data?

Right to be forgotten doesn't apply if the processing is required for exercising the right of freedom of expression and information or if it's required by law, necessary for the a task carried out in public interest or in the exercise of official authority vested in the controller, public interest in the area of public health, for archiving purposes in the public interest, scientific, historical, statistical purposes or the defence of legal claims. [40] **Question:** Do we require processing for the following reasons: exercising the right of freedom of expression and information, required by law, necessary for the task carried out in public interest or exercise of official authority, public interest in the area of public health, achieving purposes in the public interest, scientific, historical, statistical reasons or defense of legal claims?

Article 18: Right of restriction of processing

A data subject has the right to restrict processing of personal data if any of the following points apply: [41]

Question: Are we capable of restricting processing of certain data on demand without hindering business and IT systems in general?

- The data subject contests the accuracy of the data, restricting processing until the controller verifies the accuracy of the data [41]. **Question:** Are we capable of proving the accuracy of the data we hold?

- The data subject has to be informed before the restriction is lifted [41]. **Question:** Do we inform data subjects before the requested restriction is lifted and processing continues?

Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller has to inform the data subject of any rectification or erasure of personal information or restriction of processing carried out and to each recipient to whom the personal data has been disclosed, unless it is impossible or involves disproportionate effort. The controller also has to inform the data subject about those recipients if the data subject requests it. [42] **Question:** Do we inform the other recipients to who the personal data has been disclosed about rectification, erasure or restriction?

Article 20: Right to data portability

The data subjects have the right to receive the personal data concerning them which they have provided to the controller in a structured, commonly used and machine-readable format, and the data subject also has the right to transmit that data to another controller without hindrance from the controller to which the personal data has been provided to. [43] **Question:** Are we capable of providing full copies of personal information of data subjects in a structured, commonly used and machine-readable form?

The data subject also has the right to request that the personal data is transmitted directly from one controller to the other, if technically feasible. [43] **Question:** Are we technically capable of forwarding the personal information directly to another controller?

Article 21: Right to object

The data subjects have the right to object at any time to processing of personal data concerning him or her which is based on lawfulness of processing, including profiling based on those provisions. [44] **Question:** Do we do automated-decision making or profiling?

In the case of direct marketing, if the data is processed for that purpose, the data subject has the right to object at any time to processing of their personal data. [44] **Question:** Do we do direct marketing? Are we capable of complying with objections technically and business wise?

Upon first communication with the data subject, the right referred to above has to be explicitly brought to the attention of the data subject and it has to be presented clearly and separately from other information [44]. **Question:** Upon first communication with the data subject do we make the right to object explicitly clear and separate from other information?

In the case of scientific, historical or statistical purposes. The data subject will still have the right to object to processing of personal data, unless the processing is necessary for reasons of public interest. [44]

Article 22: Automated individual decision-making, including profiling

The data subject has the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects or something of similar significance to him or her. This doesn't apply if it's based on the data subject's explicit consent. [45] **Question:** Do we have consent for automated decision-making and profiling?

In the case such technology exists, the data controller has to have suitable measures to safeguard the data subject's rights and freedoms. Methods have to exist for human intervention on the part of the controller regarding the automated processes. The data subject has the right to contest the decision. [45] **Question:** Do we have methods in place for human intervention in automated processes regarding decision making and profiling?

Article 25: Data protection by design and by default

One of the key messages in EU GDPR is that data should be protected by design and by default. **Question:** Do we practice data protection by design and by default?

The controller has to take into account the state of the art, cost of implementation, scope, nature, context and purpose of processing as well as the risks involved. The goal is to protect the rights and freedoms of natural persons. The controller has to implement appropriate technical and organizational measures, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing, such as pseudonymsation and other methods in order to meet the requirements of EU GDPR and protect the rights of the data subjects. [46] **Question:** Based on our business, do we have appropriate cyber security (both technical and non-technical) in place regarding all aspects of personal data storage and processing?

Technical and organisational measures have to be in place that ensure that only personal data which is necessary for each specific purpose of the processing is processed. Such measures have to ensure that personal data is not made accessible, without the individual's intervention, to an indefinite number of natural persons. [46] In essence, this

means that the measures should prevent data leaks, which puts an emphasis on data leak prevention. **Question:** Are our both technical and organisational cyber security methods sufficient to prevent data leaks?

EU GDPR also defines a certification mechanism that can display compliance to these points [46]. Getting certified will give clarity on if the measure are appropriate.

Article 26: Joint controllers

The joint controller's article describes when two or more controllers jointly determine the purposes and means of processing.

Joint controllers have to operate in a transparent manner and determine their respective responsibilities with each other for the compliance [47]. **Question:** Are we a joint controller?

Article 27: Representatives of controllers or processors not established in the Union

In the case the controller or the processor is not established in the EU, they have to designate a representative in the Union [48].

This won't apply to a public authority or body or in the case the processing is occasional, doesn't include at a large scale processing of special categories of data or processing of personal data related to criminal convictions and offences and is unlikely to result in a risk to the rights and freedoms of natural persons [48]

Question: Are we established outside of the EU?

Article 28: Processor

Article 28 describes the role of the processor in detail.

If processing is carried out on behalf of a controller, the controller shall use only processors who are compliant with the EU GDPR [49]. **Questions:** Are we processing anything on behalf of a controller?

The processor can't engage with another processor without prior specific written authorization of the controller. If the authorization is in place, the processor has to inform

the controller of any intended changes, so they would have the opportunity to object to them. [49]

Processing by a processor has to be governed by a contract or other legal act that will describe the subject-matter, duration, nature and purpose, type of personal data, categories of data subjects and the obligations and rights of the controller. That contract or legal act stipulates: [49]

- To process the personal data only on documented instructions from the controller [49]. **Question:** Do we process personal data only based on documented instructions from the controller?

- Ensures that persons who process the personal data have committed to confidentiality [49]. **Question:** Do the people who process the personal data on our side have NDA's or any other confidentiality commitment in place?

- All measures required for security of processing must be filled [49]. **Question:** Have we filled all the security of processing requirements? This question will be answered by the questions of security of processing Article.

- If the processor uses another processor, then that processor also has to be fully compliant and in the case of non-compliance, the first processor is fully liable [49].

- The contract or legal act has to be in writing, including electronic form [49]. **Question:** Does our contract or legal act exist in writing and electronic form?

Article 30: Records of processing activities

EU GDPR puts a lot of emphasis on recording processing activates, Article 30 describes this in detail.

Question: Should we keep records of processing activities?

Each controller and controller's representative (if applicable) has to maintain a record of processing activities under its responsibility. Those records have to contain the following information [50]:

- Name and contact details of the controller and if applicable the join controller, the controllers representative and the data protection officer [50]. **Question:** Do we keep track of names and contact details of the controller, joint controller or the controller's representative and the data protection officer?

- Purpose of processing [50]. **Question:** Do we keep track of the purpose of the processing?

- Description of the categories of data subjects and categories of personal data [50]. **Question:** Do we keep track of the categories of data subjects and categories of data we process?

- Categories of recipients to whom the personal data has been or will be disclosed to [50]. **Question:** Do we keep track of categories of recipients to who the personal data has been disclosed to?

- Transfers of personal data to a third country or international organization and the details of either the country or the organization [50]. **Question:** Do we keep track of transfers of personal data to third countries or international organizations? Do we keep track of the details of these countries and organisations?

- If possible, envisaged time limits for erasure of different categories of data [50]. **Question:** Do we keep track of envisaged time limits of different categories of data?

- If possible, general description of the technical and organisational security measures [50]. **Question:** Do we keep track of the technical and organisational security measures?

Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller:

- Name and contact details of the processors and for each controller on behalf of which the processor is acting and the data protection officer [50]. **Question:** Do we keep track of names and contact details of the controller, joint controller or the controller's representative and the data protection officer?

- Categories of processing carried out on behalf of each controller [50]. **Question:** Do we keep track of the categories of processing carried on behalf of each controller?

- Transfers of personal data to third country or international organization [50].

- If possible, a general description of the technical and organisational security measures [50].

Records have to be kept in writing, including electronic form. If the supervisory authority requests it, the controller or the representative of the controller will make it available upon request. [50] **Question:** Do we keep the records in writing or electronic form?

In the case the organisation is employing fewer than 250 persons and unless the processing it carries out is not likely to result in a risk to the rights and freedoms of the data subjects, the processing is occasional, or the processing doesn't include the special categories of data, then the processor doesn't have to keep these records. [50] **Question:** Do we do any of the following: employ more than 250 people, process special categories of personal data, process more than occasionally or does our processing result in a risk to the rights and freedoms of the data subjects?

Article 32: Security of personal data

This article dictates the points required for the security of processing, taking into account the state of the art, costs of implementation, nature, scope, context and purposes of processing, as well as the risk associated. The controller and the processor, according to the situation have to apply the following methods of security: [51]

- Pseudonymisation and encryption of personal data [51]. **Question:** Do we pseudonymise and encrypt personal data?

- Ensuring ongoing CIA (confidentiality, integrity, availability) and resilience of processing systems and services [51]. **Question:** Do we have a plan in place to ensure ongoing CIA and resilience of processing systems? Do we have redundancy plans or measures for processing systems?

- In the case of a physical or technical incident, it must be ensured that the personal data can be accessed and made available in a timely manner [51]. **Question:** Do we have backups of personal data stored? Can we restore backups fast in the case of a physical or technical incident?

- A process must be established to regularly test, assess and evaluate the effectiveness of the technical and organizational measures, to ensure the security of processing [51]. **Question:** Do we have a process in place to test and assess our security measures regularly?

When the appropriate level of security is assessed, the risks presented by processing have to mitigated, in particular if the risks include accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data [51]. **Questions:** Have we mapped our security risks and planned mitigation accordingly?

It also has to be made sure that if any natural person has access to the data under the control of the controller or the processor, then this person should only execute instructions specified by the controller or the processor [51]. **Question:** Does any natural person have access to the data controlled or processed? Is the interaction with this data logged or monitored?

Article 33: Notification of a personal data breach to the supervisory authority

The EU GDPR has strictly defined that when a personal data breach occurs, the controller has to report it as fast as possible as and not later than 72 hours after having become aware of it [52]. **Question:** Do we have an action plan in the case of a data breach?

If the processor becomes aware of a personal data breach, they have to notify the controller immediately [52].

The notification has to contain the following:

- Describe the nature of the data breach, the categories and approximate number of data subjects affected and the categories and approximate number of personal data records affected [52].

- Contact details of the data protection officer or other contact point [52].

- Describe the likely consequences of the personal data breach [52].
- Describe the measures that will be taken by the controller to address the data breach, including measures to mitigate the effects, if possible [52].

The controller has to document all personal data breaches, comprising of the facts related to the incident, its effects and remedial action taken. This documentation will be the basis of verifying compliance with EU GDPR. [52] **Question:** Do we have a process for documenting data breaches?

Article 34: Communication of a personal data breach to the data subject

It's not only enough to notify the supervisory authority if the data breach is likely to result in a high risk to the rights and freedoms of naturals persons, in that case the controller has to communicated the personal data breach to the data subject right away [53].

The notification must be in plain language and contain the nature of the data breach, described in the same way as in article 33. Data subjects don't have to be notified if the leaked data is unintelligible (such as encrypted), if the high risks regarding the data leak are not likely to materialise, it would involve disproportionate effort. In the case of disproportionate effort, public communication or a similar measure will be used. [53]

Question: Does our breach notification plan of action also contain a plan on how to notify the data subjects?

Article 35: Data protection impact assessment

In the case of processing where the processing is likely to result in high risk to the rights and freedoms of natural persons, the controller, before processing, has to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data [54]. **Question:** Do we need a data protection impact assessment? Do we process anything that may result in high risk to the rights and freedoms of natural persons?

The data protection impact assessment is particularly required if:

- Processing is a systematic and extensive evaluation of personal aspects relating to natural persons which may be based on automated processing, also profiling and if based on that processing legal effects concerning the natural person or similarly

significant effects occur [54]. **Question:** Do we do large scale systematic evaluation of personal aspects related to natural persons?

- If the processing processes a large scale of special categories of data [54]. **Question:** Do we process large quantities of special category data?

- Systematic monitoring of a publicly accessible area on a large scale [54]. **Question:** Do we monitor a publicly accessible area on a large scale?

Article 37: Designation of the data protection officer

This article defines when a data protection officer has to be appointed. **Question:** Do we need a data protection officer?

A controller and the processor has to have a data protection officer in the cases where:

- The processing is carried out by a public authority [55]. **Question:** Are we a public authority?

- If the core activities of the controller or the processor consist of processing operations which by their nature require regular and systematic monitoring of data subjects on a large scale [55]. **Question:** Is one of our core activities either systematic monitoring or processing personal data of data subjects at a large scale?

- If large quantities of special categories of data are processed [55]. **Question:** Do we process large quantities of special categories of data?

Question: Do we need a data protection officer? Answered by the questions above.

Appendix 2 – Source code for the front-end application

http://eugdpr.scienceontheweb.net/

Appendix 3 – Raw data of the survey results

Q1 - On a scale of 1 to 10 how ready do you think your organization is regarding the EU GDPR now?

Q2 - On a scale of 1 to 10 how well do you know which specific Articles of the EU GDPR your organization has to deal with?

Q3 - On a scale of 1 to 10 how well can you find the relevant information to your organization from the EU GDPR document?

Q4 - On a scale of 1 to 10 rate your general understanding of the implications of the EU GDPR to your organization.

Q1 RE - After completing the Article Checker - On a scale of 1 to 10 how ready do you think your organization is regarding the EU GDPR now?

Q2 RE - After completing the Article Checker - On a scale of 1 to 10 how well do you know which Articles of the EU GDPR your organization has to deal with now?

Q3 RE - After completing the Article Checker - On a scale of 1 to 10 how well can you find the relevant information to your organization from the EU GDPR document now using the result of the Article Checker?

Q4 RE - After completing the Article Checker - On a scale of 1 to 10 rate your general understanding of the implications of the EU GDPR to your organization now.

Q1	Q2	Q3	Q4	Q1 RE	Q2 RE	Q3 RE	Q4 RE
7	10	8	9	7	10	8	9
4	1	1	4	2	3	1	2
5	2	2	4	1	8	6	6
7	7	4	7	2	9	7	9

2	2	2	3	2	5	5	5
2	3	9	8	2	2	2	2
6	5	2	5	4	8	9	9
7	9	8	9	8	9	9	9
8	9	10	10	9	10	3	2
7	7	2	9	7	8	2	9
1	4	10	7	1	5	3	6
4	1	3	3	1	8	7	7
7	8	9	10	4	9	10	10
6	10	10	10	5	10	10	10
6	4	5	8	2	9	8	9
3	1	2	5	8	10	6	10
6	5	8	8	6	8	8	7
8	4	6	6	6	5	4	8
8	9	4	10	5	10	3	10
9	3	5	8	9	7	8	7
8	8	10	10	5	10	10	10
8	6	9	10	9	8	10	10
3	4	2	5	1	8	8	6
4	1	4	6	2	9	10	8
7	2	2	4	3	10	8	7

9	8	9	9	7	10	10	10
8	7	5	9	4	9	7	9
8	8	6	9	8	9	9	9
5	4	5	4	2	10	8	9
6	5	8	9	3	9	10	10
9	8	8	10	6	8	6	10
6	8	8	8	4	10	10	9
8	9	9	10	7	10	10	10
7	8	4	7	8	9	8	9
6	7	7	8	8	8	8	8
10	8	10	10	10	10	10	10
8	6	7	9	3	9	8	10
5	4	5	7	2	8	7	9
7	9	10	10	5	10	10	10
5	4	5	7	2	8	8	9
7	5	7	9	5	9	9	10
8	5	6	8	5	9	8	9
9	6	10	10	5	10	10	10
7	3	2	6	1	7	6	9

Role	Industry	Size	Previous experience
I am or fill the role of the Data Protection Officer	Finance/Telecom	50-100 employees	I've studied the EU GDPR in great detail
I'm an owner of an organization	research	0-10 employees	I've read some news articles and overviews
I'm a high level decision maker in an organization	Education (School)	10-50 employees	I've read some news articles and overviews
I'm an owner of an organization	Non profit charity	0-10 employees	I've read some news articles and overviews

I am or will be responsible for the GDPR compliance in my organization	Market Research	0-10 employees	I've read the EU GDPR a little bit
I am or fill the role of the Data Protection Officer	UNIVERSITY	10-50 employees	I've spent more than an hour studying EU GDPR
I'm an owner of an organization, I am or will be responsible for the GDPR compliance in my organization, I am or fill the role of the Data Protection Officer	Software Development	0-10 employees	I've spent more than an hour studying EU GDPR

I am or fill the role of the Data Protection Officer	Automotive	500+ employees	I've studied the EU GDPR in great detail
I'm an owner of an organization	SaaS	0-10 employees	I've studied the EU GDPR in great detail
I am or will be responsible for the GDPR compliance in my organization, I am or fill the role of the Data Protection Officer	Online retailer	100-500 employees	I've studied the EU GDPR in great detail
I'm an owner of an organization, I'm a high level decision	Information Tech, Food Industry, Turism Sector	50-100 employees	I've spent more than an hour studying EU GDPR

maker in an organization			
I'm an owner of an organization	Marketing	0-10 employees	I've read some news articles and overviews
I'm an owner of an organization	Software Development	10-50 employees	I've spent more than an hour studying EU GDPR
I am or fill the role of the Data Protection Officer	Professional Services	50-100 employees	I've studied the EU GDPR in great detail
I am or will be responsible for the GDPR compliance	SaaS	10-50 employees	I've read the EU GDPR a little bit

in my organization			
I'm planning to start my own business sometime in the future	startup	0-10 employees	I've read some news articles and overviews
I am or fill the role of the Data Protection Officer	standardization	50-100 employees	I've studied the EU GDPR in great detail
I'm planning to start my own business sometime in the future	finance	10-50 employees	I've spent more than an hour studying EU GDPR

I am or will be responsible for the GDPR compliance in my organization, I am or fill the role of the Data Protection Officer	IT	10-50 employees	I've studied the EU GDPR in great detail
I'm planning to start my own business sometime in the future, I'm not a high level decision maker, but personally interested in GDPR, I work with personal data	Finance, IT	500+ employees	I've spent more than an hour studying EU GDPR

I'm an owner of an organization	Legal	10-50 employees	I've studied the EU GDPR in great detail
I'm a high level decision maker in an organization	telecommunication	500+ employees	I've studied the EU GDPR in great detail
I'm a high level decision maker in an organization	Marketing	10-50 employees	I've read some news articles and overviews
I'm a high level decision maker in an organization	Training	10-50 employees	I've read some news articles and overviews
I'm an owner of an organization	Cosmetics	10-50 employees	I've read some news articles and overviews

I am or fill the role of the Data Protection Officer	Telecommunication	100-500 employees	I've studied the EU GDPR in great detail
I am or will be responsible for the GDPR compliance in my organization	Data Analytics	10-50 employees	I've spent more than an hour studying EU GDPR
I'm an owner of an organization, I'm a high level decision maker in an organization, I am or will be responsible for the GDPR compliance in my organization, I am or fill the role of	Third Sector (charity)	0-10 employees	I've studied the EU GDPR in great detail

the Data Protection Officer			
I'm planning to start my own business sometime in the future	finance	50-100 employees	I've read some news articles and overviews
I'm a high level decision maker in an organization	Fintech	50-100 employees	I've read the EU GDPR a little bit
I'm an owner of an organization	software development	0-10 employees	I've read the EU GDPR a little bit

I'm planning to start my own business sometime in the future, I'm not a high level decision maker, but personally interested in GDPR	retail	10-50 employees	I've spent more than an hour studying EU GDPR
I am or fill the role of the Data Protection Officer	security	500+ employees	I've studied the EU GDPR in great detail
I am or will be responsible for the GDPR compliance in my organization	Non Profit	100-500 employees	I've spent more than an hour studying EU GDPR

I'm a high level decision maker in an organization, I am or will be responsible for the GDPR compliance in my organization	Health	100-500 employees	I've studied the EU GDPR in great detail
I'm an owner of an organization, I'm planning to start my own business sometime in the future, I am or fill the role of the Data Protection Officer	Telecommunication	500+ employees	I've spent more than an hour studying EU GDPR
I'm an owner of an organization	e-commerce	0-10 employees	I've read some news articles

			and overviews
I'm an owner of an organization	Utility software	0-10 employees	I've read some news articles and overviews
I am or fill the role of the Data Protection Officer	Fintech	50-100 employees	I've studied the EU GDPR in great detail
I am or will be responsible for the GDPR compliance in my organization	Marketing	10-50 employees	I've read the EU GDPR a little bit
I am or will be responsible for the GDPR compliance	retail	50-100 employees	I've read the EU GDPR a little bit

in my organization			
I'm an owner of an organization	IT	50-100 employees	I've read the EU GDPR a little bit
I'm a high level decision maker in an organization	banking	500+ employees	I've read the EU GDPR a little bit
I am or will be responsible for the GDPR compliance in my organization	consulting	10-50 employees	I've read some news articles and overviews